

THIS FILE IS MADE AVAILABLE THROUGH THE DECLASSIFICATION EFFORTS AND RESEARCH OF:

THE BLACK VAULT

THE BLACK VAULT IS THE LARGEST ONLINE FREEDOM OF INFORMATION ACT / GOVERNMENT RECORD CLEARING HOUSE IN THE WORLD. THE RESEARCH EFFORTS HERE ARE RESPONSIBLE FOR THE DECLASSIFICATION OF THOUSANDS OF DOCUMENTS THROUGHOUT THE U.S. GOVERNMENT, AND ALL CAN BE DOWNLOADED BY VISITING:

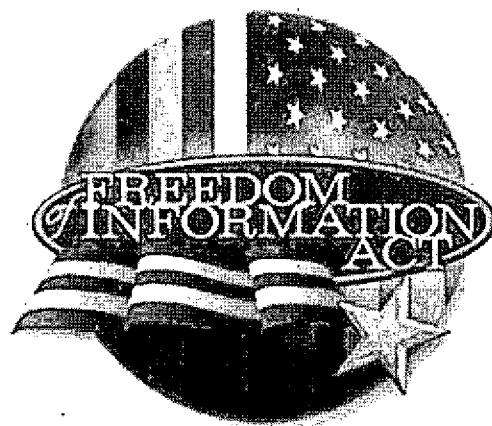
[HTTP://WWW.BLACKVAULT.COM](http://www.blackvault.com)

YOU ARE ENCOURAGED TO FORWARD THIS DOCUMENT TO YOUR FRIENDS, BUT PLEASE KEEP THIS IDENTIFYING IMAGE AT THE TOP OF THE .PDF SO OTHERS CAN DOWNLOAD MORE!

FREEDOM OF INFORMATION AND PRIVACY ACTS

**SUBJECT: MANUAL OF INVESTIGATIVE
OPERATIONS AND GUIDELINES (MIOG)**

**VOLUME 3
SECTIONS 1-13**



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.**



VOLUME III

SECTION 1-13

*Manual of
Investigative
Operations
and Guidelines*



U.S. Department of Justice
Federal Bureau of Investigation

MANUAL OF
INVESTIGATIVE
OPERATIONS
AND
GUIDELINES

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 1 - 1

SECTION 1. FEDERAL CRIMINAL LAW

1-1 GENERAL DEFINITIONS

EFFECTIVE: 10/24/85

1-1.1 United States

The term, "United States," as used in Title 18 in a territorial sense, includes all places and waters, continental or insular, subject to the jurisdiction of the United States, except the Canal Zone. (18 U.S.C. 5)

EFFECTIVE: 10/24/85

1-1.2 Department

"Department" means one of the executive departments enumerated in Section 1 of Title 5, unless the context shows that such term was intended to describe the executive, legislative, or judicial branches of the Government. (18 U.S.C. 6)

EFFECTIVE: 10/24/85

1-1.3 Agency

"Agency" includes any department, independent establishment, commission, administration, authority, board or bureau of the United States or any corporation in which the United States has a proprietary interest, unless the context shows that such term was intended to be used in a more limited sense. (18 U.S.C. 6)

EFFECTIVE: 10/24/85

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 1 - 2

1-1.4 Special Maritime and Territorial Jurisdiction of the
United States | (See MIOG, Part I, 7-3, 45-1.1 and 45-5;
Part II, 1-1.10.) |

As used in Title 18, this phrase includes the following:

"(1) The high seas, any other waters within the admiralty and maritime jurisdiction of the United States and out of the jurisdiction of any particular State, and any vessel belonging in whole or in part to the United States or any citizen thereof, or to any corporation created by or under the laws of the United States, or of any State, Territory, District, or possession thereof, when such vessel is within the admiralty and maritime jurisdiction of the United States and out of the jurisdiction of any particular State.

"(2) Any vessel registered, licensed, or enrolled under the laws of the United States, and being on a voyage upon the waters of any of the Great Lakes, or any of the waters connecting them, or upon the Saint Lawrence River where the same constitutes the International Boundary Line.

"(3) Any lands reserved or acquired for the use of the United States, and under the exclusive or concurrent jurisdiction thereof, or any place purchased or otherwise acquired by the United States by consent of the legislature of the State in which the same shall be, for the erection of a fort, magazine, arsenal, dockyard, or other needful building.

"(4) Any island, rock, or key containing deposits of guano, which may, at the discretion of the President, be considered as appertaining to the United States.

"(5) Any aircraft belonging in whole or in part to the United States, or any citizen thereof, or to any corporation created by or under the laws of the United States, or any State, Territory, District, or possession thereof, while such aircraft is in flight over the high seas, or over any other waters within the admiralty and maritime jurisdiction of the United States and out of the jurisdiction of any particular State.

"(6) Any vehicle used or designed for flight or navigation in space and on the registry of the United States pursuant to the Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies and the Convention on Registration of Objects Launched into Outer Space, while that vehicle is in flight, which is

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 1 - 3

from the moment when all external doors are closed on Earth following embarkation until the moment when one such door is opened on Earth for disembarkation or in the case of a forced landing, until the competent authorities take over the responsibility for the vehicle and for persons and property aboard.

"(7) Any place outside the jurisdiction of any nation with respect to an offense by or against a national of the United States.

"(8) To the extent permitted by international law, any foreign vessel during a voyage having a scheduled departure from or arrival in the United States with respect to an offense committed by or against a national of the United States." (18 U.S.C. 7)

EFFECTIVE: 02/11/97

1-1.5 Obligation or Other Security of the United States

The term, "obligation or other security of the United States," includes all bonds, certificates of indebtedness, national bank currency, Federal Reserve notes, Federal Reserve bank notes, coupons, United States notes, Treasury notes, gold certificates, silver certificates, fractional notes, certificates of deposit, bills, checks, or drafts for money, drawn by or upon authorized officers of the United States, stamps and other representatives of value, of whatever denomination, issued under any Act of Congress, and cancelled United States stamps. (18 U.S.C. 8)

EFFECTIVE: 10/24/85

1-1.6 Vessel of the United States

The term, "vessel of the United States," as used in Title 18 means a vessel belonging in whole or in part to the United States, or any citizen thereof, or any corporation created by or under the laws of the United States, or of any State, Territory, District, or possession thereof. (18 U.S.C. 9)

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 1 - 4

EFFECTIVE: 10/24/85

1-1.7 Interstate Commerce

The term, "interstate commerce," as used in Title 18 includes commerce between one State, Territory, Possession, or the District of Columbia and another State, Territory, Possession, or the District of Columbia. (18 U.S.C. 10)

EFFECTIVE: 10/24/85

1-1.8 Foreign Commerce

The term, "foreign commerce," as used in Title 18 includes commerce with a foreign country. (18 U.S.C. 10)

EFFECTIVE: 10/24/85

1-1.9 Foreign Government

The term, "foreign government," as used in Title 18, includes any government, faction, or body of insurgents within a country with which the United States is at peace, irrespective of recognition by the United States. (18 U.S.C. 11)

EFFECTIVE: 10/24/85

1-1.10 Assimilative Crimes Statute

Whoever within or upon any of the places now existing or hereafter reserved or acquired as provided in 18 U.S.C. 7 (see paragraph 1-1.4 above), is guilty of any act of omission which, although not made punishable by any enactment of Congress, would be punishable if committed or omitted within the jurisdiction of the State, Territory, Possession, or District in which such place is situated, by the laws thereof in force at the time of such act or omission, shall be guilty of a like offense and subject to a like punishment. (18 U.S.C. 13)

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 1 - 5

EFFECTIVE: 10/24/85

1-1.11 Citation of Code Section

Complaints filed before U.S. Magistrates for violations of Title 18, U.S.C., should refer to the revised section of the code as follows: "Title 18, U.S.C., Section (no.) _____."

EFFECTIVE: 10/24/85

1-1.12 Definition of Stolen or Counterfeit Nature of Property for Certain Crimes (See MIOG, Part I, 15-1.1.1, 15-3.1, 15-3.2, 26-1.9, 26-4.5, 52-1.5, 87-2.1.1, 87-2.1.3, 87-2.2.1, 87-2.2.2, 87-2.3.1, 87-2.3.2, 87-4.4, 91-3.10, 103-1.5, 198-2.8, and 1-1.12.1 through 1-1.12.5 below.)

Whenever it is an element of an offense in Title 18 that:

"(1) any property was embezzled, robbed, stolen, converted, taken, altered, counterfeited, falsely made, forged, or obliterated; and

"(2) the defendant knew that the property was of such character;

such element may be established by proof that the defendant, after or as a result of an official representation as to the nature of the property, believed the property to be embezzled, robbed, stolen, converted, taken, altered, counterfeited, falsely made, forged, or obliterated. . . . For purposes of this section, the term 'official representation' means any representation made by a Federal law enforcement officer (as defined in section 115) or by another person at the direction or with the approval of such an officer." (Title 18, U.S.C., Section 21).

EFFECTIVE: 10/23/95

XXXXXX
XXXXXX
XXXXXXFEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET3

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 552Section 552a☐ (b)(1)☐ (b)(7)(A)☐ (d)(5)☒ (b)(2)☐ (b)(7)(B)☐ (j)(2)☐ (b)(3)☐ (b)(7)(C)☐ (k)(1)☐ (b)(7)(D)☐ (k)(2)☒ (b)(7)(E)☐ (k)(3)☐ (b)(7)(F)☐ (k)(4)☐ (b)(4)☐ (b)(8)☐ (k)(5)☐ (b)(5)☐ (b)(9)☐ (k)(6)☐ (b)(6)☐ (k)(7)

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

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

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

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

Pages were not considered for release as they are duplicative of _____

Page(s) withheld for the following reason(s): _____

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

1106 Pt II Sec 1 p6-8

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

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 1 - 9

1-1.12.4 Establishing other Elements of Federal Offenses with Title 18, USC, Section 21 (See MIOG, Part II, 1-1.12.)

(1) The scope of section 21 casts a broad net, encompassing a number of Title 18 offenses, many of which require proof of interstate or foreign travel. Others require, for example, a showing that property belongs to the government (Title 18, USC, Section 641) or was part of an interstate shipment (Title 18, USC, Section 659). Prior to the enactment of section 21, if the government had charged a defendant with the substantive offense of receiving stolen goods, it had to prove that the defendant knew the goods were stolen and that the goods crossed a state or United States boundary. (Title 18, USC, Section 2315.) Under the new statute, it is clear that proof of the first element (knowledge that the property is stolen) can be accomplished by undercover representation that the property was "stolen." But there is no provision in the text of the statute for satisfying the interstate or foreign travel requirement merely through representation.

(2) Since Congress expressly provided for representation of only one element, it seems clear that it intended to retain the status quo with respect to the other elements of proof. This interpretation requires proof that the goods actually cross a state or United States boundary after being stolen or represented as such.

EFFECTIVE: 10/23/95

1-1.12.5 Conspiracy and Title 18, USC, Section 21 (See MIOG, Part II, 1-1.12.)

(1) With respect to inchoate crimes and conspiracy, section 21 appears to have no impact, because a conspiracy charge can be maintained regardless of whether the property was stolen or merely represented as stolen. It is possible then that a conspiracy charge could be maintained where property which is represented as stolen is also represented as having traveled in interstate commerce under circumstances where two or more of the targets agree to commit the illegal act, i.e., if the jurisdictional nexus can be supplied by evidence that the defendants had agreed to receive goods that they believed were both stolen and transported interstate. SEE UNITED STATES V. ROSE, 590 F.2d 232, 235-36 (7th Cir. 1978) (jurisdictional nexus established where defendants plotted to steal property in Arizona and have it transported

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 1 - 10

to Illinois, but unwittingly recruited undercover Agents to commit the robbery and transport the property, so neither theft nor interstate transport occurred), CERT. DENIED, 442 U.S.929 (1979); cf. UNITED STATES V. ROSA, 17 F.3d 1531, 1544-46 (2d Cir.) (jurisdictional nexus supplied because goods defendants purchased, believing they were stolen, had in fact traveled across state lines, and alternatively because at least one member of the conspiracy believed that the goods had traveled interstate), CERT. DENIED, 115 S. Ct. 221 (1994).

(2) Given the various circumstances which may suffice to supply the federal jurisdictional predicate for a conspiracy, charging a conspiracy as well as the substantive violation can enhance the potential for obtaining a conviction. Of course, the Chief Division Counsel and the appropriate United States Attorney's office should be consulted in each case when developing undercover scenarios and evaluating prosecutorial strategies. In addition, FBIHQ approval should be obtained pursuant to the Attorney General's Guidelines on FBI Undercover Operations when circumstances so require.

EFFECTIVE: 10/23/95

1-2 FEDERAL CRIMES

All federal crimes are statutory; there are no federal common law crimes.

(1) Felony

A felony is any offense punishable by death or imprisonment for a term exceeding one year. Additionally, felonies have been divided into five classifications:

(a) Class A - maximum penalty of death or life imprisonment;

(b) Class B - maximum penalty of 25 years or more in prison;

(c) Class C - maximum term of imprisonment of 10 or more years, but less than 25 years;

(d) Class D - maximum term of imprisonment of five years or more, but less than 10 years;

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 1 - 11

(e) Class E - maximum term of imprisonment of more than one year, but less than five years.

A person or an organization convicted of a felony offense may also be fined the greatest of (1) the amount specified in the law setting forth the offense; (2) twice the pecuniary gain or loss caused by the offense or \$250,000 (\$500,000 in case of a corporation).

(2) Misdemeanor

Any other offense is a misdemeanor. However, misdemeanor offenses have also been classified as follows:

(a) Class A - maximum term of imprisonment of more than six months, but not exceeding one year;

(b) Class B - maximum term of imprisonment of six months, but more than 30 days;

(c) Class C - maximum term of imprisonment of 30 days, but more than five days;

(d) Infraction - five days or less, or if no imprisonment is authorized.

A person convicted of a misdemeanor that resulted in the loss of human life may be fined up to \$250,000, or in the case of an organization, \$500,000. The maximum fine for persons convicted of other misdemeanors is \$100,000 (\$200,000 for organizations). The penalty for an infraction may include a fine of up to \$5,000 for individuals and \$10,000 for an organization.

(3) Under Title 18, USC, Section 3401, a U.S. Magistrate, under certain circumstances, may try persons accused of, and sentence persons convicted of, misdemeanors committed within the district in which the U.S. Magistrate presides.

EFFECTIVE: 02/11/97

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 1 - 12

1-3 PARTIES TO CRIME

(1) Principal

A person who commits an offense against the United States or aids, abets, counsels, commands, induces, or procures its commission, is punishable as a principal. Likewise, a person who willfully causes an act to be done which if directly performed by him/her or another would be an offense against the United States, is punishable as a principal. (Title 18, USC, Section 2) This section makes clear the intent of Congress to punish as a principal one who puts in motion or assists in the illegal enterprise or causes the commission of an indispensable element of the offense by an innocent agent or instrumentality, even though he/she intentionally refrained from the direct act constituting the completed offense.

(2) Accessory After the Fact

Any person, knowing that an offense against the United States has been committed, receives, relieves, comforts or assists the offender in order to hinder or prevent his/her apprehension, trial or punishment is an accessory after the fact. Punishment for an accessory is less severe than that of a principal. (Title 18, USC, Section 3)

(a) Classification of an offense involving an accessory is the same as the substantive offense.

(b) Character of offense should be shown as:
"(Substantive Offense) - Accessory After the Fact."

(c) Copies of reports to FBIHQ should be the same as in the case of the substantive offense.

EFFECTIVE: 02/22/88

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 1 - 13

1-4 STATUTE OF LIMITATIONS

The statute of limitations operates from the time a crime is actually committed until the time an indictment is returned or an information is instituted. An indictment or information stops the running of the statute of limitations although the accused may not be in custody or tried for some time thereafter.

(1) Capital Offense

An indictment for any offense punishable by death may be found at any time without limitation. (Title 18, USC, Section 3281)

(2) Noncapital Offense

Unless otherwise expressly provided by law, no person shall be prosecuted, tried or punished for any offense, not capital, unless the indictment is found or the information is instituted within five years next after such offense shall have been committed. (Title 18, USC, Section 3282)

(3) Fugitive

No statute of limitations shall extend to any person fleeing from justice. (Title 18, USC, Section 3290)

(4) In all investigations, particularly if the defendant is a fugitive, employees should give due regard to the statute of limitations and request U.S. Attorneys to secure indictments or file informations within the five-year period in order to avoid this plea as a bar to prosecution of the defendant.

(5) Extension of Statute of Limitations for Certain Terrorism Offenses (Title 18, USC, Section 3286):

"Notwithstanding section 3282, no person shall be prosecuted, tried or punished for any offense involving a violation of section 32 (aircraft destruction), section 36 (airport violence), section 112 (assaults upon diplomats), section 351 (crimes against Congressmen or Cabinet officers), section 1116 (crimes against diplomats), section 1203 (hostage taking), section 1361 (willful injury to government property), section 1751 (crimes against the President), section 2280 (maritime violence), section 2281 (maritime platform violence), section 2331 (terrorist acts abroad against United States nationals), section 2339 (use of weapons of mass destruction),

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 1 - 14

or section 2340A (torture) of this title or section 46502, 46504, 46505 or 46506 of title 49, unless the indictment is found or the information is instituted within eight years after the offense was committed."

(a) The above shall not apply to any offense committed MORE than five years prior to the date of the enactment of this act (September 13, 1994).

(b) For clarification regarding the statute of limitations pertaining to FBI counterterrorism extraterritorial investigations PRIOR to the passage of this legislation, the DOJ has advised the following:

1. MURDER - The statute of limitations will expire EIGHT years from the occurrence of the offense in cases in which U.S. nationals were MURDERED abroad IF the murder occurred five years PRIOR to September 13, 1994, AND DOJ has determined that the specific case is a violation of Title 18, USC, Section 2331. There is NO statute of limitations in cases where a U.S. national was murdered ON THE DATE OF THE PASSAGE OF THIS ACT (September 13, 1994).

2. ATTEMPTED MURDER OR CONSPIRACY TO MURDER - DOJ advised that the statute of limitations will expire FIVE years from the anniversary of the offense in cases of ATTEMPTED murder of a U.S. national outside the United States if the attempted murder occurred FIVE years prior to September 13, 1994.

EFFECTIVE: 02/14/97

1-5 MISPRISION OF A FELONY

It is a federal offense punishable by a fine or imprisonment of not more than three years, or both, for a person, having knowledge of the actual commission of a felony cognizable by a court of the United States, to conceal and not make known as soon as possible this fact to a judge or other person in civil or military authority under the United States. (Title 18, USC, Section 4)

(1) Classification of a misprision violation is the same as the substantive offense.

(2) Character of offense should be shown as:

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 1 - 15

"(Substantive Offense) - Misprision of Felony."

(3) Copies of reports to FBIHQ should be the same as in the case of the substantive offense.

EFFECTIVE: 02/11/97

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 2 - 1

SECTION 2. FEDERAL RULES OF CRIMINAL PROCEDURE

2-1 IN GENERAL

The Federal Rules of Criminal Procedure (FED.R.CRIM.P.) govern the procedure in all criminal proceedings in the Federal courts; and, whenever specifically provided in one of the rules, to preliminary, supplementary, and special proceedings before United States Magistrates and at proceedings before state and local judicial officers.

EFFECTIVE: 08/21/87

2-2 VENUE (RULE 18)

Except as otherwise permitted by statute or by the FED.R.CRIM.P., prosecution shall be had in a district in which the offense was committed. The court shall fix the place of trial within the district with due regard to the convenience of the defendant and the witnesses.

EFFECTIVE: 08/21/87

2-3 UNITED STATES MAGISTRATE (USMAGIS)

USMAGIS's are appointed by the judges of each Federal district court in such numbers and at such locations as the Judicial Conference of the United States may determine.

EFFECTIVE: 08/21/87

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 2 - 2

2-3.1 Duties

The chief duties of the USMAGIS's are to:

- (1) Receive complaints concerning crimes against the United States.
- (2) Issue warrants of arrest, search warrants, summonses, and subpoenas.
- (3) Conduct proceedings at the initial appearance and preliminary examination of an arrested or summoned person to determine whether there is probable cause to hold him/her for further criminal process, and conduct removal hearings under Rule 40.
- (4) Appoint counsel under the Criminal Justice Act of 1964 for arrested persons who are unable to retain counsel of their own; admit arrested persons to bail under the Bail Reform Act of 1984 (Title 18, USC, Sections 3141-3156); and commit to jail those who fail to make bail.
- (5) Try misdemeanor cases pursuant to Title 18, USC, Section 3401 when specially designated by the district court and if the accused files a written consent to be tried by the magistrate that specifically waives trial, judgment and sentencing by a judge of the district court. In all cases resulting in conviction, an appeal may be taken to a judge of the district court of the district in which the offense was committed.

EFFECTIVE: 08/21/87

2-4 STATE MAGISTRATES

Title 18, USC, Section 3041 provides that "for any offense against the United States, the offender may, by any justice or judge of the United States, or by any United States magistrate, or by any chancellor, judge of a supreme or superior court, chief or first judge of common pleas, mayor of a city, justice of the peace, or other magistrate, of any state where the offender may be found, and at the expense of the United States, be arrested and imprisoned or released . . . as the case may be, for trial before such court of the United States as by law has cognizance of the offense." Thus, for purposes of Rules 3, 4, and 5, FED.R.CRIM.P., state officials included in the foregoing statute have the same authority as a USMAGIS. State

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 2 - 3

officials, however, may not conduct preliminary proceedings under Rule 40, [FED.R.CRIM.P.]

EFFECTIVE: 08/16/82

2-5 COMPLAINTS (RULE 3)

The complaint is a written statement of the essential facts constituting the offense charged. It shall be made upon oath before a magistrate. The latter term, "magistrate," as noted, includes a [USMAGIS], a judge of the United States, and a state or local judicial officer, authorized by Title 18, USC, Section 3041 to perform the functions prescribed in Rules 3, 4, and 5. Probable cause must be shown in the complaint or in an affidavit to be filed with the complaint. References to "complaint" used in this and related paragraphs should be understood to embrace the affidavit filed with the complaint.

EFFECTIVE: 08/16/82

2-5.1 Authorization of U.S. Attorney (USA)

Special Agents shall obtain prior authority from the USA or an Assistant USA (AUSA) before filing a criminal complaint. If Agents are uncertain as to the Bureau's investigative jurisdiction, they should confer with the SAC before filing a complaint. Agents shall not urge prosecution or suggest that no prosecution be undertaken; nor shall they express an opinion as to the advisability of entering a nolle prosequi in any case investigated by the Bureau. The determination as to whether the case will be prosecuted is a function of the USA or an official of the Department of Justice when such decisions are reserved by the Department. The function of SAs of the FBI is to conduct thorough investigations of cases in a legal and ethical manner and carry through to a logical conclusion. Generally, any information desired by the USA in connection with a case investigated by SAs of this Bureau should be furnished upon his/her request. If in doubt, request FBIHQ advice.

EFFECTIVE: 08/16/82

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 2 - 4

2-5.2 Re-presentation of Cases

Special Agents shall not re-present cases to the USAs when they once have declined prosecution unless new evidence has been developed. In the event the Department instructs or if other reasons exist justifying a re-presentation of a case to the USA, only the SAC or the designated Assistant SAC (ASAC) will be authorized to make such a re-presentation of the case to the USA. This rule shall not be interpreted so as to interfere with full and complete discussions between SAs and the USAs concerning cases over which the latter has jurisdiction.

EFFECTIVE: 08/16/82

2-5.3 State Prosecutions

Criminal investigations conducted by the FBI are designed to obtain evidence for prosecution in Federal court and not in state or local courts. When Agents discuss cases with the USA or his/her assistant, it is expected that such will be done with sufficient aggressiveness to ensure the Bureau's interests are fully protected. The FBI does not have the manpower to investigate violations which are later prosecuted in other than Federal courts. During presentations of cases to USAs, it is expected that the amount of time and effort expended by FBI personnel will be made known in its proper perspective. Consideration can then be given to this factor by the USA prior to deciding whether he/she will decline prosecution in favor of handling by local authorities. Be aware that if a case is investigated by the FBI and prosecuted in local court, additional Agent time and expense may well be lost if Bureau personnel are called on to testify in state court.

EFFECTIVE: 08/16/82

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 2 - 5

2-5.4 Authority for Issuance of Warrant

The |USMAGIS's| have authority to issue warrants or summonses for any person charged with a felony or misdemeanor if: (a) a complaint under oath is filed containing sufficient facts, (b) to constitute a Federal offense, and (c) to satisfy the |USMAGIS| that probable cause exists for the issuance of a warrant. Any citizen may act as complainant, but in such cases, |USMAGIS's| will rarely issue a warrant without first securing the approval of the USA.

EFFECTIVE: 08/16/82

2-5.5 Notification to Special Agent in Charge (SAC)

The SAC shall be notified immediately when complaints are filed. This notification should be set forth by memorandum in the usual case. A copy of every complaint and of any affidavit filed with the complaint by an Agent is to be obtained and filed as serials in the field office case file. Where efforts to have process issued are unsuccessful, for any reason, this fact should be reported.

EFFECTIVE: 08/16/82

2-6 WARRANT OF ARREST OR SUMMONS (RULE 4)

EFFECTIVE: 08/16/82

2-6.1 Forms of Warrant

There are two forms of warrants for the arrest of Federal law violators. The Magistrate's Warrant is issued by the |USMAGIS| based upon a complaint. A Bench Warrant is issued by the clerk of the U.S. District Court following the return of an indictment or the filing of an information on order of the district judge.

EFFECTIVE: 08/16/82

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 2 - 6

2-6.2 Issuance of Warrant or Summons

If it appears from the complaint, or an affidavit or affidavits filed with the complaint, that there is probable cause to believe that an offense has been committed and that the defendant has committed it, a warrant for the arrest of the defendant shall issue to any officer authorized by law to execute it. The finding of probable cause may be based upon hearsay evidence in whole or in part. Warrants should be addressed to "Any United States Marshal or any other authorized officer." Upon the request of the attorney for the Government, a summons instead of a warrant shall issue. More than one warrant or summons may issue on the same complaint. If a defendant fails to appear in response to a summons, a warrant shall issue. If an indictment is returned by the grand jury or an information, supported by oath and establishing probable cause, is filed, the court shall issue a warrant for each defendant named upon the request of the USA. The court or the USA may request the issuance of a summons instead of a warrant.

EFFECTIVE: 08/28/91

2-6.3 Execution

(1) Arrest warrants shall be executed by a marshal or by some other officer authorized by law. The warrant may be executed at any place within the jurisdiction of the United States. Therefore, when a warrant has been issued and is still outstanding, it is not necessary to file another complaint and obtain another warrant in another jurisdiction for the same offense. The warrant shall be executed by the arrest of the defendant. The officer need not have the warrant in his/her possession at the time of the arrest but, upon request, he/she shall show the warrant to the defendant as soon as possible. If the officer does not have the warrant in his/her possession at the time of arrest, he/she shall then inform the defendant of the offense charged and of the fact that a warrant has been issued. When time will permit and the successful arrest of subject will in no way be jeopardized, the arresting Agent should have the warrant of arrest in his/her possession in order that the same may be exhibited to the subject upon request.

(2) A summons may be served at any place within the jurisdiction of the United States. The summons shall be served upon a defendant by delivering a copy to him/her personally, or by leaving it at his/her dwelling house or usual place of abode with some person of

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 2 - 7

suitable age and discretion then residing therein, and by mailing it to the defendant's last known address. Summonses should not be served by Bureau Agents except upon FBIHQ authority.

EFFECTIVE: 08/28/91

2-7 PROCEEDINGS BEFORE THE MAGISTRATE (RULE 5)

EFFECTIVE: 08/28/91

2-7.1 Initial Appearance (See MIOG, Part I, 88-5.2; Part II, 2-11.4.1, 11-1.4; and Legal Handbook for Special Agents, 3-5.)

Except as provided below, the arrested person shall be taken without unnecessary delay before the nearest available federal magistrate or, in the event that a federal magistrate is not reasonably available, before a state or local judicial officer authorized by Title 18, USC, Section 3041. That procedure need not be followed if the person is arrested under a warrant issued upon a complaint that charges only a violation of Title 18, USC, Section 1073 (UFAP), the arrested person is transferred without unnecessary delay to the custody of appropriate state or local authorities in the district of arrest, and the government attorney in the originating district moves promptly for the dismissal of the UFAP complaint. (The Department of Justice Criminal Division has advised FBIHQ that it is not necessary to wait until the UFAP warrant has actually been dismissed before releasing the subject to state or local authorities, but it is important that efficient procedures be implemented and followed to make sure that UFAP warrants are promptly dismissed after notification of an arrest is given.) If a person arrested without a warrant is brought before a magistrate, a complaint shall be filed forthwith which shall comply with the requirements of Rule 4(a) with respect to the showing of probable cause. A personal, telephone, or electronic presentation of the complaint setting forth probable cause for the magistrate must occur within 48 hours following a warrantless arrest if the arrestee is detained and an initial appearance cannot be held within that 48-hour period.

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 2 - 8

EFFECTIVE: 05/10/96

2-7.2 Misdemeanors

If the charge against the defendant is a misdemeanor triable by a USMAGIS under Title 18, USC, Section 3401, the USMAGIS shall proceed in accordance with the Rules of Procedure for the Trial of Misdemeanors Before U.S. Magistrates. If the charge against the defendant is not triable by the USMAGIS, the defendant shall not be called upon to plead.

EFFECTIVE: 08/28/91

2-7.3 Statement by Magistrate

The magistrate shall inform the defendant:

(1) Of the complaint against him/her and of any affidavit filed therewith.

(2) Of his/her right to retain counsel and of his/her right to request the assignment of counsel if he/she is unable to obtain counsel (followed by appointment of counsel where the arrested person requests counsel and has been unable to obtain counsel - Criminal Justice Act of 1964). The magistrate shall allow the defendant reasonable time and opportunity to consult counsel.

(3) Of the general circumstances under which he/she may secure pretrial release - Bail Reform Act of 1984 (Title 18, USC, Sections 3141-3156). The magistrate may set such conditions as are appropriate to assure the defendant's presence at subsequent judicial proceedings and to assure the safety of any other person or the community. If no condition or combination of conditions would reasonably assure the appearance of the defendant as required and the safety of any other person and the community, after a hearing the magistrate may order the detention of the person prior to trial. To assist in determining eligibility for pretrial release, the magistrate may receive information provided by or through the chief pretrial services officer of the district. Agents contacted by pretrial services officers for information relative to the defendant's pretrial release should record in the investigative file all such information provided.

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 2 - 9

(4) That defendant is not required to make a statement and that any statement made by defendant may be used against him/her.

(5) Of defendant's right to a preliminary examination.

EFFECTIVE: 08/21/87

2-7.4 Waiver of Preliminary Examination

A defendant is entitled to a preliminary examination, unless waived, when charged with any offense other than a petty offense, which is to be tried by a judge of the district court. If the defendant waives preliminary examination, the magistrate shall forthwith hold defendant to answer in the district court. If the defendant does not waive the preliminary examination, the magistrate shall schedule a preliminary examination. Such examination shall be held within a reasonable time but, in any event, not later than 10 days following the initial appearance if the defendant is in custody and no later than 20 days if defendant is not in custody, provided, however, that the preliminary examination shall not be held if the defendant is indicted or if an information against the defendant is filed in district court before the date set for the preliminary examination. With the consent of the defendant and upon a showing of good cause, taking into consideration the public interest in the prompt disposition of criminal cases, time limits specified in this rule may be extended one or more times by a Federal magistrate. In the absence of such consent by the defendant, time limits may be extended by a judge of the United States only upon a showing that extraordinary circumstances exist and that delay is indispensable to the interests of justice.

EFFECTIVE: 08/21/87

2-7.5 Custody Pending Hearing

If the arrested person is to be held for a preliminary examination or for the district court and he/she cannot furnish bond, he/she is incarcerated until presented before the USMAGIS or the U.S. District Court.

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 2 - 10

EFFECTIVE: 08/16/82

2-8 PRELIMINARY EXAMINATION (RULE 5.1)

The preliminary examination is an adversary hearing, the purpose of which is to determine if there is probable cause for holding the accused to await the action of the U.S. District Court. Witnesses testify under oath and are subject to cross-examination. The hearing is usually before a USMAGIS.

EFFECTIVE: 08/16/82

2-8.1 Role of Special Agent

Special Agents of the Bureau in practice are frequently present at such preliminary examinations before USMAGIS's in cases which they have investigated. It sometimes occurs they are requested by the USMAGIS to put on the Government's witnesses and to cross-examine the defendants. However, the USA or his/her assistant is the proper person to represent the Government at such preliminary examinations. Under no circumstances shall such Agents examine witnesses at these hearings. When it is impossible for the USA or his/her assistant to be present, the USMAGIS will usually conduct the hearing or arrange to question the witnesses himself/herself in order to ascertain the facts in the case.

EFFECTIVE: 08/16/82

2-8.2 Discharge

If from the evidence it appears that there is no probable cause to believe that an offense has been committed or that the defendant committed it, the USMAGIS shall dismiss the complaint and discharge the defendant. The discharge of the defendant shall not preclude the Government from instituting a subsequent prosecution for the same offense. If a USMAGIS discharges a defendant, this is not, if noted, a bar to further prosecution. A hearing before a USMAGIS does not constitute jeopardy.

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 2 - 11

EFFECTIVE: 08/16/82

2-8.3 Finding of Probable Cause

If from the evidence it appears that there is probable cause to believe that an offense has been committed and that the defendant committed it, the USMAGIS shall forthwith hold him/her to answer in district court. The finding of probable cause may be based upon hearsay evidence in whole or in part. The defendant may cross-examine witnesses against him/her and may introduce evidence in his/her own behalf.

EFFECTIVE: 02/11/97

2-8.4 Objections to Evidence

Objections to evidence on the ground that it was acquired by unlawful means are not properly made at the preliminary examination. Motions to suppress must be made to the trial court as provided in Rule 12.

EFFECTIVE: 08/16/82

2-9 GRAND JURY (RULE 6)

EFFECTIVE: 08/21/87

2-9.1 Purpose

The function of the grand jury is to decide if there is sufficient and probable cause for trying the defendant in court. It makes this determination based on evidence presented by the USA or AUSA in an ex parte proceeding. The grand jury operates under the direction and guidance of the U.S. District Court. Generally, only witnesses for the prosecution testify before the grand jury.

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 2 - 12

EFFECTIVE: 08/21/87

2-9.2 Persons Present

Only the USA or an assistant, the witness under examination, interpreters when needed, and, for the purpose of taking the evidence, a stenographer or operator of a recording device may be present while the grand jury is in session. No person other than the jurors may be present while the grand jury is deliberating or voting.

EFFECTIVE: 08/21/87

2-9.3 Disclosure

A grand juror, interpreter, stenographer, operator of a recording device, typist, attorney for the Government, or other Government personnel designated by the attorney for the Government shall not disclose matters occurring before the grand jury.

EFFECTIVE: 08/21/87

2-9.4 Exceptions (See MIOG, Part II, 2-9.5, 2-9.5.1, 2-9.7;
MAOP, Part II, 9-9.)

Exceptions to the foregoing rule are where disclosure:

(1) is ordered by the court preliminarily to or in connection with a judicial proceeding;

(2) is permitted by the court at the request of defendant upon showing that grounds may exist to dismiss the indictment because of matters occurring before the grand jury;

(3) is made to an attorney for the government for use in the performance of his/her duty;

(4) is made to such government personnel (including personnel of a state or subdivision of a state) as are deemed necessary by an attorney for the government to assist an attorney for

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 2 - 13

the government in the performance of his/her duty to enforce federal criminal law;

(5) is made by an attorney for the government to another federal grand jury; and

(6) is permitted by a court at the request of an attorney for the government, upon a showing that such matters may disclose a violation of state criminal law, to an appropriate official of a state or subdivision of a state for the purpose of enforcing such law.

EFFECTIVE: 07/12/95

2-9.5 Limitation of Use | (See MIOG, Part II, 2-9.5.1, 2-9.7,
23-6.6.5; MAOP, Part II, | 2-4.4.16, | 9-9.)

Pursuant to Federal Rule of Criminal Procedure 6 (e) (3) (A) (ii) (the Rule), FBI and other government personnel to whom disclosure is made under MIOG, Part II, 2-9.4 above may not use grand jury material thus disclosed for any purpose other than assisting the attorney for the government in the performance of his/her duty to enforce federal criminal law. Grand jury secrecy continues indefinitely, regardless of whether there is an indictment, unless the material becomes a matter of public record, such as by being introduced at trial. Because of the severe limitations on the use of information that is obtained by the use of a grand jury subpoena, whenever possible, alternatives to the grand jury subpoena, such as administrative subpoenas, search warrants, witness interviews, and electronic surveillance should be considered as a method of obtaining evidence, especially if future civil sanctions are likely. The following requirements are necessary because of the Rule's mandate of secrecy.

(1) Disclosure of grand jury material cannot be made within the FBI for unrelated investigations unless a government attorney has determined that such disclosure to a particular investigator is needed to assist that attorney in a specific criminal investigation. The ability of government attorneys to freely share grand jury material with other government attorneys for related or unrelated criminal investigations does not extend to investigators without case specific authorization from the government attorney. Therefore, grand jury material cannot be entrusted to a general system of records, freely accessible to individual Agents acting on

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 2 - 14

| their own. (See MAOP, Part II, 2-4.4.4|and 2-4.4.16.)|

(2) In the event that a government attorney authorizes the disclosure of grand jury material in the possession of the FBI for use in an unrelated federal criminal matter, such approval should be documented in the appropriate grand jury subfile(s). That documentation will, of course, be in addition to any necessary supplementation to the government attorney's Rule 6(e) disclosure letter and/or to the internal disclosure list.

(3) Grand jury information cannot be used for civil cases or noncriminal investigations without a court order. The U.S. Attorney's Office (USAO) should be consulted immediately for precautionary instructions if the possibility arises that grand jury material will have application in civil law enforcement functions (e.g., civil RICO or civil forfeiture). There are very limited exceptions that allow government attorneys to use grand jury materials or information in civil matters (e.g., civil penalty proceedings concerning banking law violations). However, these exceptions do not automatically apply to investigative personnel. Therefore, any similar use of grand jury information by the FBI must be approved by the government attorney.

(4) Disclosure cannot be made without a court order for use in noncriminal investigations such as background, applicant, or foreign counterintelligence (unless in the prosecutive stage and the use is authorized as outlined above).

(5) The Rule allows a government attorney to disclose grand jury material to state and local authorities so that they can provide assistance to that attorney in enforcing federal criminal law. The same rules apply as with disclosure to federal officers. A court order is required in order for a government attorney to make a disclosure of grand jury material relative to a state law violation. The Rule contains no specific provision concerning disclosure to foreign officials. The USAO should be consulted with regard to the possibility of such a disclosure pursuant to a treaty, or with a court order upon a showing of particularized need preliminary to a judicial proceeding. (See MAOP, Part II, 9-3.1.3.)

(6) Personnel of the government who are preparing a response to a Freedom of Information Act or Privacy Act request may properly access grand jury material under the Rule because they are considered to be assisting the grand jury attorney by ensuring against any improper disclosure.

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 2 - 15

EFFECTIVE: 10/16/96

2-9.5.1 Matters Occurring Before the Grand Jury

(1) There can be no routine dissemination of matters occurring before the grand jury, unless such dissemination comes within the exceptions enumerated in MIOG, Part II, 2-9.4 and detailed further in MIOG, Part II, 2-9.5 above (see MAOP, Part II, 9-9). There is no uniform legal definition of what constitutes matters occurring before the grand jury except for what is generally referred to as "core" grand jury material. The two other categories of matters occurring before the grand jury are documents created independent of the grand jury but obtained by grand jury subpoena, and data extracted from records obtained by grand jury subpoena.

(2) Core grand jury material includes the following:

- (a) Names of targets and witnesses
- (b) Grand jury testimony
- (c) Grand jury subpoenas
- (d) Documents with references to grand jury testimony (including summaries and analyses)
- (e) Documents that clearly reveal their connection to the grand jury process
- (f) Other material that reveals the strategy, direction, testimony, or other proceedings of a grand jury

(3) The need for secrecy with regard to documents created independently, and later obtained by grand jury subpoena, has been viewed in several ways by federal courts. Because of the lack of uniformity of interpretation by the courts concerning subpoenaed business records and Rule 6(e), all such grand jury subpoenaed documents should be treated as 6(e) material.

(4) Information extracted from business records that were obtained by grand jury subpoena is often used to facilitate investigations. Some of that type of data is, by a statute or case law, subject to the Rule. In other cases, the determination of

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 2 - 16

whether data must be considered subject to the Rule depends on the case law and local practice in the federal districts.

(a) Information extracted from grand jury subpoenaed financial records subject to the Right to Financial Privacy Act of 1978 (Title 12, USC, Section 3420) must be treated as grand jury material "unless such record has been used in the prosecution of a crime for which the grand jury issued an indictment or presentment" (See MIOG, Part II, 23-6.6.5.)

(b) With the approval of the U.S. Attorney's Office (USAO), information from subpoenaed telephone records may be disclosed for use in unrelated federal criminal investigations in those districts where such material is not considered a "matter occurring before a grand jury." If the USAO approves generally of this procedure, such information may be used in unrelated CRIMINAL investigations without authorization from a government attorney in each instance. However, to prevent disclosures (such as in the civil context) which might constitute an abuse of the grand jury's coercive powers, subpoenaed telephone records should be memorialized only in a database or other system of records dedicated exclusively for use in federal criminal investigations. Therefore, any system of records, such as general indices or the Criminal Law Enforcement Application (CLEA), which is accessible by the general FBI population for civil or other noncriminal purposes, is not a suitable repository for business records or information, including telephone data, subpoenaed by a federal grand jury. (See 2-9.7.)

(c) Except for the information described in (b) above, both grand jury subpoenaed documents and the information extracted from them may be memorialized only in databases or other systems of records that are accessible only by those assisting the attorney for the government in the specific criminal investigation to which the documents or information relate.

EFFECTIVE: 07/12/95

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 2 - 17

2-9.5.2 Physical Evidence and Statements

Physical evidence and statements of witnesses may be matters occurring before the grand jury:

(1) Physical evidence provided pursuant to or as a result of grand jury process is a matter occurring before the grand jury whether or not such evidence is presented to the grand jury. Physical evidence provided voluntarily (not pursuant to or in lieu of a grand jury subpoena) is not a grand jury matter irrespective of whether such evidence was previously or is thereafter presented to the grand jury.

(2) Statements of witnesses obtained pursuant to, or as a result of, grand jury process are matters occurring before the grand jury irrespective of whether such witnesses testified before the grand jury or are not required to testify. Voluntary statements of witnesses made outside of the grand jury context (not pursuant to or in lieu of a grand jury subpoena) are not grand jury matters irrespective of whether the witness previously testified or will thereafter testify before the grand jury.

EFFECTIVE: 07/12/95

2-9.6 Documentation of Disclosures of Grand Jury Material

Rule 6 (e) (3) (B) requires that when a federal prosecutor makes a disclosure of grand jury material to government investigators and other persons supporting the grand jury investigation, he/she must promptly provide the district court, before whom was impaneled the grand jury whose material has been so disclosed, with the names of the persons to whom such disclosure has been made, and certify that he/she has advised such persons of their obligation of secrecy under the Rule. In order to document the certification required by the Rule, government attorneys often execute and deliver to the court a form, normally referred to as a "Certification" or "Rule 6(e) letter." A copy of this document should accompany grand jury material in the FBI's custody.

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 2 - 18

EFFECTIVE: 07/12/95

2-9.6.1 Documentation of Internal Disclosures of Grand Jury
Material

Practical considerations often require Agents assisting government attorneys to seek additional assistance in the SAME investigation from others within the FBI. In many districts, support personnel and supervisors of case Agents need not be routinely included in the list provided to the court. In lieu of a Rule 6(e) letter from the U.S. Attorney's Office (USAO) containing an exhaustive list of names of FBI personnel, an FBI record of additional internal disclosures is to be maintained by the case Agent in order to establish accountability. Use of this "internal certification" procedure should be authorized by the appropriate USAO. The internal form should record the date of disclosure as well as the identity and position of the recipient. Such internal disclosures, of course, may be made only in support of the same investigation in which a federal prosecutor has previously issued a Rule 6(e) letter. In addition, the internal record should reflect that all recipients of grand jury materials were advised of the secrecy requirements of Rule 6(e). Whenever practicable, recipients should be listed prior to disclosure.

EFFECTIVE: 07/12/95

2-9.7 Storage of Grand Jury Material (See MIOG, Part II,
23-6.6.5; MAOP, Part II, 9-9.)

As detailed above in MIOG, Part II, 2-9.3 through 2-9.5, the grand jury rule of secrecy requires that the FBI cannot make or allow unauthorized disclosure of grand jury material. Material and records obtained pursuant to the grand jury process frequently are stored in FBI space. Unauthorized disclosures of grand jury material entrusted to FBI personnel should be reported to the appropriate government attorney, who must, in turn, notify the court. In order to protect against unauthorized disclosure, grand jury material must be secured in the following manner:

- (1) It must be marked with the following warning: "GRAND

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 2 - 19

JURY MATERIAL - DISSEMINATE ONLY PURSUANT TO RULE 6(e)."

(2) Access to grand jury material must be limited to authorized persons, i.e., those assisting an attorney for the government in a specific criminal investigation (see MIOG, Part II, 2-9.5), and when not in use must be placed in a subfile which is locked in a container with a combination lock, the combination of which is known only by such authorized persons. The combinations are to be changed annually. Absent chain-of-custody considerations, subfiles need not be kept in an evidence or bulky exhibit room, and may be entrusted to an Information Management Assistant or Evidence Control Technician if their names are placed on the internal certification list. (See MAOP, Part II, 2-4.4.4, 2-4.4.16, and 2-5.1.)

(3) FD-302s and other internal documents that contain grand jury information must be prepared on removable diskettes that are placed in secure storage when not in use. The hard copies must be kept in the grand jury subfile. (See MAOP, Part II, 10-13.8; Correspondence Guide-Field, 2-11.4.10.)

(4) Documents containing grand jury information cannot be placed in manual or automated record systems that can be accessed by persons who are not on the disclosure list. A nondisclosure warning on the documents, or an electronic tagging warning, is not sufficient protection for grand jury information. Such information must be kept only in files to which access is properly restricted. (See MIOG, Part II, 2-9.5.1.)

(5) Transmittal to other field offices of documents containing grand jury material must be by registered mail (or other traceable courier such as Federal Express approved by the Security Programs Manager). Couriers and other personnel employed in these services will be unaware of the contents of the material transmitted due to the wrapping procedures specified below; and therefore, do not require a background investigation for this purpose. The names of persons who transport the material need not be placed on a disclosure list, but the lead office must provide the case Agent in the originating office with a list of the names of personnel in the lead office to whom disclosure is made. Those names are to be added to the internal certification list at the originating office.

(6) Grand jury material which is to be transmitted outside a facility shall be enclosed in opaque inner and outer covers. The inner cover shall be a sealed wrapper or envelope which contains the addresses of the sender and the addressee authorized

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 2 - 20

access to the grand jury material. The inner cover shall be conspicuously marked "Grand Jury Information To Be Opened By Addressee Only." The outer cover shall be sealed, addressed, return addressed and bear no indication that the envelope contains grand jury material. When the size, weight or nature of the grand jury material precludes the use of envelopes or standard packaging, the material used for packaging or covering shall be of sufficient strength and durability to protect the information from unauthorized disclosure or accidental exposure.

(7) When the government attorney, in consultation with the Security Programs Manager (SPM), determines the greater sensitivity of, or threats to, grand jury material necessitate a more secure transmission method, the material may be transmitted by: U.S. Postal Service registered mail, return receipt requested; an express mail service, approved for the transmission of national security information; or hand carried by the cognizant government attorney or his or her designated representative.

(8) Grand jury material containing classified national security information must be handled, processed and stored in accordance with Title 28, Code of Federal Regulations, Part 17. Grand jury material containing other types of sensitive information such as federal tax return information, witness security information and other types of highly sensitive information that have more stringent security requirements shall be stored and protected pursuant to the security regulations governing such information and special security instructions provided by the organization originating the information.

(9) Original documents that were obtained through the grand jury process should be returned to the attorney for the government or, with the government attorney's permission, to the owner if there is no indictment or the prosecution has concluded (see MAOP, Part II, 2-4.4.4 and 2-4.4.16).

EFFECTIVE: 04/29/97

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 2 - 21

2-9.8 Requests for Subpoenas in Fugitive Investigations

The Department of Justice has 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 should not be requested in FBI fugitive investigations. There are, however, limited situations in which courts have recognized that grand jury efforts to locate a fugitive are proper. These situations are described below.

(1) The use of grand jury process to locate a fugitive is proper when the grand jury is interested in hearing the fugitive's testimony. Thus if the grand jury seeks the testimony of the fugitive in the investigation of Federal criminal violations before it, it may subpoena other witnesses and records in an effort to locate the fugitive witness. However, interest in the fugitive's testimony must not be a pretext. The sole motive for inquiring into the fugitive's location must be the potential value of fugitive's testimony. A subpoena for the fugitive witness must be approved by the grand jury before seeking to subpoena witnesses or records to locate the fugitive. Further, it is not proper to seek to obtain grand jury testimony from any witness, including a fugitive, concerning an already returned indictment. Thus it would not be proper to seek to locate a fugitive for the purpose of having fugitive testify about matters for which an indictment has already been returned, unless there are additional unindicted defendants to be discovered or additional criminal acts to be investigated through the testimony of the fugitive. Current policy on "target" witnesses must be observed. Grand jury subpoenas for witnesses and records aimed at locating a fugitive witness who is a target of the grand jury investigation will be approved only where a target subpoena already has been approved by the responsible Assistant Attorney General.

(2) Use of the grand jury to learn the present location of a fugitive is proper when present location is an element of the offense under investigation. On adequate facts, the present location of a fugitive might tend to establish that another person is harboring fugitive, or has committed misprision, or is an accessory after the fact in the present concealment of the fugitive. However, this justification could be viewed as a subterfuge if the suspected harborer or the person potentially guilty of misprision or as an accessory were given immunity in the grand jury in order to compel his/her testimony about the location of the fugitive. In order to ensure the proper use of investigations for harboring, misprision, and accessory after the fact based on acts of concealment, the U.S.

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 2 - 22

Attorneys must consult with the Department of Justice prior to initiating grand jury investigations for these offenses. With regard to escaped Federal prisoner and bond default matters, the present location of a fugitive is not relevant evidence in a grand jury investigation as these offenses address the circumstances of a prior departure from a known location. The fugitive's present location is not a relevant factor as it is in harboring or misprision investigations. Inasmuch as unlawful flight to avoid prosecution cases are, as a rule, not prosecuted and cannot be prosecuted without written authorization from the Attorney General or an Assistant Attorney General, any effort to use the grand jury in the investigation of such cases shall be preceded by consultation with the Department of Justice and by written authorization to prosecute from the Assistant Attorney General in charge of the Criminal Division.

EFFECTIVE: 08/21/87

2-10 INDICTMENT AND INFORMATION (RULE 7)

EFFECTIVE: 08/21/87

2-10.1 Definitions

An indictment is a written accusation against one or more persons of a crime presented to and proffered upon oath or examination by a grand jury legally convoked. An information is an accusation, in the nature of an indictment, filed by a USA supported by oath or affirmation showing probable cause.

EFFECTIVE: 02/11/97

2-10.2 Nature of Crime

Any capital offense must be prosecuted by indictment. A felony is also prosecuted by indictment unless indictment is waived in which case it may be prosecuted by information. Any other offense may be prosecuted by indictment or by information.

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 2 - 23

EFFECTIVE: 08/21/87

2-10.3 Waiver of Indictment

A felony may be prosecuted by information if the defendant, after he/she has been advised of the nature of the charge and of his/her rights, waives in open court prosecution by indictment.

EFFECTIVE: 10/22/84

2-10.4 Advice by Agents

All Agents should advise persons whom they arrest of the provisions of the preceding paragraph (Rule 7b, FED.R.CRIM.P.), after the defendant has indicated his/her guilt and has signed a confession. If a defendant indicates a desire to waive an indictment, that desire should be promptly brought to the attention of the responsible Assistant United States Attorney (AUSA). The Agent should record both the defendant's intent to waive indictment and the fact the AUSA was advised in a memorandum to the investigative file and in the prosecutive status portion of the prosecutive report.

EFFECTIVE: 10/22/84

| 2-10.5 | Deleted |

EFFECTIVE: 10/22/84

2-11 ARREST IN DISTRICT OTHER THAN DISTRICT OF PROSECUTION
(RULE 20; RULE 40)

EFFECTIVE: 10/22/84

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 2 - 24

2-11.1 Place of Arrest

An offender who has committed a Federal violation in one judicial district (district of prosecution) may be located and arrested in a different judicial district (district of asylum).

EFFECTIVE: 10/22/84

2-11.2 Disposition in District Asylum

Under certain conditions, the prosecution may proceed in the district of asylum. (Rule 20).

EFFECTIVE: 10/22/84

2-11.2.1 Where Indictment or Information Pending

A defendant arrested, held, or present in a district other than that in which an indictment or information is pending against him/her may state in writing that he/she wishes to plead guilty or nolo contendere, to waive trial in the district in which the indictment or information is pending, and to consent to disposition of the case in the district in which he/she was arrested, held, or present, subject to the approval of the USA for each district. Upon receipt of the defendant's statement and of written approval of the USAs the clerk of the court in which the indictment or information is pending shall transmit the papers in the proceeding or certified copies thereof to the clerk of the court for the district in which the defendant was arrested, held, or present, and the prosecution shall continue in that district.

EFFECTIVE: 10/22/84

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 2 - 25

2-11.2.2 Where Indictment or Information Not Pending

A defendant arrested, held, or present in a district other than the district in which a complaint is pending against him/her may state in writing that he/she wishes to plead guilty or nolo contendere, to waive trial in the district in which the warrant was issued, and to consent to disposition of the case in the district in which he/she was arrested, held, or present, subject to the approval of the USA for each district. Upon receipt of the defendant's statement and of written approval of the USAs and upon the filing of an information or the return of an indictment, the clerk of the court for district in which the warrant was issued shall transmit the papers in the proceeding or certified copies thereof to the clerk of the court for the district in which the defendant was arrested, held, or present, and the prosecution shall continue in that district. When the defendant is brought before the court to plead to an information filed in the district where the warrant was issued, he/she may at that time waive indictment as provided in Rule 7, and the prosecution may continue based upon the information originally filed.

EFFECTIVE: 10/22/84

2-11.3 Commitment to Another District (Rule 40)

The following procedures apply as to a person arrested in a district other than that in which the prosecution is pending, when the prosecution is to proceed in the district where the prosecution is pending.

(1) Prompt Appearance - A person arrested in a district other than the district of prosecution shall be taken without unnecessary delay before the nearest available federal magistrate.

(2) Preliminary Proceedings - Preliminary proceedings shall be conducted in accordance with Rules 5 and 5.1, FED.R.CRIM.P. The magistrate shall advise the accused of those rights specified in Rule 5 (see paragraph 2-7.3, supra) and of the provisions of Rule 20 (see paragraph 2-11.2, supra).

(3) Accused Held to Answer - The accused shall be held to answer if, from the evidence produced during the preliminary examination, the magistrate determines there is probable cause; or, if no preliminary examination is held, because an indictment has been returned or an information filed (see paragraph 2-7.4, supra) or

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 2 - 26

because the accused elects to have the preliminary examination conducted in the district of prosecution, the accused shall be held to answer upon a finding that he/she is the person named in the information, indictment, or warrant.

(4) Production of Warrant - If the accused is held to answer, he/she shall be held to answer in the district court in which prosecution is pending, upon production of a warrant or a certified copy thereof.

(5) Transmittal of Papers - In connection with the above proceedings, Agents in the district of prosecution should immediately request the United States Marshal to forward certified copies of the necessary papers to the USA in the district where the arrest occurred and should so notify the USA in the district of prosecution. These documents, however, should not be transmitted through Bureau field offices.

(6) Notification - When the papers described in the preceding paragraph have been forwarded, the SAC in the district of prosecution will immediately notify the office covering the district of asylum.

EFFECTIVE: 02/14/97

2-11.3.1 Arrest of Probationer

If a person is arrested for a probation violation in a district other than the district of supervision, he/she shall be taken without unnecessary delay before the nearest available Federal magistrate. The magistrate shall order the probationer held to answer in the district court of the district having probation supervision upon production of certified copies of the probation order, the warrant, and the application for the warrant, and upon a finding that the person arrested is the person named in the warrant.

EFFECTIVE: 02/08/80

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 2 - 27

|| 2-11.3.2 Failure to Appear

Whenever a warrant is issued because of the failure of the person named therein to appear as required pursuant to a subpoena or the terms of release, and the person is arrested in a district other than that in which the warrant was issued, the person arrested shall be taken before the nearest available Federal magistrate without unnecessary delay. Upon production of the warrant or a certified copy thereof, and upon a finding that the person arrested is the person named in the warrant, the magistrate shall hold the person to answer in the district in which the warrant issued.

EFFECTIVE: 02/08/80

2-11.4 Custody of Prisoners in a District of Asylum

EFFECTIVE: 10/25/89

2-11.4.1 Custody by U.S. Marshal

Upon written request of an SA, the U.S. Marshal in the district of asylum is authorized to take custody of a prisoner even though U.S. Marshal has not received the warrant or other court papers from the district of prosecution. U.S. Marshal is likewise authorized to take the accused before the nearest available Federal magistrate for commitment to jail, pending receipt of the necessary papers. The written request to the Marshal is to be signed by the SA, and will include the name of the person arrested, the Federal charge upon which subject is being held, the district in which prosecution is pending, and a statement as to whether or not directions have been given for the forwarding of the warrant to the Marshal having custody of the prisoner.

EFFECTIVE: 10/25/89

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 2 - 28

2-11.4.2 Use of Form FD-351

Form FD-351 may be used to request the Marshal to assume custody of a prisoner. Since the form also provides space for details of the process issued, a copy of the FD-351 may be sent to the USA and the USM for information and necessary action.

EFFECTIVE: 10/25/89

~~2-11.4.3 Marshal Unable to Assume Custody~~

If, due to emergency circumstances, the Marshal is unable to comply with a request to assume custody, the SA should maintain custody and if circumstances dictate, provide the necessary transportation and ensure initial appearance of the prisoner before the magistrate.

EFFECTIVE: 10/25/89

2-12 FUGITIVES LOCATED IN FOREIGN COUNTRIES; EXTRADITION

EFFECTIVE: 10/25/89

2-12.1 Notification to USA

|As soon as it appears likely that a fugitive may be located in a foreign country, you should notify the prosecutor, either the U.S. Attorney or the local prosecutor in unlawful flight cases, that he or she should contact the Office of International Affairs (OIA), Criminal Division, U.S. Department of Justice, promptly. In addition, as soon as such an arrest appears likely, you are to notify the substantive division at FBIHQ, with copy to the Office of Liaison and International Affairs, so that FBIHQ may notify OIA. |

EFFECTIVE: 10/25/89

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 2 - 29

2-12.2 Request for Arrest and Extradition

FBI employees have no authority to request foreign officials to arrest and extradite fugitives who are wanted for violations of the laws of the United States. Requests for the arrest and extradition of such fugitives must be forwarded to the Attorney General by the USA in whose district the prosecution is pending. Departmental regulations require the USAs to furnish the Attorney General with certain information and certified papers for use in effecting the arrest and extradition of foreign fugitives.

EFFECTIVE: 10/25/89

2-12.3 Information Furnished the USA

FBI employees should be prepared to furnish certain information to the USA in order for USA to institute the formal steps necessary to extradite a fugitive from a foreign country. Information which the USA may require includes:

- (1) Evidence that an arrest warrant, if one is outstanding, cannot be executed in the United States because of the flight of the accused to a known locality in a foreign country;
- (2) Evidence for presentation to the surrendering government sufficient to make out a strong case against the accused, such a case as would justify the committal of the accused under the laws of the United States;
- (3) Full name of the accused, together with any assumed names;
- (4) Physical description of the accused;
- (5) Place and address in the foreign country where the accused can be found;
- (6) Date of indictment, if an indictment has been filed;
- (7) Description of the offense or offenses charged;
- (8) Date of the commission of the offense and the place where committed.

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 2 - 30

EFFECTIVE: 10/25/89

2-12.4 Investigations to Locate Fugitives

FBI employees who are conducting investigations as to the whereabouts of fugitives in foreign countries have no authority to employ attorneys or other persons to represent the United States and interested officials and attorneys of a foreign country should be informed to this effect.

EFFECTIVE: 01/31/78

2-12.5 Deportation Proceedings

In deportation proceedings FBI employees should consult the USA in whose district the prosecution is pending and the USA into whose jurisdiction the subject would be deported before making official allegations in the foreign country alleging that the fugitive is an alien to that country, a citizen of the United States, and a person who should be deported. Employees also should consult the nearest American consul stationed in the foreign country and keep him advised of developments in any deportation proceedings.

EFFECTIVE: 01/31/78

2-12.6 Evidence of Fugitive's Citizenship

In all cases in which the apprehension of a fugitive is desired in a foreign country, FBI employees should collect and forward to the appropriate USA evidence of the citizenship of the person whose arrest is desired. Naturalization papers and birth or baptismal certificates duly notarized or certified by the proper authorities constitute evidence of citizenship.

EFFECTIVE: 01/31/78

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 3 - 1

SECTION 3. ADMISSIBILITY OF EVIDENCE IN CRIMINAL CASES

3-1 INTRODUCTION

(1) The Federal Rules of Evidence (FED.R.EVID.), a uniform code of evidence approved by the Supreme Court and enacted into law by Congress, with amendments, govern proceedings in the Federal courts and before U.S. Magistrates in criminal and civil cases. There are 62 Rules set forth under 11 main Articles. State rules of evidence have no application at Federal criminal trials.

(2) Except for a general rule on privileges which applies to all stages of a case, the Rules do not apply to such proceedings as the issuance of arrest warrants, search warrants, or criminal summonses; preliminary examinations; grand jury proceedings; or bail, sentencing, probation, and extradition proceedings.

(3) The Rules do not incorporate principles of the Fourth, Fifth, and Sixth Amendments to the Constitution, and the judicial interpretation thereof, affecting the admissibility of evidence obtained by Special Agents through means such as search and seizure, interrogation of persons in custody, and eyewitness identification procedures.

EFFECTIVE: 08/16/82

3-2 NECESSITY FOR RULES OF EVIDENCE

In our adversary trial system, the issues in a case are decided on facts presented to the jury. When a defendant is charged with a crime, the facts in issue are (1) the elements of the statute as alleged in the indictment and denied by his/her plea of not guilty, and (2) the facts which he/she may allege in defense denied by the prosecution. All matters of law are decided by the judge, e.g., whether an item of evidence is admissible, and all matters of fact are decided by the jury, e.g., what weight and credibility is to be given to the evidence. The judge also decides facts upon which the admissibility of evidence may depend e.g., whether a witness whose former testimony is offered in evidence is "unavailable" under the former-testimony exception to the hearsay rule. The judge is not limited by the rules of evidence in passing upon such preliminary questions. Every element necessary to constitute the crime charged against the defendant must be proved beyond

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 3 - 2

a reasonable doubt.

EFFECTIVE: 08/16/82

3-3 RELEVANCY

(1) The fundamental principle of the law of evidence is that of relevancy. "Relevant evidence" means evidence having any tendency to make the existence of any fact that is of consequence to the determination of the action more probable or less probable than it would be without the evidence.

(2) All relevant evidence is admissible except as otherwise provided by: (a) the Constitution, e.g., the search and seizure exclusionary rule based on the Fourth Amendment; (b) Act of Congress, e.g., Title 47, USC, Section 605 dealing with interception of wire or radio communications; (c) other rules prescribed by the Supreme Court, e.g., the "Mallory Rule" excluding statements elicited during detention in violation of Rule 5(a) of the Federal Rules of Criminal Procedure (FED.R.CRIM.P.); and (d) the FED.R.EVID.

(3) The test to be applied in determining the relevancy of an item of evidence is its connection by reason of logic, experience, or science with the facts to be proved in the case. Evidence showing the defendant's motive, preparation, opportunity to commit a particular crime, or his/her threats to the victim of the crime, or attempts to destroy incriminating evidence is relevant. A fact not immediately relevant to the facts in issue may become so, e.g., a prior inconsistent statement affecting the credibility of a witness.

(4) The principle of relevancy emphasizes the need during investigation of a clear understanding of the elements of the crime involved. Agents should develop all evidence which can reasonably be obtained to prove such elements. This is necessary since the FBI has the responsibility of furnishing the USA or the Department of Justice all evidence bearing on any contemplated prosecution. The defense that may be interposed by the defendant is generally not known in advance.

(5) Although relevant, evidence may be excluded if its probative value is substantially outweighed by the danger of unfair prejudice, confusion of the issues, or misleading the jury, or by considerations of undue delay, waste of time, or needless presentation of cumulative evidence.

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 3 - 3

(6) Evidence of a person's character or a trait of his/her character is not admissible for the purpose of proving that he/she acted in conformity therewith on a particular occasion, except:

(a) Evidence of a pertinent trait of his/her character offered by an accused, or by the prosecution to rebut the same.

(b) Evidence of a pertinent trait of character of the victim of the crime offered by an accused, or by the prosecution to rebut the same, or evidence of a character trait of peacefulness of the victim offered by the prosecution in a homicide case to rebut evidence that the victim was the first aggressor.

(c) Evidence of the character of a witness for truthfulness or untruthfulness to attack or support his/her credibility.

(7) Evidence of other crimes is not admissible to prove the character of a person in order to show that he/she acted in conformity therewith. It may, however, be admissible for other purposes, such as proof of motive, opportunity, intent, preparation, plan, knowledge, identity, or absence of mistake or accident.

(8) In all cases in which evidence of character or a trait of character of a person is admissible, proof may be made by testimony as to reputation or by testimony in the form of an opinion. On cross-examination, inquiry is allowable into relevant specific instances of conduct. In cases in which character or a trait of character of a person is an essential element of a charge or defense, proof may also be made of specific instances of his/her conduct.

(9) Evidence of the habit of a person or the routine practice of an organization, whether corroborated or not and regardless of the presence of eyewitnesses, is relevant to prove that the conduct of the person or organization on a particular occasion was in conformity with the habit or routine practice.

EFFECTIVE: 08/16/82

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 3 - 4

3-4 GENERAL TYPES OF EVIDENCE

Evidence may be classified in several ways; e.g., according to its form, or according to the way it tends to prove a fact.

(1) According to its form, evidence is testimonial, documentary, or real. Testimonial evidence, the most common type, consists of the oral assertions of witnesses. Documentary evidence consists of the words, figures, or other symbols conveying information set down on a writing, recording, or photograph. Real evidence consists of tangible things involved in a case, such as physical objects or substances.

(2) According to the way it tends to prove a fact, evidence is either direct or circumstantial. It is direct when it immediately establishes the very fact to be proved. It is circumstantial when it establishes other facts so relevant to the fact to be proved that they support an inference of its existence. Thus, if a defendant is charged with murder on a Government reservation and a witness testifies that he/she saw the defendant stab the victim, the evidence is direct. If a witness testifies that he/she saw the defendant running from the scene of the stabbing, or that he/she had seen the defendant purchase a knife of the kind used in the killing the day before the crime, the evidence is circumstantial. In an ITSMV case, the testimony of the owner of an automobile that he/she saw the defendant steal his/her car is direct evidence as it establishes the theft of the car which is an element of the statute. If a used car dealer testifies that the defendant tried to sell this car to him/her at a low price, the evidence is circumstantial.

(3) Direct and circumstantial evidence are equally admissible. Circumstantial evidence may present problems of relevancy where direct evidence does not, but circumstantial evidence is not inferior to direct evidence and may be more persuasive than it.

EFFECTIVE: 08/16/82

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 3 - 5

3-5 JUDICIAL NOTICE

(1) Judicial notice is the process by which a court accepts a relevant fact as true without evidence thereof. A judicially noticed fact must be a fact which is not subject to reasonable dispute in that it is either (a) generally known within the territorial jurisdiction of the trial court or (b) capable of accurate and ready determination by resort to sources whose accuracy cannot reasonably be questioned. An example of judicially noticed fact would be: the time of sunset on a certain date as determined by the records of the U.S. Department of Commerce National Weather Service. In a criminal case, the court instructs the jury that it may, but is not required to, accept as conclusive any facts judicially noticed.

(2) In investigations in which it appears pertinent to establish facts as part of the case which may fall within this rule, Agents should not assume that such facts need not be proven. Where facts may fall within this rule, consideration should be given to discussing with the USA the necessity for investigation. As to the taking of judicial notice of matters of foreign law, see Rule 26.1 of the FED.R.CRIM.P.

EFFECTIVE: 08/16/82

3-6 PRESUMPTIONS

(1) A presumption is a standardized inference which permits, but does not require, the jury to accept the existence of a presumed fact, e.g., once a conspiracy is shown to exist, it is presumed to continue until an affirmative act of termination. A presumption is not evidence but a way of dealing with evidence. It acts to shift the burden of producing evidence to the contrary to the party against whom it operates. Congress has created various presumptions by statute to lessen the burden of proof upon the prosecution. For example, the Selective Service Act provides that it is unlawful to possess a draft card not lawfully issued to the holder with intent to use it for the purpose of false identification. It further provides that the possession of such a card is deemed sufficient evidence to establish such an intent unless the defendant explains his possession to the satisfaction of the jury. Because of its relationship to the burden of proof, the impact of a presumption is potentially great. Generally, a statute creating a presumption is constitutional if there is a natural and rational evidentiary relation, in accordance with the experience of mankind, between the fact proved and the one presumed.

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 3 - 6

EFFECTIVE: 08/16/82

3-7 WITNESSES

EFFECTIVE: 06/15/81

3-7.1 Competency

(1) In General - A witness is said to be competent when|he/she|is qualified to testify under the law. The Rules contain a broad general provision that every person is competent to be a witness except as otherwise provided in the code. The only persons so specifically designated as not being competent are (a) the judge presiding at the trial and (b) a member of the trial jury. By reason of this broad general provision, the specific grounds of immaturity, mental incapacity, religious belief, and conviction of crime on which persons were disqualified as witnesses at common law are abolished. The common law incompetency of the parties in a case, their spouses, and other persons having an interest in the outcome of the trial are likewise abolished.

(2) Requirement of Personal Knowledge - A witness may not testify unless evidence is introduced sufficient to support a finding that|he/she|has personal, i.e., firsthand knowledge of the matter. Although a lay witness must have had an opportunity to observe, and must have actually observed a matter, a witness testifying as an expert is allowed to express opinions on facts made known to|him/her|at or before a hearing of which|he/she|does not have personal knowledge. The cross-examination of a witness is limited to the subject matter of|his/her|direct examination and matters affecting|his/her|credibility. Leading questions are not to be used on the direct examination of a witness except to develop|his/her|testimony but ordinarily are permitted on cross-examination.

(3) |The common law rule that one spouse is disqualified from testifying against the other has been abolished. Today, a husband or wife may testify for or against his or her spouse, so long as the testifying party chooses to so testify. The abolition of this "adverse spousal testimony" privilege leaves undisturbed the right of a husband or wife to prevent the testimonial disclosure of confidential communications made in the privacy of the marital relationship (the

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 3 - 7

| husband-wife privilege). See Section 3-8.3, *infra*.|

(4) Handwriting - The admitted or proved handwriting of any person is admissible, for purposes of comparison, to determine genuineness of other handwriting attributed to such person by statute 28 U.S.C. 1731.

EFFECTIVE: 06/15/81

3-7.2 Impeachment of Witnesses

(1) The credibility of a witness may be attacked by any party, including the party calling him/her. Thus, the traditional rule against impeaching one's own witness is abandoned under the Rules.

(2) The credibility of a witness may be attacked or supported by evidence in the form of reputation or opinion, but subject to limitations. The evidence may refer only to character for truthfulness or untruthfulness, and evidence of truthful character is admissible only after the character of the witness for truthfulness has been attacked by opinion or reputation, evidence or otherwise.

(3) Specific instances of the conduct of a witness for the purpose of attacking or supporting his/her credibility, other than conviction of crime, may not be proved by extrinsic evidence. They may, however, in the discretion of the court, if probative of truthfulness or untruthfulness, be inquired into on cross-examination of the witness concerning his/her character for truthfulness or untruthfulness, or concerning the character for truthfulness or untruthfulness of another witness as to which character the witness being cross-examined has testified.

(4) The giving of testimony, whether by an accused or by any other witness, does not operate as a waiver of his/her privilege against self-incrimination when examined with respect to matters which relate only to credibility.

(5) For the purpose of attacking the credibility of a witness, evidence that he/she has been convicted of a crime is admissible, within limitations, if elicited from him/her or established by public record during cross-examination, but only if the crime was punishable as a felony and the court determines that the probative value of admitting the evidence outweighs its prejudicial effect to the defendant, or if the crime involved dishonesty or false statement

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 3 - 8

regardless of the punishment.

EFFECTIVE: 06/15/81

3-7.2.1 Duty to Disclose Potential Impeachment Material Regarding
Government Employee/Witnesses

(1) FBI Agents and other investigative personnel are obligated to inform prosecutors with whom they work of potential impeachment information prior to providing a sworn statement or testimony in any criminal case.

(2) The failure of the prosecution to disclose evidence favorable to an accused upon request violates due process where the evidence is material either to guilt or to punishment, irrespective of the good faith or bad faith of the prosecution. *BRADY v. MARYLAND*, 373 U.S. 83 (1963). Impeachment evidence, which is any evidence that may impact on the credibility or reliability of a witness, can also be *BRADY* material. *GIGLIO v. UNITED STATES*, 405 U.S. 83 (1972). Moreover, the failure of the defendant to request favorable evidence does not leave the government free of obligation. *UNITED STATES v. AGURS*, 427 U.S. 97 (1976). Regardless of the request, favorable evidence is material, and constitutional error results from its suppression by the government, "if there is a reasonable probability that, had the evidence been disclosed to the defense, the result of the proceeding would have been different." *UNITED STATES v. BAGLEY*, 473 U.S. 667 (1985). Additionally, if the failure to disclose the evidence "undermines confidence" in the verdict, it must be disclosed. *KYLES v. WHITLEY*, 115 S.Ct. 1555, 1556 (1995). The prosecutor has a duty to learn of any favorable evidence known to others acting on the government's behalf, including the police. *Id.* at 1567.

(3) When a federal prosecutor identifies an agency employee as a potential witness or affiant in a specific criminal case or investigation the employee must disclose potential impeachment material known to them. This duty includes those instances when there is no specific request from the prosecutor.

(4) Generally, the term "potential impeachment material" includes, but is not limited to, the following:

(a) specific instances of conduct, or misconduct, that may be used to question a witness's credibility or character for truthfulness; (b) evidence in the form of opinion as to reputation

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 3 - 9

about a witness's character for truthfulness; (c) prior inconsistent statements; and (d) information that may be used to suggest that a witness is biased.

(5) | Because the duty to learn of potential impeachment material lies with the prosecution, a prosecutor may also request that the employee-witness' agency review the employee's personnel files for potential impeachment information. When an individual prosecutor determines that it is necessary to request potential impeachment information from the employee-witness' agency, the prosecutor should notify the designated requesting official, who in turn is authorized to request potential impeachment information from the employee-witness' agency official, the CDC.

(a) Each U.S. Attorney's Office is required to designate a requesting official to serve as point of contact to receive potential impeachment information from agencies. Also the requesting official is required to inform the agency official (CDC) of relevant case law and court practices and rulings that govern the definition and disclosure of impeachment information in that district.

(b) The agency official within the FBI is the CDC for the division in which the investigation or case is pending. In certain instances outlined below, the Investigative Law Unit (ILU) of the Office of the General Counsel (OGC) will be responsible for conducting the review of some personnel files in lieu of the CDC. However, the CDC will still be responsible for disclosing the information located by OGC to the requesting official/prosecutor.

(6) | FBI Plan for Review and Disclosure

(a) All requests from a requesting official/prosecutor for potential impeachment information should be in writing, and should be directed to the CDC. Upon receiving a request from the requesting official/prosecutor, the CDC should ensure that all relevant personnel (67 classification) and/or administrative files (263 classification and 66 classification) for the employee-witness are identified and reviewed to determine whether the files contain any potential impeachment information.

(b) All FBI employee-witness' personnel and related administrative files maintained in the field division where the employee-witness is located should be reviewed. If the CDC is aware of additional related files at FBIHQ or elsewhere, not maintained by the field division, but which could contain potential impeachment

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 3 - 10

information, the CDC should ensure that those files are also reviewed.

(c) When the employee-witness is located in a division other than where the investigation or case is pending, the CDC should request that the CDC in that division conduct a review of the employee-witness personnel files.

(d) FBIHQ review of some employee-witness personnel files will be required where the employee was previously assigned to FBIHQ. The field division personnel files in that instance may only begin at the time the employee was assigned to that division; therefore, the bulk of that employee's personnel file may be maintained at FBIHQ. Thus, where the employee-witness is located at FBIHQ or has previously been assigned to FBIHQ, the CDC should request that the employee-witness' personnel files be reviewed by FBIHQ. The ILU, OGC, will be responsible for conducting FBIHQ reviews.

(7) When the CDC makes a request for FBIHQ to conduct a review of an employee-witness' personnel file, or requests a review by a CDC in another division, the following information should be included in the written request:

(a) The full case name and/or docket number;

(b) The name, address, telephone and facsimile number of the requesting official;

(c) The official Bureau name and Social Security Account Number for each employee whose file is to be reviewed;

(d) The results (summary or documents with appropriate redactions) of the file review conducted by the CDC, if any;

(e) Any additional or specific requests provided by the requesting official concerning the review;

(f) Copies of any relevant court rules or orders governing the request; and

(g) Any additional facts or circumstances that might be relevant to the requested review.

(8) After the review has been conducted, the CDC should

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 3 - 11

notify the requesting official, in writing, that the review has been conducted and should advise the requesting official of the following:

(a) Substantiated allegations - any finding of misconduct that reflects upon the truthfulness or possible bias of the employee, including a finding of lack of candor during an administrative inquiry;

(b) Criminal charges - any past or pending criminal charge brought against the employee;

(c) Pending investigations or allegations - any credible allegation of misconduct that reflects upon the truthfulness or possible bias of the employee that is the subject of a pending investigation; and

(d) Unsubstantiated allegations - allegations that are not credible, and allegations that have resulted in exoneration.

Allegations of misconduct that are not credible, cannot be proved, or result in the exoneration of an employee-witness are rarely considered to be impeaching material. However, the duty to learn of potential impeachment material lies with the prosecutor, and the prosecutor's ultimate burden is to ensure that all BRADY/GIGLIO material has been provided to the defendant. Therefore, the policy requires that such allegations that reflect upon the truthfulness or bias of the employee, to the extent maintained by the FBI, be provided to the prosecutor under the following circumstances:

1. When it is required by a court decision in the district where the investigation or case is being pursued;

2. When, on or after the effective date of this policy:

a. the allegation was made by a federal prosecutor, magistrate judge, or judge; or

b. the allegation received publicity;

3. When the requesting official and the agency official agree that such disclosure is appropriate, based upon exceptional circumstances involving the nature of the case or the role of the agency witness; or

4. When disclosure is otherwise deemed

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 3 - 12

| appropriate by the agency.

| NOTE: The CDC is required to advise the prosecuting office, to the extent determined, whether any of the aforementioned allegations were found to be unsubstantiated, not credible, or resulted in the employee's exoneration. When there is uncertainty as to whether information is of potential impeachment value, the CDC should consult with the OGC. However, in general, such uncertainty should be resolved in favor of disclosure to the requesting official. |

| (9) | A copy of any written allegation relating to truthfulness or possible bias that is made against an FBI employee by a federal prosecutor or judge, or that receives publicity, should be retained in order to comply with this policy. If there is no written allegation or information, the CDC should make a notation of the information that comes to his/her attention in the appropriate personnel or administrative file. |

| (10) | In order to ensure that special care is taken to protect the confidentiality of unsubstantiated allegations and the privacy interests and reputations of agency employee-witnesses, the CDC should request that all information and documentation that was not disclosed to the defense be expeditiously returned to the CDC. Prosecuting offices, however, are permitted to keep motions, responses, legal memoranda, court orders, and internal office memoranda or correspondence, in the relevant criminal case file. |

| (11) | In order to ensure that all disciplinary and related information is reviewed, each CDC should develop and implement a plan whereby the CDC is notified in a timely manner of new or pending disciplinary matters concerning employee-witnesses. The CDC in the division where the investigation or case is pending is also responsible for ascertaining and notifying the requesting official of any additional information that becomes available until a prosecution is concluded. |

| (12) Supervisory personnel should familiarize themselves with any potential impeachment material in an employee's personnel file and consider that information when making investigative assignments that may result in that employee becoming an affiant or testifying in court. |

| (13) When information or documentation is provided to a prosecutor, the prosecutor should share that information only on a need-to-know basis with co-counsel or other appropriate supervisory personnel within the prosecutor's office. Before the information or

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 3 - 13

documentation is shared or provided to either a court or defense counsel, the prosecuting attorney should be requested to promptly advise the CDC who provided the information of the prosecutor's intent to disclose the information. Additionally, the CDC or other agency officials communicating with the Assistant United States Attorney should make the employee aware of the decision to disclose information from his or her personnel file.

(14) Before disclosing an allegation that has not resulted in (a) a FINDING of misconduct reflecting upon the truthfulness or possible bias of the employee, or (b) a criminal charge against the employee, the prosecutor should be requested to seek an EX PARTE, IN CAMERA review and decision by the court regarding whether such information must be disclosed to defense counsel. Whenever such information is released to the defense, the prosecuting attorney should, unless clearly inappropriate, seek a protective order from the court limiting the use and further dissemination of the information and requiring the return of government documents reflecting the information.

(15) | Deleted |

(16) | Deleted |

EFFECTIVE: 02/21/97

3-7.3 Refreshing Memory of Witnesses

(1) Generally, the memory of a witness may be refreshed before trial or while he/she is on the stand at trial. If a witness uses a writing to refresh his/her memory for the purpose of testifying either while testifying or before testifying, if the court in its discretion determines it is necessary in the interests of justice, an adverse party is entitled to have the writing produced at the hearing, to inspect it, to cross-examine the witness thereon, and to introduce in evidence those portions which relate to the testimony of the witness. If it is claimed that the writing contains matters not related to the subject matter of the testimony, the court examines the writing in camera, excises any portions not so related, and orders delivery of the remainder to the party entitled thereto. If the prosecution elects not to comply, the court strikes the testimony or declares a mistrial. Thus, the production of writings used by a witness while testifying is required; but it is discretionary with the court as to whether writings used by a witness to

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 3 - 14

refresh his/her memory before trial will be produced.

(2) This rule is expressly made subject to Rule 17(h),
FED.R.CRIM.P., and Rule 26.2, FED.R.CRIM.P., and items falling within its
purview are producible only as provided by its terms. Rule 26.2,
FED.R.CRIM.P., applies to statements relevant to the testimony of all
witnesses in criminal cases and does not require that the statement be
consulted for purposes of refreshment before or while testifying; whereas
this evidentiary rule is not limited to statements relevant to witness
testimony, applies to all cases, and requires that the writing be
consulted for purposes of refreshment while or before testifying.

EFFECTIVE: 08/16/82

3-7.4 Prior Statements of Witnesses

(1) Generally, if a witness testifies to material facts at
a trial and has previously made a statement concerning such facts before
trial, he/she may be examined concerning them. The prior statement is
admissible to impeach his/her credibility when it is inconsistent with
his/her testimony, or to support his/her credibility, if attacked, when
the statement is consistent with his/her testimony. An attack upon the
credibility of a witness by proof that he/she has previously made
statements inconsistent with his/her present testimony is the most
frequently employed method of attack.

(2) In examining a witness concerning a prior statement made
by him/her, whether written or not, the statement need not be shown nor
its contents disclosed to him/her at that time, but on request the same
is shown or disclosed to opposing counsel.

(3) Extrinsic evidence of a prior inconsistent statement by
a witness is not admissible unless the witness is afforded an opportunity
to explain or deny it and the opposite party is afforded an opportunity
to interrogate him/her thereon, or the interests of justice otherwise
require; in other words, an impeaching statement must first be shown to
the witness before it can be proved by extrinsic evidence.

EFFECTIVE: 08/16/82

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 3 - 15

3-7.5 Court Witnesses and Exclusion of Witnesses

(1) The court may call witnesses and interrogate them, and all parties may cross-examine them.

(2) At the request of a party the court orders witnesses excluded so that they cannot hear the testimony of other witnesses. The Rules, however, do not authorize exclusion of a party who is a natural person, or a person whose presence is shown by a party to be essential to the presentation of his/her case, or an officer or employee of a party which is not a natural person designated as its representative by its attorney. It has been held that an officer who has been in charge of an investigation may be allowed to remain in court despite the fact that he/she will be a witness.

EFFECTIVE: 08/21/87

3-8 PRIVILEGES

EFFECTIVE: 08/21/87

3-8.1 In General

(1) Under the general rule on privileges, the privilege of a witness is governed by the principles of the common law as they may be interpreted by Federal courts in the light of reason and experience, except as otherwise required by the Constitution, Act of Congress, or Supreme Court rules.

(2) At common law certain persons by virtue of their relationship with a defendant cannot testify to confidential communications, either oral or written, obtained as a result of this relationship. The courts recognize the necessity for a free exchange of information between such persons and protect the relationship through adherence to the privilege rule. Privilege under this rule means that a witness cannot be forced to disclose any communication based on the confidential relationship. A privilege ordinarily can be waived by the person holding it. The following types of witnesses should be considered with respect to this rule.

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 3 - 16

EFFECTIVE: 08/21/87

3-8.2 Attorney and Client

Communications either oral or written between an attorney and client in the course of their professional relationship are considered privileged, the privilege belonging to the client. The privilege attaches only to communications needed to obtain legal services. The rule is designed to secure the client's freedom of mind in committing his/her affairs to the attorney's knowledge. The client is entitled to have the attorney honor the privilege even though the relationship has ceased. Communications between an attorney and client about a crime or fraud to be committed in the future are not privileged. The privilege under this rule may be waived by the client alone although the lawyer can claim the privilege on behalf of his/her client. A client's identity or occupation will not ordinarily qualify as confidential information, but the privilege has been held to protect a client's address from disclosure.

EFFECTIVE: 08/21/87

3-8.3 Husband and Wife

(1) Confidential communications, oral or written, between husband and wife are considered privileged and cannot be disclosed through the testimony of either spouse in the absence of a waiver. For example, a wife cannot be permitted to testify as to her husband's perjury confessed to her by the husband in the confidence of their marital relationship. All communications in private between spouses are presumed to be confidential. Either spouse is precluded from disclosing such communications, the basis for the privilege being the protection of marital confidence regarded as essential to this relationship. The one possible exception to the rule is communications between husband and wife relating to offenses against her, a wife being competent to testify against her husband in such cases. The privilege generally extends only to confidential communications, i.e., it does not extend to acts which would not have been performed but for the marital relationship.

(2) The legal relationship of husband and wife must exist at the time of the communication and, thus, a communication made before marriage, or after the marriage has terminated, is not privileged. The privilege of communications occurring during the marriage is not affected

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 3 - 17

by the death or divorce of either spouse. Communications by either spouse in the presence of third persons not intended to be confidential are not considered privileged.

EFFECTIVE: 08/21/87

3-8.4 Informants

The identity of an informant is privileged. The Government holds the privilege and, generally, is not required to disclose his/her identity. The privilege is founded upon the public interest in effective law enforcement. Citizens are to be encouraged to inform the Government of crime. The privilege, however, is not absolute and the public interest is balanced against the defendant's right to prepare his/her defense and to a fair trial. For example, disclosure may be required where the informant was a participant in the crime charged, or where the defendant's participation was the result of entrapment by the informant. In situations where the court requires disclosure and Government withholds, the court will dismiss the case. The privilege may arise not only at trial but at a proceeding to determine probable cause, e.g., in arrest and search situations. Where probable cause is established by evidence apart from the informant's information, the court may or may not require disclosure.

EFFECTIVE: 08/21/87

3-8.5 FBI Files and Records

The files and records of the FBI and official information in the possession of employees are considered privileged under Departmental Order 919-80, dated 12/18/80, which prohibits the production of such records, or the disclosure of information therefrom, or other official information in possession of employees under subpoena duces tecum, order, or otherwise without approval of an appropriate Department official or the Attorney General. This regulation is based on statutory authority contained in Title 5, USC, Section 301. (D. O. 919-80 set forth in MIOG, Part II, Section 6.)

EFFECTIVE: 08/21/87

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 3 - 18

3-8.6 Other Privileges

Most state courts by statute recognize a privilege as to communications between physician and patient, with exceptions, and also as to communications between a member of the clergy and penitent. These privileges did not exist at common law and have not been created by Federal statute. However, Federal courts have recognized a privilege for a confession-like statement to a member of the clergy without the assistance of any statute. Several states, by statute, grant a privilege to journalists to withhold their sources of information and also to accountants, but these privileges have not been recognized by Federal statute. The First Amendment to the Constitution does not accord a newsperson a privilege against appearing before a grand jury and answering questions as to either the identity of his/her news source or information he/she received in confidence.

EFFECTIVE: 08/21/87

3-9 OPINIONS AND EXPERT TESTIMONY

(1) If a person is testifying as a lay witness and not as an expert witness, his/her testimony in the form of opinions or inferences is limited to those opinions or inferences which are (a) rationally based on his/her perception and (b) helpful to a clear understanding of his/her testimony or the determination of a fact in issue. Thus, an ordinary witness may express an opinion provided it is based upon his/her firsthand knowledge and is helpful in resolving issues. The law prefers testimony to concrete rather than abstract facts, and a detailed account to a broad assertion. Examples of opinions which are generally allowed are: That a person appeared nervous, intoxicated, weak, or sick; as to what a person appeared to be doing; as to a condition, e.g., that a floor was slippery; handwriting; the speed of a moving vehicle; and the value of a person's own property.

(2) If scientific, technical or other specialized knowledge will assist the jury to understand the evidence or to determine a fact in issue, a witness qualified as an expert by knowledge, skill, experience, training, or education may testify thereto in the form of an opinion or otherwise.

(3) The facts or data upon which an expert bases his/her opinion or inference may be those perceived by or made known to him/her at or before the hearing. If of a type reasonably relied upon by experts in the particular field in forming opinions or inferences upon the

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 3 - 19

subject, the facts or data need not be admissible in evidence.

(4) An expert witness may testify in terms of opinion or inference and give his/her reasons therefor without prior disclosure of the underlying facts or data, unless the court requires otherwise. The expert may in any event be required to disclose the underlying facts or data on cross-examination.

(5) The court may on its own motion or on the motion of any party enter an order to show cause why expert witnesses should not be appointed by the court and may request the parties to submit nominations. An expert witness is not appointed by the court unless he/she consents to act. He/She is subject to cross-examination by each party, including the party calling him/her as a witness.

EFFECTIVE: 08/21/87

3-10 HEARSAY

EFFECTIVE: 08/16/82

3-10.1 In General

(1) Hearsay is simply defined as evidence based on something a witness has heard someone else say rather than on what he/she has himself/herself seen or experienced. Thus, if a witness testifies that he/she heard another person say "The defendant shot the victim," or if he/she produces a letter so stating sent to him/her by that other person, such evidence is hearsay. Technically, hearsay is defined as a statement, other than one made by the declarant while testifying at a trial or hearing, offered in evidence to prove the truth of the matter asserted. A "statement" is defined as an oral or written assertion, or nonverbal conduct of a person if it is intended by him/her as an assertion. A "declarant" is defined as a person who makes a "statement." A declarant who makes an out-of-court statement is a witness and, thus, must have had firsthand knowledge.

(2) The testimony of a witness is evaluated in terms of his/her perception, memory, narration, and sincerity. Ideally, a witness is required to testify orally to the relevant facts of which he/she has personal knowledge, under oath, confronting the defendant, in the presence of the jury with his/her demeanor under its

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 3 - 20

scrutiny, and subject to cross-examination by the adversary party. The general principle, therefore, is that hearsay evidence is not admissible. In this regard the Rules provide that hearsay is not admissible except as provided by the FED.R.EVID. or by other rules prescribed by the Supreme Court pursuant to statutory authority, e.g., Rule 4(a) of the FED.R.CRIM.P. on affidavits to show grounds for issuing warrants, or by Act of Congress.

(3) Despite the desirability of giving testimony under ideal conditions, the law does not demand that they be attained in all situations. Thus, while it excludes hearsay generally as it is admittedly not equal in quality to testimony of the declarant on the stand, rather than lose it completely it allows hearsay in under certain circumstances believed to give it some particular assurance of credibility diminishing the risk of untrustworthiness and in the interests of justice.

(4) The Rules provide for two distinct classes of exceptions to the hearsay rule.

(a) The first class deals with situations where the availability of the declarant is regarded as immaterial - the hearsay statements in the 23 individual exceptions within this class being deemed to possess circumstantial guarantees of trustworthiness sufficient to justify nonproduction of the declarant in person even though he/she may be available.

(b) The second class, which consists of 4 specific exceptions deals with situations where the unavailability of the declarant is made a condition to the admission of the hearsay statement. Unavailability includes situations in which the declarant is unable to be present or to testify because of death, physical or mental illness; when he/she persists in refusing to testify despite a court order to do so; when he/she is exempted on the ground of privilege; when he/she testifies to a lack of memory; or when he/she is absent and the proponent of his/her statement is unable to procure his/her attendance by process or other reasonable means, or in the case of statements under belief of impending death, statements against interest, and statements of personal or family history he/she is unable to procure his/her attendance or testimony, e.g., through deposition, by such means. A declarant is not unavailable as a witness if his/her exemption, refusal, claim of lack of memory, inability or absence is due to the procurement or wrongdoing of the proponent of his/her statement for the purpose of preventing the witness from attending or testifying.

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 3 - 21

EFFECTIVE: 08/16/82

3-10.2 Hearsay Exceptions - Availability of Declarant Immaterial

EFFECTIVE: 08/16/82

3-10.2.1 Present Sense Impression

A statement describing or explaining an event or condition made while the declarant was perceiving the event or condition, or immediately thereafter.

EFFECTIVE: 08/16/82

3-10.2.2 Excited Utterance

A statement relating to a startling event or condition made while the declarant was under the stress of excitement caused by the event or condition.

EFFECTIVE: 08/16/82

3-10.2.3 Then Existing Mental, Emotional, or Physical Condition

A statement of the declarant's then existing state of mind, emotion, sensation, or physical condition (such as intent, plan, motive, design, mental feeling, pain and bodily health), but not including a statement of memory or belief to prove the fact remembered or believed.

EFFECTIVE: 03/08/79

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 3 - 22

3-10.2.4 Recorded Recollection

A memorandum or record concerning a matter about which a witness once had knowledge but now has insufficient recollection to enable witness to testify fully and accurately, shown to have been made or adopted by the witness when the matter was fresh in witness' memory and to reflect that knowledge correctly. If admitted, the memorandum or record may be read into evidence but may not itself be received as an exhibit unless offered by an adverse party.

EFFECTIVE: 03/08/79

3-10.2.5 Records of Regularly Conducted Activity

A memorandum, report, record, or data compilation, in any form, of acts, events, conditions, or diagnosis, made at or near the time by, or from information transmitted by, a person with knowledge, if kept in the course of a regularly conducted business activity, and if it was the regular practice of that business activity to make the memorandum, report, record, or data compilation, all as shown by the testimony of the custodian or other qualified witness, unless the source of information or the method or circumstances of preparation indicate lack of trustworthiness. The term "business" as used in this paragraph includes business, institution, association, profession, occupation, and calling of every kind, whether or not conducted for profit. (28 U.S.C. 1732) Absence of entry in such records is admissible to prove the nonoccurrence or nonexistence of such matters.

EFFECTIVE: 03/08/79

3-10.2.6 Financial Records of a Customer

Customers' records in possession of a financial institution (broadly defined) may be obtained by the FBI only in accordance with the provisions of the Right to Financial Privacy Act of 1978 or through the issuance of a Federal Grand Jury subpoena. (See MIOG, Part II, 23-6)

EFFECTIVE: 03/08/79

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 3 - 23

||3-10.2.7| Public Records and Reports

Records, reports, statements, or data compilations, in any form, of public offices or agencies, Federal or non-Federal, setting forth (a) the activities of the office or agency, or (b) matters observed pursuant to duty imposed by law as to which matters there was a duty to report, excluding, however, in criminal cases matters observed by police officers and other law enforcement personnel, or (c) in civil actions and proceedings and against the Government in criminal cases, factual findings, i.e., nonevaluative and nonopinion reports, resulting from an investigation made pursuant to authority granted by law, unless the sources of information or other circumstances indicate lack of trustworthiness. Records of vital statistics in a public office are admissible. The absence of a public record is also admissible.

EFFECTIVE: 03/08/79

||3-10.2.8| Judgment of Previous Conviction

Evidence of a final judgment, entered after a trial or upon a plea of guilty (but not upon a plea of nolo contendere), adjudging a person guilty of a crime punishable by death or imprisonment in excess of one year, to prove any fact essential to sustain the judgment, but not including, when offered by the Government in a criminal prosecution for purposes other than impeachment, judgments against persons other than the accused.

EFFECTIVE: 03/08/79

||3-10.2.9| Reputation as to Character

Reputation of a person's character among his/her associates or in the community.

EFFECTIVE: 03/08/79

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 3 - 24

||3-10.2.10| Miscellaneous

Records of religious organizations; marriage, baptismal, and similar certificates; family records; records of documents affecting an interest in property; ancient documents; market reports; learned treatises; reputation concerning personal or family history; and others, are likewise specifically made admissible under this class of exceptions.

EFFECTIVE: 03/08/79

3-10.3 Hearsay Exceptions - Declarant Unavailable

EFFECTIVE: 03/08/79

3-10.3.1 Former Testimony

Testimony given as a witness at another hearing of the same or a different proceeding, or in a deposition taken in compliance with law in the course of the same or another proceeding, if the party against whom the testimony is now offered, or, in a civil action or proceeding, a predecessor in interest, had an opportunity and similar motive to develop the testimony by direct, cross, or redirect examination.

EFFECTIVE: 03/08/79

3-10.3.2 Statement Under Belief of Impending Death

In a prosecution for homicide or in a civil action or proceeding, a statement made by a declarant while believing that|his/her|death was imminent, concerning the cause or circumstances of what|declarant|believed to be|his/her| impending death.

EFFECTIVE: 03/08/79

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 3 - 25

3-10.3.3 Statement Against Interest

A statement which was at the time of its making so far contrary to the declarant's pecuniary or proprietary interest, or so far tended to subject declarant to civil or criminal liability, or to render invalid a claim by declarant against another, that a reasonable person in that position would not have made the statement unless they believed it to be true. A statement tending to expose the declarant to criminal liability and offered to exculpate the accused is not admissible unless corroborating circumstances clearly indicate the trustworthiness of the statement.

EFFECTIVE: 03/08/79

3-10.3.4 Statement of Personal or Family History

(1) A statement concerning the declarant's own birth, adoption, marriage, divorce, legitimacy, relationship by blood, adoption, or marriage, ancestry, or other similar fact of personal or family history, even though declarant had no means of acquiring personal knowledge of the matter stated; or

(2) A statement concerning the foregoing matters, and death also, of another person, if the declarant was related to the other by blood, adoption, or marriage or was so intimately associated with the other's family as to be likely to have accurate information concerning the matter declared.

EFFECTIVE: 03/08/79

3-10.4 Statements Which Are Not Hearsay

Prior statements by a witness and admissions by a party-opponent are not considered to be hearsay under the Rules although they literally fall within the definition of hearsay.

EFFECTIVE: 08/21/87

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 3 - 26

3-10.4.1 Prior Statement by Witness

(1) A statement is not hearsay if the declarant testifies at a trial or hearing and is subject to cross-examination concerning the statement and the prior statement is inconsistent with his/her testimony and was given under oath subject to the penalty of perjury at a trial, hearing, or other proceeding, or in a deposition. If the declarant admits that he/she made the prior statement and that it was true, he/she adopts the statement. If he/she denies having made the statement, or admits having made it but denies its truth, the prior statement is admissible as substantive evidence.

(2) Thus, in keeping with the modern view of the hearsay rule, when a witness testifies to material facts and the opponent can prove that the witness has previously made statements under oath inconsistent with his/her present testimony, the previous statements are admissible as substantive evidence.

(3) Also, a statement is not hearsay if the declarant testifies at the trial or hearing and is subject to cross-examination concerning the statement, and the statement is consistent with his/her testimony and is offered to rebut an express or implied charge against him/her of recent fabrication or improper influence or motive. Prior consistent statements traditionally have been admissible to rebut such a charge, but under this rule are substantive evidence.

EFFECTIVE: 08/21/87

3-10.4.2 Admission by Party-Opponent

(1) Generally, an admission is a statement by a party of the existence of a fact relevant to the case but inconsistent with the position the party takes at the time of trial. The Rules provide, in part, that a statement is not hearsay if the statement is offered against a party and is (a) his/her own statement, the classic example of an admission, or (b) a statement of which he/she manifested his/her adoption or belief in its truth, or (c) a statement by a coconspirator of a party during the course and in furtherance of the conspiracy, or (d) a statement by a person authorized by the party to make a statement concerning the subject, or (e) a statement by the party's agent or servant concerning a matter within the scope of his/her agency or employment, made during the existence of the relationship.

(2) No guarantee of trustworthiness is required in the case

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 3 - 27

of an admission by a party because his/her responsibility is considered sufficient to justify its reception in evidence against him/her. Admissions by a party-opponent include confessions, i.e., a confession is a species of admission. In a criminal case, a confession constitutes a direct acknowledgment by the defendant of his/her guilt of the crime charged against him/her, whereas an admission is an acknowledgment by the defendant of certain facts which tend, together with other facts, to establish his/her guilt. As a narrative of the defendant's personal conduct a confession stands somewhat apart from an admission, calls for separate treatment, and special rules are applicable to it. Generally, a confession is admissible in evidence if it is satisfactorily shown that the defendant, in keeping with the traditional doctrine, made it voluntarily without inducements; and, if in keeping with the constitutional guarantees, the confession was not obtained in violation of the defendant's rights to remain silent and to have the assistance of counsel.

(3) If a statement is made by another person in the presence and hearing of a party containing assertions of fact which if untrue, the party would under all the circumstances naturally be expected to deny, his/her failure to speak has traditionally been receivable against him/her as an admission. These "tacit admissions" are received with caution, however, when they occur in the course of criminal investigation. The courts have surrounded them with various restrictions and safeguards, and the constitutional Miranda Rule serves to circumscribe them.

(4) As a matter of substantive law, the acts and declarations of one conspirator occurring while the conspiracy is in progress and in its furtherance are provable against another conspirator as acts for which the latter is criminally responsible. The declarations of one conspirator may also be proved against another conspirator as representative admissions to prove the truth of the matter asserted. The existence of the conspiracy must be proved independently to justify the admission of the declarations. Admissions made after the termination of the conspiracy are excluded.

EFFECTIVE: 08/21/87

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 3 - 28

3-10.5 Hearsay Within Hearsay

Hearsay included within hearsay is not excluded under the hearsay rule if each part of the combined statements conforms with an exception to the hearsay rule provided in these rules. Thus, in multiple hearsay situations, where the objections attaching to simple hearsay are even more involved, each of the out-of-court statements must satisfy the requirements of some exception to the hearsay rule.

EFFECTIVE: 08/21/87

3-10.6 Attacking and Supporting Credibility of Declarant

When a hearsay statement, or a statement of a coconspirator of a party, has been admitted in evidence, the credibility of the declarant may be attacked, and if attacked may be supported, by any evidence which would be admissible if the declarant had testified as a witness. Evidence of a statement or conduct by the declarant at any time, inconsistent with his/her hearsay statement, is not subject to any requirement that he/she may have been afforded an opportunity to deny or explain. If the party against whom a hearsay statement has been admitted calls the declarant as a witness, the party is entitled to examine him/her on the statement as if under cross-examination. Thus, the credibility of a hearsay declarant may be attacked and supported as though he/she had in fact testified. The credibility of a coconspirator may also be attacked or supported as in the case of a hearsay declarant even though the statement of a coconspirator of a party is not hearsay under the Rules.

EFFECTIVE: 08/21/87

3-11 CONTENTS OF WRITINGS, RECORDINGS, AND PHOTOGRAPHS

(1) The evidentiary doctrine governing the admissibility of the contents or terms of a written document was formerly called the "best evidence rule." Aimed at preventing inaccuracies and fraud by requiring the production of the original document itself, the best evidence rule was essentially related to writings. Modern techniques of recording, however, have expanded methods of storing data, e.g., by computers, photographic systems, and other developments. The instant rule applies to these expanded methods of recording facts as well as to traditional writings.

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 3 - 29

(2) Under the Rules an "original" of a writing or recording is the writing or recording itself, any counterpart intended to have the same effect, a photograph or its negative or print, or a computer printout. Thus, a carbon copy of a sales ticket or any print from the negative of a photograph is deemed to be an "original" for the purposes of this rule. A "duplicate" is a counterpart produced by techniques which accurately reproduce the original, e.g., produced by the same impression as the original or from the same matrix. In large measure, a duplicate is given the status of an original, e.g., a bank microfilm record of checks cleared.

(3) The general rule is that in order to prove the contents of a writing, recording, or photograph, the original writing, recording, or photograph is required, except as otherwise provided by the Rules or by Act of Congress. When a witness merely identifies a photograph or motion picture as a correct representation of events which he saw, however, this rule does not apply since it does not constitute an effort to prove the contents of the picture but is solely to use the picture to illustrate the witness' testimony. On the other hand, this rule does apply to an automatic photograph of a bank robbery as the photograph is used to prove its contents and has independent probative value.

(4) A duplicate is admissible to the same extent as an original unless a question is raised as to the authenticity of the original or it would be unfair in the circumstances to admit it.

(5) The original is not required, and other evidence of the contents of a writing, recording, or photograph is admissible if all originals are lost or have been destroyed, unless the proponent lost or destroyed them in bad faith; or no original can be obtained by judicial process; or at a time when an original was under the control of the party against whom offered, he was put on notice that the contents would be a subject of proof and he does not produce the original; or the writing, recording, or photograph is not closely related to a controlling issue. Under the foregoing circumstances, secondary evidence of the contents, with no degrees, is admissible.

(6) Contents of writings, recordings, or photographs may be proved by the testimony or deposition of the party against whom offered or by his written admission without accounting for the nonproduction of the original. The contents of public records, if otherwise admissible, may be proved by certified copies or testified to be correct by a witness who has compared it with the original. The contents of voluminous writings, recordings, or photographs which cannot conveniently be examined in court may be presented in the form of a chart, summary, or

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 3 - 30

calculation, but the originals or duplicates shall be available for examination by other parties and the court may order that they be produced in court.

(7) The identity and address of the person in possession of admissible writings, recordings, or photographs who can properly produce and identify them should always be ascertained and included in an investigative report. It should likewise be shown exactly what writings are to be produced voluntarily or under subpoena duces tecum.

EFFECTIVE: 08/21/87

3-12 IDENTIFICATION OR AUTHENTICATION OF REAL AND DOCUMENTARY EVIDENCE

(1) Real evidence, often called physical or demonstrative evidence, consists as noted of tangible things. Its variety is legion. It may constitute direct evidence, e.g., the jewelry stolen in a robbery; or circumstantial evidence, e.g., the latent fingerprint of the defendant lifted from the doorknob of the burglarized room. It may have played an active role in the crime, e.g., the fatal weapon in a murder case; or it may be employed for illustrative purposes, e.g., the photograph, chart, or model used to clarify trial testimony. Documentary evidence consists of words and figures set down on a writing, recording, or photograph, such as a letter, report, book of account, memorandum, or bank deposit slip. A document may be private or public in character.

(2) Before items of real and documentary evidence can be admitted in evidence, they must be identified or authenticated in some manner. They do not prove themselves. They must be shown to be what they are purported to be. For example, an article of clothing found at the scene of a crime cannot constitute relevant evidence against the defendant unless his ownership or previous possession of it is shown. A document purporting to be from the defendant relied upon to establish an admission by him, has no probative value unless it is shown that he authored it. This condition precedent to admissibility is satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims. Compliance with the requirements of identification or authentication, however, does not assure the admission of an item of real or documentary evidence into evidence since other rules of evidence may bar its admissibility.

(3) The requisite identification or authentication of real and documentary evidence may consist, for example, of the testimony of

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 3 - 31

a witness that he was present at the time and place when narcotics were taken from the defendant and, accounting for their custody through the period until trial including laboratory analysis, that the narcotics in court are those taken from the defendant. It may be the testimony of a witness who was present at the signing of a document in issue. It may consist of nonexpert opinion as to the genuineness of handwriting based on familiarity with the handwriting not acquired for purposes of the trial, or comparison by expert witnesses. A voice may be identified by opinion based upon hearing it at any time under circumstances connecting it with the alleged speaker.

(4) Prima facie authentication is accorded to certain documents and, accordingly, extrinsic evidence of authenticity as a condition precedent to admissibility is not required. Self-authenticating documents include domestic public documents, under seal or not under seal, foreign public documents, certified copies of public records, official publications, e.g., statutes and court reports, newspapers and periodicals, and writings acknowledged before a notary public. This presumptive authentication does not preclude evidentiary challenge to the genuineness of such documents. Although a newspaper may be received in evidence as authentic, the question of authority and responsibility for items therein contained remains open.

(5) To insure that items of real evidence will be admissible, it is essential that they be properly identified by the Agent when they are found, e.g., at a crime scene; that he make notes describing the evidence at that time and the way it was marked; that it is packaged carefully and the container properly identified; and that a chain of custody and a record thereof is maintained from the time of discovery to the time of the trial. This complete and rigorously adhered-to system of identification and custody negates the possibility of substitution, alteration, and tampering of real evidence and insures its admission at trial.

EFFECTIVE: 01/31/78

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 3 - 32

3-13 CONSTITUTIONAL SAFEGUARDS

(1) Constitutional safeguards, such as the protection against unlawful searches and seizures secured by the Fourth Amendment, the protection against self-incrimination secured by the Fifth Amendment, and the protection against denial of the right to the assistance of counsel at a critical stage in the prosecution secured by the Sixth Amendment must be borne in mind at all times during the course of investigation to ensure that evidence is obtained legally. Any evidence obtained in violation of constitutional rights is inadmissible.

(2) Agents are expected to be familiar with the FED.R.EVID., the basic doctrines of which should be considered in all investigations, whether criminal or civil. Likewise, these Rules must be considered in preparation of both investigative and prosecutive summary reports.

(3) All reasonable precautions must be taken to ensure that evidence obtained by Agents is admissible.

EFFECTIVE: 08/16/82

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 4 - 1

SECTION 4. JUVENILES AND JUVENILE DELINQUENCY ACT

4-1 GENERAL STATEMENT

EFFECTIVE: 02/22/88

4-1.1 Purpose of Act

The Juvenile Justice and Delinquency Prevention Act of 1974, Public Law 93-415, Title 18, USC, Sections 5031-5042 (hereinafter Act), and its pertinent legislative history, recognize that juvenile delinquency is primarily a concern of the states. The Act places virtually all juvenile cases in state courts and establishes limited, definable circumstances for the exercise of Federal jurisdiction. The discussion below outlines the procedures which govern the handling of juveniles in the Federal courts.

EFFECTIVE: 02/22/88

4-2 SPECIFIC PROVISIONS OF THE ACT

EFFECTIVE: 02/22/88

4-2.1 Definitions

(1) Juvenile - A person who has not attained his/her 18th birthday. For purpose of proceedings and disposition, a juvenile is a person who has not attained his/her 21st birthday. (See LHBSA, 3-16.1.)

(2) Juvenile Delinquency - The violation of a federal law by a person prior to his/her 18th birthday which would have been a "crime" if committed by an adult or a violation by such person of Title 18, USC, Section 922(x) (juvenile's possession, sale, delivery, or transfer of handgun and/or handgun ammunition).

(3) Federal Juvenile Judge - United States District Judge

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 4 - 2

(U.S.D.J.)

(4) Federal Juvenile Court - United States District Court (U.S.D.C.). The Act allows the court to be convened at any time or place within the judicial district and permits proceedings in the judge's chambers.

EFFECTIVE: 10/01/97

4-2.2 Arrest Procedure

The standard pre-arrest procedures applicable to adults (discussion with USA, filing of complaint, issuance of warrant) also govern arrests of juveniles. After arrest, however, the Act imposes several additional responsibilities on the arresting Agents.

EFFECTIVE: 02/22/88

4-2.2.1 Advice of Rights

The arresting Agents should immediately advise the arrested juvenile of his/her "legal rights" in language comprehensible to the juvenile. The rights found on the standard Miranda form, FD-395, appear to meet this requirement. However, inasmuch as no interview will be conducted (see 4-2.2.5 below), it will not be necessary to obtain a waiver signature from the juvenile at this time.

EFFECTIVE: 02/22/88

4-2.2.2 Notification of USA and Juvenile's Parents

(1) The Act requires the arresting Agent to immediately notify the USA and the juvenile's parents, guardian, or custodian of such custody. The parents, guardian, or custodian must also be notified of the juvenile's rights and the nature of the alleged offense.

(2) Because of the affirmative duties these provisions place on an arresting Agent, it can be anticipated that defendants will challenge the Bureau's compliance with the Act. Thus, it is necessary

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 4 - 3

that separate FD-302s be prepared to clearly demonstrate that (a) the juvenile was advised of his/her rights, (b) the USA was notified, (c) the parent(s), guardian, or custodian was notified, and (d) the juvenile was taken before a magistrate (see discussion in 4-2.2.6 below).

EFFECTIVE: 08/21/87

4-2.2.3 Fingerprinting and Photographing

The Act forbids fingerprinting and photographing a juvenile unless he/she is to be prosecuted as an adult, or the trial judge consents. Fingerprinting and photographing of a juvenile shall be done whenever a juvenile has been found guilty of committing an act which if committed by an adult would be a felony that is a crime of violence or a violation of Title 21, USC, Section 841 (manufacturing, distributing, dispensing of controlled substances or possession with intent to do same), section 952(a) (importation of controlled substances), section 955 (possession of controlled substances on board vessels arriving in or departing from United States) or section 959 (manufacture or distribution of controlled substances for purposes of unlawful importation). Because usually it will not be known at the time of arrest whether the arrestee will be prosecuted as an adult or handled as a juvenile offender, Agents are not to fingerprint or photograph a juvenile without consent of the judge.

EFFECTIVE: 08/21/87

4-2.2.4 Press Releases

The Act also prohibits making public either the name or picture of the juvenile. A press release is permissible concerning the arrest of a juvenile if carefully worded to contain no identifying information.

EFFECTIVE: 08/21/87

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 4 - 4

4-2.2.5 Interviews of Juveniles

A juvenile is not to be interrogated for a confession or admission of his/her own guilt, or even an exculpatory statement between the time of his/her arrest for a Federal offense and his/her initial appearance before the magistrate who advises him/her of his/her rights. Information volunteered by the arrested juvenile concerning his/her own guilt will be recorded in the Agent's notes for use in subsequent proceedings, and clarifying questions may be asked as necessary to make certain what the juvenile intends to say. The volunteered statement may be reduced to writing if such action does not involve any delay in the juvenile's appearance before the magistrate. The juvenile may, however, be questioned concerning the guilt of someone else if such questioning does not cause any delay in bringing him/her before the magistrate. These notes apply only from and after an arrest of a juvenile, as defined by Federal law for a Federal offense. They do not apply when the juvenile is still a suspect for a Federal offense under arrest by state or local officers on a state or local charge. The latter type situations do not come within the terms of the Act.

EFFECTIVE: 08/21/87

4-2.2.6 Initial Appearance Before Magistrate (See MIOG, Part II, 4-2.2.2; LHBSA, 3-16.2 (3).)

Bureau Agents must take the arrested juvenile before a magistrate forthwith. The magistrate must release the juvenile to his/her parents or guardian (or other responsible party) unless the magistrate determines that detention is necessary to secure the juvenile's timely appearance before the court, or to ensure the juvenile's safety or that of others. This determination can be made only after a hearing at which the juvenile is represented by counsel.

EFFECTIVE: 10/01/97

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 4 - 5

4-2.3 Detention

(1) The Act requires detention in certain types of facilities whenever possible. It also contains an absolute bar to detention in facilities where regular contact with adults results. Consequently, local juvenile facilities must be utilized whenever available. Local jail facilities approved by the Bureau of Prisons may be utilized when the more appropriate local juvenile facilities are not available, but only if the juvenile will have no regular contact with adults and insofar as possible, with adjudicated delinquents. If such a facility is not available locally, the juvenile must be released or transported to such a facility.

(2) Each office will ascertain through the United States Marshal the locations of those detention facilities within the field office territory which meet the criteria of this section and make such information available to all Agents assigned to the field office on a current basis. When suitable detention facilities are more conveniently located within the territory of an adjoining field office, such facilities should be used whenever possible.

EFFECTIVE: 02/22/88

4-2.4 Prosecution

(1) Certification - Once a juvenile has been taken into federal custody, or arrested by local authorities for an act which also constitutes a federal crime, a decision must be reached on the question of whether to prosecute the juvenile in state or federal court. As previously noted in paragraph 4-1.1, supra, the Act has the effect of placing most juvenile cases in state court. Thus, in order to pursue the case federally, the USA must file papers in U.S. District Court certifying that his/her investigation and research have determined that (a) the case is one of exclusive federal jurisdiction, or (b) the state has concurrent jurisdiction but the local prosecutor refuses to prosecute, or (c) the state does not have programs and services adequate for the needs of the juvenile, or (d) the offense charged is a crime of violence that is a felony or is a violation of Title 18, USC, Section 922(x) or 924(b), (g), or (h) (firearms offenses); Title 21, USC, Section 841, 952(a), 953, 955, 959, 960(b)(1), (b)(2), or (b)(3) (controlled substance offenses); and that there is a substantial federal interest in the case or offense. Federal jurisdiction always lies if the case involves an offense committed within the special maritime and territorial jurisdiction of

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 4 - 6

the United States and the maximum authorized term of imprisonment does not exceed 6 months. Without the existence of one of these grounds, a court of the United States cannot proceed against a juvenile and the juvenile must be surrendered to the appropriate state authorities.

(a) With regard to (1) (c), it is the responsibility of the Chief Probation Officer to conduct a study of the state juvenile facilities in his/her district to determine whether there are programs and services adequate for the needs of juveniles.

(b) The certification procedure is to be begun after the arrest process has been completed. If the juvenile is arrested in a distant district, he/she may be removed to the district of prosecution pursuant to Rule 40, FED.R.CRIM.P., before certification inasmuch as the USA in the district of prosecution is the only party who can determine whether one of the factors in (1) above exists which can invoke federal jurisdiction.

(2) Prosecution/Motion to Transfer to Adult Court - After proper certification has been made and the case has been accepted in federal court, the decision must be made whether to handle the defendant as a juvenile or transfer the matter to adult court. The Act shows a strong preference for proceeding as a juvenile. A juvenile action is commenced by the USA filing an information in the appropriate district court, in chambers, or otherwise.

(a) A transfer to adult court can be initiated by either (1) a written request of the juvenile, upon advice of counsel, or (2) the USA filing a motion to transfer (Motion to Proceed Against the Juvenile as an Adult). A motion to transfer may be filed: (1) where the offender was 15 years or older when the alleged act was committed if (a) the act would be a felony that is a crime of violence if it had been committed by an adult or if (b) the act is an offense under Title 18, USC, Section 922(x), 924(b), (g), or (h), or Title 21, USC, Section 841, 952(a), 955, or 959; or (2) where the offender was 13 years or older when the alleged act was committed if (a) the crime of violence is an offense under Title 18, USC, Section 113(a)(1) (assault with intent to commit murder), (a)(2) (assault with intent to commit any felony), or (a)(3) (assault with a dangerous weapon with the intent to do bodily harm), 1111 (murder), or 1113 (attempt to commit murder or manslaughter) or if (b) the crime is an offense under Title 18, USC, Section 2111 (robbery), 2113 (bank robbery), 2241(a) (aggravated sexual abuse), or 2241(c) (sexual act with a minor under 12 years or an attempt to do so), and is committed while the juvenile offender is in possession of a firearm. In addition, the court must find, after a hearing, that such a transfer

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 4 - 7

would be in the interest of justice. Transfer to adult status is mandatory when a juvenile of 16 years or older, who has a prior conviction or adjudication of an act which if committed by an adult would be one of the above-described offenses, allegedly commits a similar offense or an offense which would be a felony if committed by an adult and that involves the use, attempted use, or threatened use of physical force, or is an offense under Title 18, USC, Section 32 (destruction of aircraft or aircraft facilities), 81 (arson), 844(d), (e), (f), (h), or (i) (offenses involving explosives), or 2275 (firing or tampering with vessels).|

(b) To assure uniformity in those cases in which adult prosecution is desired, the USA must obtain authority from the Department of Justice before filing a motion to transfer to adult court. The juvenile will be afforded a hearing on this motion at which he/she has the right to be assisted by counsel. The judge must make findings of fact on the juvenile's age, background, nature of the offense, extent of juvenile's intellectual development, etc., before ruling on the motion to transfer. |In addition, the judge must consider the extent to which the juvenile played a leadership role in an organization or influenced others to take part in criminal activity involving the use or distribution of controlled substances or firearms.| Statements made by the juvenile in connection with a transfer hearing shall not be admissible at a subsequent criminal prosecution in adult court.

(3) Trial - If the juvenile is not proceeded against as an adult, the USA shall proceed by information for the alleged act of juvenile delinquency. The Act provides that the delinquency trial must take place within 30 days from the date the juvenile was placed in custody or the information shall be dismissed with prejudice, e.g., unless the delay was caused or consented to by the juvenile or his/her attorney, or would be in the interest of justice in the particular case. This provision is inapplicable if the juvenile is not detained (in custody). The juvenile trial can take place at any place within the district and will be tried by the judge (delinquency matters are not tried by a jury) in chambers or otherwise.

(4) |Prosecution/Disposition|- If the juvenile is adjudicated delinquent by the judge, a separate dispositional hearing must be held within 20 days after the adjudication. At this hearing the judge may (a) suspend the adjudication of delinquency; (b) place the juvenile on probation; (c) commit him/her to the custody of the Attorney General; or (d) enter an order of restitution. The maximum term of probation or commitment shall not extend beyond the juvenile's 21st birthday or the maximum term which could have been imposed on an

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 4 - 8

adult, whichever is sooner, unless the juvenile is between 18 and 21 years old at the time of disposition, in which case the maximum shall not exceed the lesser of three years or the maximum term which could have been imposed on an adult convicted of the same offense. |The term of commitment for a juvenile, who if convicted as an adult would be convicted of a Class A, B, or C felony, shall not exceed five years. |

EFFECTIVE: 10/01/97

4-2.5 Use of Juvenile Records

After the USA has filed an information initiating juvenile delinquency proceedings against a Bureau subject, any information or records in possession of the Bureau shall not be disclosed, directly or indirectly, unless authorized by the Act. This limitation applies to records obtained or prepared in the discharge of an official duty by an employee of the court or the FBI. Exceptions to this rule are set forth below:

- (1) Inquiries from the judge, USA, or defense counsel;
- (2) Inquiries from another court of law;
- (3) Inquiries from an agency preparing a presentence report for another court;
- (4) Inquiries from law enforcement agencies where the request for information is related to the investigation of a crime or a position within that agency;
- (5) Inquiries, in writing, from the director of a treatment agency or the director of a facility to which the juvenile has been committed by the court;
- (6) Inquiries from an agency considering the person for a position immediately and directly affecting the national security; and
- (7) Inquiries from any victim of such juvenile delinquency, or if the victim is deceased from the immediate family of such victim, related to the final disposition of such juvenile by the court.
- (8) Whenever a juvenile has on two separate occasions

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 4 - 9

been found guilty of committing an act, which if committed by an adult would be a felony crime of violence or an offense under Title 21, USC, Section 841, 952(a), 955 or 959, or whenever a juvenile has been found guilty of committing a single act after his/her 13th birthday, which if committed by an adult would be an offense under Title 18, USC, Section 113(a)(1), (a)(2), or (a)(3), 1111 or 1113, or, while the juvenile is in possession of a firearm, an offense under Title 18, USC, Section 2111, 2113, 2241(a) or 2241(c), the court shall transmit to the Criminal Justice Information Services Division the information concerning the adjudications, including name, offenses, sentences, court, dates of adjudication and notice that the proceedings were juvenile delinquency adjudications.

The limitations on disclosure apply to any juvenile records in possession of the Bureau, including arrest data, such as fingerprints and photographs. However, the records of a juvenile transferred for adult prosecution, or submitted to the FBI under the circumstances described in subparagraph (8) above, may be disseminated in the manner applicable to adult offenders.

EFFECTIVE: 10/01/97

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 5 - 1

SECTION 5. THE SPEEDY TRIAL ACT

5-1 GENERAL PROVISIONS

(1) The Speedy Trial Act, Title 18, USC, Sections 3161-3174, governs the time periods under which the government must file formal charges and be prepared to try an accused.

(2) The Act requires that an information or indictment be filed within 30 days from the date on which a person is arrested or served with a criminal summons. If the charge is a felony and no grand jury has been in session during the 30-day period, the time may be extended an additional 30 days.

(3) Upon a not guilty plea, the Speedy Trial Act requires the trial to commence no sooner than 30 days nor later than 70 days from the date of the public filing of the information or indictment or the defendant's first court appearance in the district where the charges are pending, whichever is later. The 70-day period may be extended by periods of excludable delay specified in the statute.

EFFECTIVE: 02/14/97

5-1.1 Sanctions in the Act

The failure to file an information or indictment against an arrested individual within the required period shall result in dismissal of the charge, possibly with prejudice. Failure to bring a defendant to trial within the specified time period will permit a defendant to move to have the indictment or information dismissed. Again, the judge may dismiss with prejudice.

EFFECTIVE: 08/21/87

5-2 EFFECT ON INVESTIGATIVE OPERATIONS

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 5 - 2

EFFECTIVE: 08/21/87

5-2.1 Arrest by State Authorities

(1) The arrest of a potential Federal defendant by state or local authorities on state charges does not activate the Act. However, if the state arrest is at the behest of Federal authorities it is likely to be viewed as an attempt to subvert the Act and the time limits would date from the time of the state arrest.

(2) If state authorities make a good faith arrest on state charges and later turn the defendant over to Federal authorities, the statute will begin to run when the state authorities turn the defendant over to Federal custody.

EFFECTIVE: 08/21/87

|| 5-2.2 | Issuance of Search Warrant for the Person

In investigating nonviolent offenses in which suspects can be expected to have evidence on their person (e.g., - gambling matters), consideration should be given to seizing the evidence under the authority of a search warrant rather than incident to the suspect's arrest. The issuance and execution of a search warrant for the person of a suspect does not activate the Act.

EFFECTIVE: 08/21/87

5-3 COMPLIANCE WITH THE ACT

EFFECTIVE: 08/21/87

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 5 - 3

5-3.1 Inform U.S. Attorney When Arrest Made

Agents should ensure that the U.S. Attorney is informed promptly of all Bureau arrests. This is to avoid the situation in which a Bureau fugitive or defendant is arrested on or near the last day in which a grand jury is in session. Because the Act requires prompt indictment after arrest, failure to advise the U.S. Attorney about the arrest might result in an inability to present the case to the grand jury within the specified time limits.

EFFECTIVE: 08/21/87

5-3.2 Timely Preparation of Reports

Agents should ensure that reports are complete and promptly submitted to the U.S. Attorney. All significant developments in an investigative matter, such as the unavailability of an essential witness, should be brought to the U.S. Attorney's attention without delay.

EFFECTIVE: 08/21/87

5-3.3 Filing of Complaints

Agents should seek the authority of the U.S. Attorney prior to filing a complaint. Premature arrests of Bureau subjects might unnecessarily invoke the Speedy Trial Act.

EFFECTIVE: 08/21/87

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 6 - 1

SECTION 6. COURT APPEARANCE AND TESTIMONY OF AGENTS

6-1 DEPARTMENTAL ORDER, REGULATIONS, AND LEGISLATION

EFFECTIVE: 07/27/81

6-1.1 Production or Disclosure in Federal and State Procedures

Source: Attorney General Order No. 919-80, 45 Fed. Reg. 83210, as codified in Chapter I, Subpart B, Section 16.21 et seq., Title 28, Code of Federal Regulations. This order prescribes procedures with respect to the production or disclosure of material or information in response to subpoenas or demands of courts or other authorities, except Congress, in state and Federal proceedings.

EFFECTIVE: 07/27/81

6-1.2 Chapter I, Part 16, Title 28, Code of Federal Regulations

"Section 16.21 Purpose and Scope.

"(a) This subpart sets forth procedures to be followed with respect to the production or disclosure of any material contained in the files of the Department, any information relating to material contained in the files of the Department, or any information acquired by any person while such person was an employee of the Department as a part of the performance of that person's official duties or because of that person's official status:

"(1) in all federal and state proceedings in which the United States is a party; and

"(2) in all federal and state proceedings in which the United States is not a party, including any proceedings in which the Department is representing a government employee solely in that employee's individual capacity, when a subpoena, order, or other demand (hereinafter collectively referred to as a 'demand') of a court or other authority is issued for such material or information.

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 6 - 2

"(b) For purposes of this subpart, the term 'employee of the Department' includes all officers, and employees of the United States appointed by, or subject to the supervision, jurisdiction, or control of the Attorney General of the United States, including U.S. attorneys, U.S. marshals, U.S. trustees and members of the staffs of those officials.

"(c) Nothing in this subpart is intended to impede the appropriate disclosure, in the absence of a demand, of information by Department law enforcement agencies to federal, state, local and foreign law enforcement, prosecutive, or regulatory agencies.

"(d) This subpart is intended only to provide guidance for the internal operations of the Department of Justice, and is not intended to, and does not, and may not be relied upon to create any right or benefit, substantive or procedural, enforceable at law by a party against the United States.

"Section 16.22 General prohibition of production or disclosure in federal and state proceedings in which the United States is not a party.

"(a) In any federal or state case or matter in which the United States is not a party, no employee or former employee of the Department of Justice shall, in response to a demand, produce any material contained in the files of the Department, or disclose any information relating to or based upon material contained in the files of the Department, or disclose any information or produce any material acquired as part of the performance of that person's official duties or because of that person's official status without prior approval of the proper Department official in accordance with Sections 16.24 and 16.25 of this chapter.

"(b) Whenever a demand is made upon an employee or former employee as described in subsection (a) of this section, the employee shall immediately notify the United States Attorney for the district where the issuing authority is located. The responsible United States attorney shall follow procedures set forth in Section 16.24 of this chapter.

"(c) If oral testimony is sought by a demand in any case or matter in which the United States is not a party, an affidavit, or, if that is not feasible, a statement by the party seeking the testimony or by his attorney, setting forth a summary of the testimony sought and its relevance to the proceeding, must be furnished to the responsible United States attorney. Any authorization for testimony

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 6 - 3

by a present or former employee of the Department shall be limited to the scope of the demand as summarized in such statement.

"(d) When information other than oral testimony is sought by a demand, the responsible United States attorney shall request a summary of the information sought and its relevance to the proceeding.

"Section 16.23 General disclosure authority in federal and state proceedings in which the United States is a party.

"(a) Every attorney in the Department of Justice in charge of any case or matter in which the United States is a party is authorized, after consultation with the 'originating component' as defined in Section 16.24(a) of this chapter, to reveal and furnish to any person, including an actual or prospective witness, a grand jury, counsel, or a court, either during or preparatory to a proceeding, such testimony, and relevant unclassified material, documents, or information secured by any attorney, or investigator of the Department of Justice, as such attorney shall deem necessary or desirable to the discharge of the attorney's official duties, provided, such an attorney shall consider, with respect to any disclosure, the factors set forth in Section 16.26(a) of this chapter, and further provided, an attorney shall not reveal or furnish any material, documents, testimony or information when, in the attorney's judgment, any of the factors specified in Section 16.26(b) exists, without the express prior approval by the Assistant Attorney General in charge of the division responsible for the case or proceeding, the Director of the Executive Office for United States Trustees (hereinafter referred to as 'the EOUST'), or such persons' designees.

"(b) An attorney may seek higher level review at any stage of a proceeding, including prior to the issuance of a court order, when the attorney determines that a factor specified in Section 16.26(b) exists or foresees that higher level approval for will be required before disclosure of the information or testimony in question. Upon referral of a matter under this subsection, the responsible Assistant Attorney General, the Director of EOUST, or their designees shall follow procedures set forth in Section 16.24 of this chapter.

"(c) If oral testimony is sought by a demand in a case or matter in which the United States is a party, an affidavit, or, if that is not feasible, a statement by the party seeking the testimony or by the party's attorney setting forth a summary of the testimony sought must be furnished to the Department attorney handling the case or matter.

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 6 - 4

"Section 16.24 Procedures in the event of a demand where disclosure is not otherwise authorized.

"(a) Whenever a matter is referred under Section 16.22 of this chapter to a United States Attorney or, under Section 16.23 of this chapter, to an Assistant Attorney General, the Director of the EOUST, or their designees (hereinafter collectively referred to as the 'responsible official'), the responsible official shall immediately advise the official in charge of the bureau, division, office, or agency of the Department that was responsible for the collection, assembly, or other preparation of the material demanded or that, at the time the person whose testimony was demanded acquired the information in question, employed such person (hereinafter collectively referred to as the 'originating component'), or that official's designee. In any instance in which the responsible official is also the official in charge of the originating component the responsible official may perform all functions and make all determinations that this regulation vests in the originating component.

"(b) The responsible official, subject to the terms of paragraph (c) of this section, may authorize the appearance and testimony of a present or former Department employee, or the production of material from Department files if:

"(1) there is no objection after inquiry of the originating component;

"(2) the demanded disclosure, in the judgment of the responsible official, is appropriate under the factors specified in Section 16.26(a) of this chapter; and

"(3) none of the factors specified in Section 16.26(b) of this chapter exists with respect to the demanded disclosure.

"(c) It is Department policy that the responsible official shall, following any necessary consultation with the originating component, authorize testimony by a present or former employee of the Department or the production of material from Department files without further authorization from Department officials whenever possible, provided that, when information is collected, assembled, or prepared in connection with litigation or an investigation supervised by a division of the Department or by the EOUST, the Assistant Attorney General in charge of such a division or

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 6 - 5

the Director of the EOUST may require that the originating component obtain the division or the EOUST's approval before authorizing a responsible official to disclose such information. Prior to authorizing such testimony or production, however, the responsible official shall, through negotiation and, if necessary, appropriate motions, seek to limit the demand to information, the disclosure of which would not be inconsistent with the considerations specified in Section 16.26 of this chapter.

"(d) (1) In a case in which the United States is not a party, if the responsible U.S. attorney and the originating component disagree with respect to the appropriateness of demanded testimony or of a particular disclosure, or if they agree that such testimony or such a disclosure should not be made, they shall determine if the demand involves information that was collected, assembled, or prepared in connection with litigation or an investigation supervised by a division of this Department or the EOUST. If so, the U.S. attorney shall notify the Director of the EOUST or the Assistant Attorney General in charge of the division responsible for such litigation or investigation, who may:

"(A) authorize personally or through a Deputy Assistant Attorney General, the demanded testimony or other disclosure of the information if such testimony or other disclosure, in the Assistant or Deputy Assistant Attorney General's judgment or in the judgment of the Director of the EOUST, is consistent with the factors specified in Section 16.26(a) of this chapter, and none of the factors specified in Section 16.26(b) of this chapter exists with respect to the demanded disclosure;

"(B) authorize, personally or by a designee, the responsible official, through negotiations and, if necessary, appropriate motions, to seek to limit the demand to matters, the disclosure of which, through testimony or documents, would not be inconsistent with the considerations, specified in Section 16.26 of this chapter, and otherwise to take all appropriate steps to limit the scope or obtain the withdrawal of a demand; or

"(C) if, after all appropriate steps have been taken to limit the scope or obtain the withdrawal of a demand, the Director of the EOUST or the Assistant or Deputy Assistant Attorney General does not authorize the demanded testimony or other disclosure, refer the matter, personally or through a Deputy Assistant Attorney General, for final resolution to the Deputy or Associate Attorney General, as indicated in Section 16.25 of this chapter.

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 6 - 6

"(2) If the demand for testimony or other disclosure in such case does not involve information that was collected, assembled, or prepared in connection with litigation or an investigation supervised by a division of this Department, the originating component shall decide whether disclosure is appropriate, except that, when especially significant issues are raised, the responsible official may refer the matter to the Deputy or Associate Attorney General, as indicated in Section 16.25 of this chapter. If the originating component determines that disclosure would not be appropriate and the responsible official does not refer the matter for higher level review, the responsible official shall take all appropriate steps to limit the scope or obtain the withdrawal of a demand.

"(e) In a case in which the United States is a party, the Assistant Attorney General or the Director of the EOUST responsible for the case or matter, or such persons' designees, are authorized, after consultation with the originating component, to exercise the authorities specified in Section 16.24(d) (1) (A)-(C) of this chapter, provided that, if a demand involves information that was collected, assembled, or prepared originally in connection with litigation or an investigation supervised by another unit of the Department, the responsible official shall notify the other division or the EOUST concerning the demand and the anticipated response. If two litigating units of the Department are unable to resolve a disagreement concerning disclosure, the Assistant Attorneys General in charge of the two divisions in disagreement, or the Director of the EOUST and the appropriate Assistant Attorney General, may refer the matter to the Deputy or Associate Attorney General, as indicated in Section 16.25(b) of this chapter.

"(f) In any case or matter in which the responsible official and the originating component agree that it would not be appropriate to authorize testimony or otherwise to disclose the information demanded, even if a court were so to require, no Department attorney responding to the demand should make any representation that implies that the Department would, in fact, comply with the demand if directed to do so by a court. After taking all appropriate steps in such cases to limit the scope or obtain the withdrawal of a demand, the responsible official shall refer the matter to the Deputy or Associate Attorney General, as indicated in Section 16.25 of this chapter.

"(g) In any case or matter in which the Attorney General is personally involved in the claim of privilege, the responsible official may consult with the Attorney General and proceed in accord

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 6 - 7

with the Attorney General's instructions without subsequent review by the Deputy or Associate Attorney General.

"Section 16.25 Final action by the Deputy or Associate Attorney General.

"(a) Unless otherwise indicated, all matters to be referred under Section 16.24 by an Assistant Attorney General, the Director of the EOUST, or such person's designees to the Deputy or Associate Attorney General shall be referred (1) to the Deputy Attorney General, if the matter is referred personally by or through the designee of an Assistant Attorney General who is within the general supervision of the Deputy Attorney General, or (2) to the Associate Attorney General, in all other cases.

"(b) All other matters to be referred under Section 16.24 to the Deputy or Associate Attorney General shall be referred (1) to the Deputy Attorney General, if the originating component is within the supervision of the Deputy Attorney General or is an independent agency that, for administrative purposes, is within the Department of Justice, or (2) to the Associate Attorney General, if the originating component is within the supervision of the Associate Attorney General.

"(c) Upon referral, the Deputy or Associate Attorney General shall make the final decision and give notice thereof to the responsible official and such other persons as circumstances may warrant.

"Section 16.26 Considerations in determining whether production or disclosure should be made pursuant to a demand.

"(a) In deciding whether to make disclosures pursuant to a demand, Department officials and attorneys should consider:

"(1) Whether such disclosure is appropriate under the rules of procedure governing the case or matter in which the demand arose, and

"(2) Whether disclosure is appropriate under the relevant substantive law concerning privilege.

"(b) Among the demands in response to which disclosure will not be made by any Department official are those demands with respect to which any of the following factors exist:

"(1) Disclosure would violate a statute, such as the

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 6 - 8

income tax laws, 26 U.S.C. 6103 and 7213, or a rule of procedure, such as the grand jury secrecy rule, F.R.Cr.P., Rule 6(e),

"(2) Disclosure would violate a specific regulation;

"(3) Disclosure would reveal classified information, unless appropriately declassified by the originating agency,

"(4) Disclosure would reveal a confidential source or informant, unless the investigative agency and the source or informant have no objection,

"(5) Disclosure would reveal investigatory records compiled for law enforcement purposes, and would interfere with enforcement proceedings or disclose investigative techniques and procedures the effectiveness of which would thereby be impaired,

"(6) Disclosure would improperly reveal trade secrets without the owner's consent.

"(c) In all cases not involving considerations specified in subsections (b)(1)-(6) of this section, the Deputy or Associate Attorney General will authorize disclosure unless, in that person's judgment, after considering subsection (a) of this section, disclosure is unwarranted. The Deputy or Associate Attorney General will not approve disclosure if the circumstances specified in subsection (b)(1)-(3) of this section exist. The Deputy or Associate Attorney General will not approve disclosure if any of the conditions in subsections (b)(4)-(6) of this section exist, unless the Deputy or Associate Attorney General determines that the administration of justice requires disclosure. In this regard, if disclosure is necessary to pursue a civil or criminal prosecution or affirmative relief, such as an injunction, consideration shall be given to:

"(1) the seriousness of the violation or crime involved,

"(2) the past history or criminal record of the violator or accused,

"(3) the importance of the relief sought,

"(4) the importance of the legal issues presented,

"(5) other matters brought to the attention of the Deputy or Associate Attorney General.

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 6 - 9

"(d) Assistant Attorneys General, United States attorneys, the Director of the EOUST, United States trustees, and their designees, are authorized to issue instructions to attorneys and to adopt supervisory practices, consistent with this subpart, in order to help foster consistent application of the foregoing standards and the requirements of this subpart.

"Section 16.27 Procedure in the event a Department decision concerning a demand is not made prior to the time a response to the demand is required.

"If response to a demand is required before the instructions from the appropriate Department official are received, the responsible official or other Department attorney designated for the purpose shall appear and furnish the court or other authority with a copy of the regulations contained in this subpart and inform the court or other authority that the demand has been or is being, as the case may be, referred for the prompt consideration of the appropriate Department official and shall respectfully request the court or authority to stay the demand pending receipt of the requested instructions.

"Section 16.28 Procedure in the event of an adverse ruling.

"If the court or other authority declines to stay the effect of the demand in response to a request made in accordance with Section 16.27 of this chapter pending receipt of instructions, or if the court or other authority rules that the demand must be complied with irrespective of instructions rendered in accordance with Sections 16.24 and 16.25 of this chapter not to produce the material or disclose the information sought, the employee or former employee upon whom the demand has been made shall, if so directed by the responsible Department official, respectfully decline to comply with the demand. See United States ex rel. Touhy v. Ragen, 340 U.S. 462 (1951).

"Section 16.29 Delegation by Assistant Attorneys General.

"With respect to any function that this subpart permits the designee of an Assistant Attorney General to perform, the Assistant Attorneys General are authorized to delegate their authority, in any case or matter or any category of cases or matters, to subordinate division officials or U.S. attorneys, as appropriate."

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 6 - 10

It should be noted that the above regulations do not apply to requests for information under either the Freedom of Information or Privacy Acts.

EFFECTIVE: 07/27/81

6-1.3 Exception To Chapter I, Part 16, Title 28, Code of Federal Regulations

(1) Whenever a demand is made upon an employee or former employee of the Department for the production of material, or the disclosure of information pertaining to investigations supervised and/or reviewed by the Civil Rights Division, the employee shall immediately notify the USA for the district from which the demand has been issued. The U.S. Attorney shall immediately contact the Deputy Assistant Attorney General of the Civil Rights Division who shall refer the matter to the appropriate Section Chief for review of the information whose disclosure is sought. If the Section Chief approves a demand for the production of material or disclosure of information, he or she shall so notify the USA and such other persons as circumstances may warrant.

(2) If the Section Chief does not authorize disclosure he or she shall notify the Assistant Attorney General of the Civil Rights Division or a designated Deputy Assistant Attorney General, who may:

(a) Authorize personally the demanded testimony or other disclosure of the information if such testimony or other disclosure, in the Assistant or Deputy Assistant Attorney General's judgment is consistent with the factors specified in 28 C.F.R. Section 16.26(a) of this part and none of the factors specified in 28 C.F.R. Section 16.26(b) exists with respect to the demanded disclosure; or

(b) Authorize negotiations and, if necessary, appropriate motions, to seek to limit the demand to matters, the disclosure of which would not be inconsistent with the considerations specified in 28 C.F.R. Section 16.26, and otherwise to take all appropriate steps to limit the scope or obtain the withdrawal of a demand; or

(c) If, after all appropriate steps have been taken to limit the scope or obtain the withdrawal of a demand, the Assistant or Deputy Assistant Attorney General does not authorize the demanded

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 6 - 11

testimony or other disclosure, refer the matter, for final resolution to the Deputy or Associate Attorney General, as indicated in 28 C.F.R. Section 16.25.

EFFECTIVE: 07/27/81

6-1.3.1 Instructions For Handling Demands In Civil Rights Cases

Upon receipt of a demand for production of material, or disclosure of information pertaining to a civil rights investigation, immediately notify the USA for the district in which the demand arose. Notify FBIHQ, Criminal Investigative Division, Attention: Civil Rights Unit, by an appropriate communication of receipt of the demand, the results of your contact with the USA and all pertinent factors you believe appropriate for consideration in reaching a resolution to the demand. A copy of the demand, if possible, should be forwarded with your initial communication. This information will be furnished to the Civil Rights Division (CRD), DOJ, for their final determination which generally will be communicated directly to the USA. You will be notified by FBIHQ of the action taken by the CRD. In all instances, keep FBIHQ appropriately advised of all developments concerning each such demand.

EFFECTIVE: 01/09/84

6-1.4 Jencks Act, Rule 26.2, Federal Rules of Criminal Procedure (FED.R.CRIM.P.)

The Jencks Act, originally enacted in 1957 and contained in Title 18, USC, Section 3500, provides for the production of statements of Government witnesses. The statute was broadened in 1980 and 1983, moved to FED.R.CRIM.P., and now provides that after any witness other than the defendant testifies on direct examination at a pretrial suppression hearing or in a Federal criminal trial, the court, upon motion of a party who did not call the witness, shall order the attorney for the Government or the defendant and his/her attorney, as the case may be, to produce, for the examination and use of the moving party any statement of the witness that is in their possession and that relates to the subject matter concerning which the witness has testified.

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 6 - 12

EFFECTIVE: 01/09/84

6-1.4.1 Matter Deemed Irrelevant

The statute affords the Government an opportunity to object to the production of an entire statement if portions do not relate to the testimony of the witness. The court may excise such parts before delivery of the statement to the defendant.

EFFECTIVE: 01/09/84

6-1.4.2 Noncompliance by the Government

If the United States elects not to comply with a production order, the court may strike from the record the testimony of the witness, or may in its discretion declare a mistrial.

EFFECTIVE: 08/16/82

6-1.4.3 Definition of Statement

The term "statement" as used in Rule 26.2, |FED.R.CRIM.P.,| is defined as follows:

(1) A written statement made by the witness and signed or otherwise adopted by him/her;

(2) A stenographic, mechanical, electrical, or other recording, or a transcription thereof, which is a substantially verbatim recital of an oral statement made by the witness and recorded contemporaneously with the making of an oral statement;

(3) A statement, however taken or recorded, or a transcription thereof, if any, made by the witness to a grand jury.

EFFECTIVE: 08/16/82

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 6 - 13

6-1.4.4 Review by FBI

Before trial, it is the responsibility of the Agent most familiar with the case to review carefully all statements and reports which are to be delivered to the USA and which may be the subject of a motion under Rule 26.2, FED.R.CRIM.P. If any document contains material which is privileged or confidential, or which might disclose the identity of confidential informants or confidential investigative techniques, this fact should be clearly expressed to the USA in writing.

EFFECTIVE: 08/16/82

6-1.4.5 National Security Cases

Documents having a national security aspect will be reviewed by FBIHQ. The field office will be advised as to what may be delivered to the USA.

EFFECTIVE: 08/16/82

6-1.4.6 Prompt Delivery to the USA

All statements and reports should be delivered to the USA in sufficient time for him/her to review such materials before trial. Any FBI employee directed by the court to deliver these documents should advise that they are in the possession of the USA.

EFFECTIVE: 08/16/82

6-1.4.7 Advice to FBIHQ - Problem Cases

Should it appear that the position taken by the judge, USA, or other person with respect to any phase of the production of documents is of present or potential concern to the Bureau, FBIHQ should be advised under the caption of the case as quickly as the urgency of the matter requires. Such problems include: (1) failure to properly use and safeguard the documents and return them to the FBI when no longer needed for court purposes; (2) any tendency by the USA to produce unnecessary material or failure to advise the court of

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 6 - 14

those parts of the documents which should be excised before surrender to the defense; (3) any fact indicating that a defendant who has received statements of prosecution witnesses before they testify has injured or threatened a witness or otherwise attempted to obstruct justice by making the witness unavailable or by making witness change his/her testimony.

EFFECTIVE: 08/21/87

6-1.4.8 Government Agent as Witness

Reports of Government Agents appearing as witnesses in Federal criminal trials, which contain summaries of information given to them by other persons, constitute prior statements made by a witness. To the extent that the reports relate to the Agent-witness' direct testimony, they are producible under Rule 26.2, FED.R.CRIM.P. Thus, where the Agent testifies concerning admissions or other statements made to Agent by a defendant, that part of Agent's report which reflects interview with the defendant, including Agent's own impressions is producible. However, if the same report also reflects statements made by persons other than the defendant, the part dealing with these latter matters should be deleted prior to production, since these are matters about which the Agent will not have testified because of the hearsay rule. This same procedure should be followed if the Agent, who testifies as a witness, is not the Agent who wrote the report, but the report is based upon Agent's notes as well as the notes of the Agent who prepared it and checks it for accuracy before it is submitted. In such cases, the report will be in effect the joint statement of both Agents.

EFFECTIVE: 08/21/87

6-1.4.9 Investigative Notes

Generally an oral statement by a witness is recorded contemporaneously on Form FD-302, and this form will be producible under Rule 26.2, FED.R.CRIM.P., once the witness has testified. In some jurisdictions, the Government may also be required to produce the investigative notes of the Agent who interviewed the witness and prepared the FD-302. Accordingly, Agents are required to retain all interview notes in the 1-A portion of the investigative file. (See also, Legal Handbook for Special Agents, Section 7-13.)

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 6 - 15

EFFECTIVE: 08/21/87

6-2 CRIMINAL TRIALS IN BUREAU CASES WHERE BUREAU FILES ARE
SUBPOENAED

EFFECTIVE: 08/21/87

6-2.1 Statements of All Witnesses, Such as FD-302s

(1) These statements are controlled by the USA. (See Paragraph 6-1.4, supra.) Before trial, review all documents of this type pertinent to case and deliver to USA before the trial, except for those having national security aspect. Documents of the latter type will be reviewed at FBIHQ and the field will be advised what may be furnished. In other cases review shall be by SAC, ASAC, or Agent most familiar with the case.

(2) If any document contains material which is privileged or confidential, or which might disclose identity of confidential informant or confidential investigative technique, make that fact known clearly to USA in writing.

(3) Any Bureau witness or employee directed by the court to deliver these documents should courteously advise that they are in the possession of the USA.

(4) Should it appear that the position taken by the judge, USA, or other person with respect to any phase of the production of documents is of present or potential concern to the Bureau, FBIHQ should be advised under the caption of the case as quickly as the urgency of the matter requires. Such problems include: (a) failure to properly use and safeguard the documents and return them to the FBI when no longer needed for court purposes; (b) any tendency by the USA to produce unnecessary material or failure to advise the court of those parts of documents which should be excised before surrender to the defense; (c) any fact indicating that a defendant who has received statements of prosecution witnesses before they testify has injured or threatened a witness or otherwise attempted to obstruct justice by making the witness unavailable or by making witness change his/her testimony.

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 6 - 16

EFFECTIVE: 07/14/88

6-2.2 Other Bureau Files, Manuals, Recordings, Etc.

(1) Upon receipt of a demand for other Bureau documents the employee on whom the demand is made will bring it immediately to the attention of the Principal Legal Advisor (PLA), or if absent, to a Legal Advisor for handling. The USA in the district where the demand was issued shall be immediately notified of receipt of the demand.

(2) The PLA is authorized to exercise the responsibilities of the originating component as defined in Paragraph 6-1.2, supra. (See 28 CFR 16.24.) If the PLA concurs with the USA that disclosure of the document(s) subject to the demand should be made and none of the factors cited in Paragraph 6-1.2, supra, (see 28 CFR 16.26 (b)) or other relevant considerations are present, i.e. the Privacy Act, see Paragraph 6-4, infra, no communication with FBIHQ is necessary. Record the response to the demand, together with all documents relating thereto under the 197 classification.

(3) If the PLA disagrees with the USA as to the appropriateness of disclosure, or if both agree that disclosure should not be made, refer the matter to FBIHQ, Office of the General Counsel, by appropriate communication consistent with the exigencies of the circumstances for resolution with the Department of Justice (DOJ). Your communication should set forth in detail the nature of the demand and your objections thereto. Request the USA to appear with the employee on whom the demand is made. If the court declines to defer a ruling until instructions are received from the DOJ, the employee on whom the demand is made shall respectfully decline to produce as set forth in Paragraph 6-1.2, supra. (See 28 CFR Sections 16.27 and 16.28.)

EFFECTIVE: 09/09/94

6-3 AGENT OR EMPLOYEE TESTIMONY GENERALLY: FEDERAL
PROSECUTIONS

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 6 - 17

EFFECTIVE: 07/14/88

6-3.1 Subpoena or Request to Testify

On receipt of request from USA or issuance of subpoena for appearance of an Agent from another field office in any Federal case, SAC of office of appearance should direct communication to office of assignment of Agent setting forth all available details. SAC of office to whom Agent is assigned should be satisfied that presence of Agent is necessary and should record SAC's views by notation on incoming communication, or if request is oral, by memorandum to the file. The above also applies to non-Agent employees. (See MAOP, Part II, 2-3.3.1, regarding indexing requirements.)

EFFECTIVE: 07/14/88

6-3.2 Advice to USA

Agents must advise the appropriate USA handling important cases in which statute of limitations will run shortly, or cases of great public interest, of fact that subpoena has been issued and that Agent must comply.

EFFECTIVE: 05/25/90

6-3.3 While Waiting to Testify

If Agent or employee has arrived in field office of testimony but his/her presence is not immediately necessary as a witness, SAC should assign work to him/her provided there is no interference with appearance as witness or departure after testimony.

EFFECTIVE: 05/25/90

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 6 - 18

6-3.4 Cooperation of USA

USAs should advise SAC of impending subpoena. Secure USA's cooperation in such matters.

EFFECTIVE: 05/25/90

6-3.5 Agent at Counsel Table

If SAC is satisfied that such action is justified, SAC is authorized to approve request by USA that Agent sit at counsel table during trial. If the request involves an Agent assigned to a field office other than that in which trial occurs, SAC in whose territory trial is being held and who approves request must ensure that SAC to whom Agent is assigned is appropriately advised.

EFFECTIVE: 05/25/90

6-3.6 Delay of Trial

Office of prosecution is responsible for notification when trial is being delayed. Communication advising of delay in trial must specifically state whether Bureau personnel are prospective witnesses. If FBI witness is assigned to FBIHQ, direct communication to appropriate FBIHQ division and state name and title, if known, of witness. Include all information so that action at FBIHQ can be taken without file check or search for previous communications. If witness needed at later date, so state and show date needed, if known. Every communication to Bureau showing a delay in trial of a Bureau case must state the specific reason for the delay.

EFFECTIVE: 05/25/90

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 6 - 19

6-3.7 Manner of Testifying

Agent, or other employee testifying, must describe official status with the Federal Bureau of Investigation, such as Special Agent. Give all testimony clearly, modestly, and without bias, prejudice, emotion, exaggeration, or misrepresentation. Speak distinctly so that the court, jury, counsel, and spectators may hear. Avoid testimony not relevant to prosecution. To prevent prejudice to the rights of the accused during the trial, Agents or other employees testifying in the case should avoid unnecessary contact or conversation with jurors or witnesses and should be aware of the possible existence of an order issued by the court prohibiting communications among witnesses during the course of the trial. Such orders, often referred to as sequestration orders, are within the province of a judge, federal or state; and FBI employees must comply with the provisions of such orders in cases in which they are testifying.

EFFECTIVE: 09/11/97

6-3.8 Requests for Documents While Testifying

If documents are those covered by 6-1.4, supra, and are in the hands of USA, courteously advise court that USA has possession. If directed to produce any other Bureau file, report, or official document, refer to and follow instructions set forth in Paragraph 6-2.2, supra.

EFFECTIVE: 05/25/90

6-3.9 Testimony of FBI Laboratory Division Employees

(1) Mark communication concerning witness appearance of these employees for the attention of the appropriate sections of the Laboratory Division.

(2) Under certain circumstances where the expert findings are negative and where funds are available under state, local and Federal criminal codes, the defense may be required to bear the expense for travel and expert witness fees of Laboratory Division

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 6 - 20

employees. You should immediately forward any such requests to the appropriate sections of the Laboratory Division.

EFFECTIVE: 09/24/93

6-4 CIVIL TRIALS IN BUREAU CASES

Refer to and follow instructions set forth in Paragraph 6-2.2, supra. The Privacy Act, 5 USC 552a, generally prohibits disclosure of information from FBI records systems about an individual, retrievable by the individual's name or other identifier, to a third party or another agency without the written consent of the individual. 5 USC 552a(b) identifies eleven exceptions to the above nondisclosure rule. The Act contains both civil and criminal penalties for violation thereof. Disclosure to those demands originating with local, state or other Federal law enforcement authorities may be made pursuant to Section 552a(b)(3) of the Act, the "routine use" exception, or they may fall within the Section 552a(b)(7) exception for unconsented disclosure. However, certain demands, primarily those involving civil litigation to which the United States is not a party, will raise Privacy Act considerations where the demand seeks information concerning an individual other than on whose behalf the demand was issued. Although Section 552a(b)(11) of the Act provides for disclosure "pursuant to the order of a court of competent jurisdiction," limited case law and departmental policy state that a subpoena does not meet the requirements of subsection (b)(11) since it is not signed by a judge and is always subject to being quashed or modified by a court. In such circumstances, the Privacy Act considerations will be brought to the attention of the USA with a request that a court order for disclosure be required prior to compliance. If the USA does not concur with this requirement, promptly notify FBIHQ, Office of the General Counsel, for resolution.

EFFECTIVE: 09/09/94

6-5 STATE AND MILITARY CRIMINAL TRIALS

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 6 - 21

EFFECTIVE: 08/16/82

6-5.1 Statements of All Witnesses, Such as FD-302s

(1) Department policy concerning requests for production of FD-302s and FBI Laboratory reports in state courts is that such requests will be honored where (a) the document is one which we would be required to produce under Rule 26.2, FED.R.CRIM.P., or otherwise if the case were in Federal Court; (b) the document is of a type produced under the law of that state, and (c) no overriding policy consideration, such as national security, opposes granting the request.

(2) Requests of this type may be anticipated where both the Bureau and state or military officers have investigated the same act.

(3) In each case, state and military, the PLA is to advise the USA and handle pursuant to Paragraph 6-2.2, supra. In the event a demand calls for the appearance of the Director, without making provision for an authorized representative as a substitute, developments should be monitored closely and reported as they occur. It is of extreme importance to quash such subpoenas or to arrange for a substitute whenever possible.

EFFECTIVE: 08/16/82

6-5.2 Other Bureau Files, Manuals, Recordings, Etc.

Handle as directed under Paragraph 6-2.2, supra.

EFFECTIVE: 08/16/82

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 6 - 22

6-5.3 Agent or Employee Testimony Generally: State, Local,
Military Prosecutions

On receipt of a subpoena, demand, or request for testimony, the employee upon whom the demand is made will promptly notify the PLA, or if absent, a Legal Advisor, of the demand. The USA will be immediately notified of receipt of the demand. If the PLA and the USA agree that disclosure may be made, i.e., none of the factors cited in Paragraph 6-1.2, supra, (see 28 CFR 16.26(b)) or other relevant considerations are present, no communication with FBIHQ is necessary. Record the nature of the testimony furnished by memorandum, together with all documents relating thereto, in the substantive case file from which the demand arose. If the PLA disagrees with the USA as to the appropriateness of disclosure, or if both agree that disclosure should not be made, refer the demand to FBIHQ by appropriate communication consistent with the exigencies of the circumstances for resolution with the Department. Your communication to FBIHQ should set forth in detail the nature of the demand and your objections thereto. Request the USA to appear with the employee on whom the demand is made. If the Court or other authority declines to defer a ruling until instructions are received from the Department, the employee on whom the demand is made shall respectfully decline to testify as set forth in Paragraph 6-2.2, supra.

EFFECTIVE: 08/16/82

6-6 STATE CIVIL TRIALS

Handle requests for both documents and testimony as directed in Paragraphs 6-2.2, 6-4 and 6-5.3, supra.

EFFECTIVE: 08/16/82

6-7 ADMINISTRATIVE HEARINGS AT WHICH DEPARTMENT OF JUSTICE IS
NOT REPRESENTED BY U.S. ATTORNEY OR OTHER ATTORNEY

EFFECTIVE: 08/16/82

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 6 - 23

6-7.1 Statements of All Witnesses, Such as FD-302s

Rule 26.2, FED.R.CRIM.P., requires, in part, that statements of witnesses for the prosecution, made to the Government before trial, be made available to the defense for cross-examination after the witness has testified in a criminal case. The Department of Justice has advised, however, that the same practice will be followed in administrative hearings. Except for unusual cases, which should be brought immediately to the attention of FBIHQ, Office of the General Counsel, field offices will take no action until there is an actual demand for the statement of a witness to be used in an administrative hearing. On such demand, take the following action:

(1) Advise requesting agency that question of making these documents available must be resolved with the USA. Advise USA promptly.

(2) Obtain from requesting agency a detailed statement, in nature of witness sheet, showing anticipated testimony of witness on whom FD-302 is requested.

(3) Find in field office files the FD-302 which represents the first recording of witness' report to FBI.

(4) Advise USA of testimony anticipated and of that information contained in the FD-302, if any, which you believe should be excised as irrelevant or privileged.

EFFECTIVE: 09/09/94

6-7.2 Other Documents of Any Kind

| Handle pursuant to Paragraph 6-2.2 supra. |

EFFECTIVE: 07/27/81

6-7.3 Testimony of FBI Personnel

| Follow same procedure as in Paragraph 6-5.3, supra. |

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 6 - 24

EFFECTIVE: 07/27/81

6-8 ADMINISTRATIVE HEARINGS AT WHICH DEPARTMENT OF JUSTICE IS
REPRESENTED BY U.S. ATTORNEY OR OTHER ATTORNEY

EFFECTIVE: 07/27/81

6-8.1 Statements of All Witnesses, Such as FD-302s

| Handle pursuant to Paragraph 6-2.2, supra. |

EFFECTIVE: 07/27/81

6-8.2 Other Documents of Any Kind

| Handle pursuant to Paragraph 6-2.2, supra. |

EFFECTIVE: 07/27/81

6-8.3 Testimony of FBI Personnel

| Handle pursuant to Paragraph 6-5.3, supra. |

EFFECTIVE: 07/27/81

6-9 HABEAS CORPUS PROCEEDINGS IN FBI CASES

EFFECTIVE: 07/27/81

| 6-9.1 | Deleted |

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 6 - 25

EFFECTIVE: 07/27/81

6-9.2 Responsibility of SAC

It is the responsibility of each SAC to insure immediate notification of his office regarding the filing of habeas corpus proceedings in cases investigated by the FBI. Where such proceedings are filed, FBIHQ must be immediately advised of all pertinent facts and developments. Copies of petitions for writs of habeas corpus and other pleadings and briefs in such proceedings must be immediately obtained and forwarded to FBIHQ. It is the responsibility of each SAC to take appropriate action to insure the complete refutation of all false allegations of mistreatment, misconduct, or otherwise on the part of Agents which may be raised in such proceedings. The official court records in each instance must clearly show a thorough and complete refutation of such false allegations.

EFFECTIVE: 07/27/81

6-9.3 Refutation of False Allegations

Whenever, during the course of a trial in either Federal or state courts, derogatory statements or false allegations of misconduct, brutality, or other illegal treatment are made against Agents of the FBI, immediate steps are to be taken by the Agents present through the U.S. Attorney or state prosecutor to ensure a complete refutation on the official court record of such false statements or allegations. Agents in attendance at such trials should immediately advise the SAC of the field office where the case is being tried of the facts concerning such derogatory statements and false allegations. It is the responsibility of the SAC to determine and ensure that all false statements and allegations are adequately refuted on the official court records and to promptly advise FBIHQ of all pertinent facts and circumstances.

EFFECTIVE: 05/26/89

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 6 - 26

6-10 OTHER TRIALS AND HEARINGS

If testimony or documents are subpoenaed or requested for any trial or hearing of a type different from those listed above, such as a Federal trial for a criminal offense within the jurisdiction of another agency, advise USA promptly and adapt from instructions above the procedures appropriate to the case. If in doubt, consult Office of the General Counsel, FBIHQ.

EFFECTIVE: 09/09/94

6-11 OTHER REQUESTS - MISCELLANEOUS

When a request for information from Bureau files is received through a medium other than a court order or a subpoena, the person or organization requesting information from FBI files should be informed that Bureau files are confidential and information contained therein can be disclosed only pursuant to regulations of the Attorney General. The provisions of Attorney General Order No. 919-80 do not prohibit the dissemination of information gathered by the FBI to other concerned law enforcement, prosecutive, or regulatory agencies. (See Paragraph 6-1.2, supra.)

EFFECTIVE: 05/26/89

6-12 SUBPOENAS DIRECTED TO FBIHQ

(1) Under ordinary circumstances, subpoenas directed to FBIHQ, including those addressed to the Director by name or title and those addressed to other FBIHQ personnel, will be delivered by Deputy U.S. Marshal to the Washington Metropolitan Field Office (WMFO). Where subpoenas are accepted, immediately notify the interested division and Office of the General Counsel at FBIHQ so appropriate action may be taken. Where the Director is sued in his individual capacity in a civil action, and such civil action alleges matters arising out of his official conduct as Director of the FBI, the General Counsel - Office of the General Counsel has been authorized by appointment to accept service on behalf of the Director.

(2) If a subpoena is delivered to FBIHQ rather than WMFO, subpoena is accepted by Office of the General Counsel.

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 6 - 27

(3) Subpoenas from Congressional Committees are accepted by WMFO if served there, or by Office of the General Counsel if served at FBIHQ. In either event, the division having jurisdiction of subject matter takes immediate action to secure facts and refers the matter with any necessary recommendations to the Attorney General or Deputy Attorney General.

(4) No supervisor shall accept a subpoena calling for appearance of a field office employee in a court proceeding. Should a Deputy U.S. Marshal attempt to leave a subpoena for such an employee, advise him/her of the office to which the employee is presently assigned.

EFFECTIVE: 09/09/94

6-13 OTHER CONTACTS WITH JUDICIAL OFFICIALS REGARDING PENDING CASES

Occasionally the FBI will obtain information regarding a case in litigation which should be brought to the attention of the court in which the case is pending. Examples include allegations regarding jury tampering, perjury and coercion of a witness. When this is required, care should be taken that it be accomplished in a way which avoids any appearance that the FBI is attempting to improperly influence the administration of justice. If at all possible, a Government attorney should convey the information to the court. If the case is in Federal court, the appropriate attorney would normally be from the local USA's office. If the case is pending in state court, then a local prosecutor should probably be utilized to convey the information, but the action should still be coordinated with the USA's office. In no event should FBI employees have contact with court personnel regarding a pending case unless a Government attorney is present. If for any reason it is believed that the above instructions cannot or should not be complied with, FBIHQ should be contacted for guidance.

EFFECTIVE: 05/26/89

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 6 - 28

6-14 BRIEFING MATERIAL PREPARED FOR PRESENTATION OUTSIDE THE
FBI

Briefing material prepared for presentation outside the FBI or testimony by Bureau officials should include the name and initials of the senior Bureau official approving the material and the date it was prepared. Additionally, divisions responsible for the preparation of the material are required to maintain records reflecting the source of the information used in the preparation of the briefing material and the names of the individuals who drafted the material.

EFFECTIVE: 05/26/89

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 7 - 1

SECTION 7. INTERVIEWS

7-1 USE OF CREDENTIALS FOR IDENTIFICATION | (See Legal Handbook
for Special Agents, 7-17.) |

Credentials 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: 01/30/97

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

EFFECTIVE: 01/08/79

7-2.1 Thoroughness and Precautions During Interviews | (See
LHBSA, 7-2.1.) |

(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

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 7 - 2

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, an electronic communication 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: 12/20/96

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

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 7 - 3

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

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 7 - 4

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

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 7 - 5

channelizing|electronic communications|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: 12/20/96

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

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 7 - 6

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

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 7 - 7

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

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 7 - 8

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, an electronic communication (EC) is sent out the same day to another field office or FBIHQ setting forth the essential facts of the complaint. FD-71 is a letter-size preinserted carbon white form or an FD-71 macro 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: 06/12/97

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.

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 7 - 9

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.

Sensitive

**Manual of Investigative Operations and Guidelines
Part II**

PAGE 7 - 10

EFFECTIVE: 01/31/78

**Sensitive
PRINTED: 02/18/98**

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 8 - 1

SECTION 8. DESCRIPTIONS OF PERSONS

8-1 POLICY FOR DESCRIPTION OF PERSONS

|(1)| The best available descriptions of all subjects, suspects and all victims shall be included in the first reports written after the descriptions are obtained, and supplemented later. When a subject, suspect or victim is interviewed, a complete description must be obtained and recorded. No word or phrase is to be used in descriptions in any report or communication which can be regarded as objectionable or offensive by any race, creed, or religious sect. The following or similar phrases should not be used: "Jewish Accent," "Polish Jew," "Irish Catholic," "English Methodist," etc.

|(2)| There are three possible ways in which Agents may obtain physical descriptions:

|(a)| From the records of other agencies.

|(b)| From personal observation and/or interview of the person. Where possible, a description should always be obtained.

|(c)| From other individuals who know or have seen the person. Considerable assistance can be given to individuals in obtaining descriptions from them by one thoroughly familiar with all the items to be considered in compiling a physical description.

EFFECTIVE: 05/28/85

8-1.1 Specific Descriptive Items

EFFECTIVE: 05/28/85

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 8 - 2

8-1.1.1 Names and Aliases

(1) The person should be asked his/her full name, first, middle and last, and requested to spell each name completely.

(2) The person should be asked if he/she has ever been known under any other name.

(3) Initials are not generally considered as aliases unless the circumstances of a particular case so indicate.

(4) All nicknames should be obtained and included.

EFFECTIVE: 05/28/85

8-1.1.2 Sex

The sex of the person described should always be designated as certain names carry both a feminine and masculine connotation.

EFFECTIVE: 05/28/85

8-1.1.3 Race

EFFECTIVE: 05/28/85

8-1.1.4 Age

(1) The date and place of birth should be obtained.

(2) If not obtained from the person described, it may be obtained from state records, baptismal records, family Bibles, etc.

EFFECTIVE: 05/28/85

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 8 - 3

8-1.1.5 Residences

- (1) The present address of the person should be obtained.
- (2) Obtain former residences and approximate dates in connection therewith.
- (3) If no present address indicated, the residence most regularly frequented; e.g., father's address.

EFFECTIVE: 05/28/85

8-1.1.6 Height

The most accurate method of obtaining height is from actual measurement. However, in many instances this method is not possible. In this case an approximate height of person will suffice.

EFFECTIVE: 01/31/78

8-1.1.7 Weight

- (1) If available, the person should be weighed and appropriate consideration should be given to allow for clothing. In the absence of being able to weigh the person, an approximate weight should be included in the description.

EFFECTIVE: 01/31/78

8-1.1.8 Build

Extra large, large, medium, slender, stocky, short, heavy, obese, etc.

EFFECTIVE: 01/31/78

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 8 - 4

8-1.1.9 Hair

(1) Color: Black, brown (dark, medium, light, chestnut), red (auburn, carrot top), sandy, blond, grey (iron grey, mixed grey, silver), white.

(2) Texture: Fine, coarse, kinky, curly, wavy, straight.

(3) Quantity: Thick, thin, bald (describe type of).

(4) Style: Parted on left, right or middle, pompadour, unkempt, Afro, etc.

(5) Hairline: Pointed, straight, rounded.

EFFECTIVE: 01/31/78

8-1.1.10 Forehead

(1) Slope (profile view): Receding, medium, vertical, prominent or bulging.

(2) Height: Low, medium, high.

(3) Width: Narrow, medium, wide.

(4) Peculiarities: Wrinkles (horizontal, vertical, or combined).

EFFECTIVE: 01/31/78

8-1.1.11 Eyes

(1) Color: Blue, grey, hazel, green, brown, maroon, black.

(2) Size: Small, large.

(3) Peculiarities: Protruding, sunken, shortsighted, squinted, blinking, cross-eyed, wide set, close set, long lashes, cataract, watery, bloodshot, whites discolored, scars on whites of eyes, wears glasses, or contact lenses.

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 8 - 5

(4) Eyebrows: Color differs from hair, heavy, arched, united, oblique upward, oblique downward.

EFFECTIVE: 01/31/78

8-1.1.12 Nose

(1) Line (profile): Straight, concave, hooked, Roman, sinuous.

(2) Base: Horizontal, upward, downward.

(3) Projection: Small, medium, large.

(4) Length: Short, medium, long.

(5) Bridge curve: Flat, medium, recessed or deep.

(6) Width of bridge: Wide, medium, narrow.

(7) Width of base: Wide, medium, narrow.

(8) Peculiarities: Crushed, twisted, dilated nostrils, pointed, bulbous.

EFFECTIVE: 01/31/78

8-1.1.13 Mouth

(1) Size: Wide, medium, narrow.

(2) Shape: Habitually open, corners elevated or depressed, tightly closed.

(3) Lips: Long upper, short upper, thin, thick, upper prominent, lower prominent or pendent, pouting.

EFFECTIVE: 01/31/78

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 8 - 6

8-1.1.14 Chin

(1) Profile view: Projecting or prominent, receding, vertical, pointed, long, short, double chin, flabby throat.

(2) Front view: Wide, square, round, dimple, cleft, bulbous.

EFFECTIVE: 01/31/78

8-1.1.15 Teeth

Protruding upper or lower, irregular, gold visible, some missing, stained, decayed, false, buck.

EFFECTIVE: 01/31/78

8-1.1.16 Ears

(1) Size: Large, medium, small.

(2) Shape: Rectangular, oval, round, triangular.

(3) Position on head: Low or high.

(4) Slope (profile): Vertical, receding.

(5) Slope (full-faced): Protruding, medium close set.

(6) Upper rim: Large, small, medium, flat.

(7) Lower rim: Large, small, medium, flat.

(8) Lobe: Long, medium, short, wide, pointed, rounded, descending, no lobes or squared.

EFFECTIVE: 01/31/78

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 8 - 7

8-1.1.17 Neck

Short, long, thin, thick, prominent Adam's apple, goiter, prominent jaws.

EFFECTIVE: 01/31/78

8-1.1.18 Head

(1) Shape: Area above ears large, area above ears small, back of head bulges, back of head flat, top of head flat, top of head pointed, small for body, large for body.

(2) Angle: Holds head to the right or to the left, forward or backward.

EFFECTIVE: 01/31/78

8-1.1.19 Face

(1) Complexion: Pale, fair, medium, dark, light brown, medium brown, dark brown, sallow, ruddy, pock-marked, pimpled, freckled, weather-beaten, swarthy, tanned.

(2) Shape: Round, square, oval, long, broad, heart-shaped, prominent cheek bones, sunken cheeks, flabby, drawn, bony.

(3) Expression: Meditative, dull, nervous, stern, scheming, smiling, suffering, frightened, sad, distorted, innocent, vivacious.

EFFECTIVE: 01/31/78

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 8 - 8

8-1.1.20 Voice

- (1) Quantity: Soft, low, loud, harsh.
- (2) Quality: Refined, vulgar, foreign accent, lisping, stuttering, stammering, throaty, husky, southern accent, effeminate.
- (3) Rate of speech: Rapid, slow, precise.

EFFECTIVE: 01/31/78

8-1.1.21 Legs and Hands

Short, medium, long, skinny, fat, straight, knock-kneed, bowlegged, right or left handed, amputee, etc.

EFFECTIVE: 01/31/78

8-1.1.22 Gait

Trudging, energetic, swaying, light, graceful, calm and leisurely, long steps, short steps, stiff, pigeon-toed, waddles, slew-footed, clubfooted.

EFFECTIVE: 01/31/78

8-1.1.23 Education

Illiterate, noticeably poor English, noticeably good English, grammar school, high school, business school, night school, college, apparently well-educated.

EFFECTIVE: 01/31/78

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 8 - 9

8-1.1.24 Scars

(1) Scars, particularly on the face and hands, should be fully described as to location, shape, size, and color.

(2) Moles, warts, cysts, blackheads, tattoos.

EFFECTIVE: 01/31/78

8-1.1.25 Peculiarities

(1) Peculiarities of any type are most important in the description of persons.

(2) Peculiarities, such as mannerisms, habits, impressions, regardless of how seemingly unimportant should be included.

(3) The following should be considered under peculiarities: senile, invalid, paralytic, feeble-minded, deaf, dumb, totally blind, deformities, amputations.

EFFECTIVE: 01/31/78

8-1.1.26 Occupation

The specific occupation should be stated in all instances.

EFFECTIVE: 01/31/78

8-1.1.27 Marital Status

(1) The status of a person should be stated as married, single, divorced, separated, widow, widower, or common-law.

(2) If married, the full and complete name of the wife, including the maiden name, should be set forth when known.

(3) Information as to the date and place of the marriage, including the name of the minister who performed the ceremony, should

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 8 - 10

be included if possible.

(4) If divorced, the time, place, and the grounds should be obtained.

EFFECTIVE: 01/31/78

8-1.1.28 Close Relatives

(1) The names and addresses of close relatives should be obtained when possible. Close relatives are parents, spouse, brothers and sisters, and adult offspring. Special instances, such as more distant relatives who occupy same residence as applicant, will require broadening of this definition.

(2) Where pertinent, list close friends and associates.

EFFECTIVE: 01/31/78

8-1.1.29 Nationality

(1) The nationality or extraction of the individual being described may sometimes be very important.

(2) The country of birth should be obtained.

EFFECTIVE: 01/31/78

8-1.1.30 Fingerprint Classification

This should be set forth whenever known.

EFFECTIVE: 01/31/78

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 8 - 11

8-1.1.31 FBI or Police Number

These numbers should be set forth whenever they are available.

EFFECTIVE: 01/31/78

8-1.1.32 Social Security Number

This number should be included when available. (See MIOG, I, 190-8.1(2)).

EFFECTIVE: 01/31/78

8-1.1.33 Other Identifying Numbers

Alien registration number, military service number, driver's license number, etc., should be set forth when known.

EFFECTIVE: 01/31/78

8-1.1.34 Identification Record Showing Source

The source for descriptive data will be furnished, if necessary, for clarification, such as former address which only sets forth street and city or state. The source which furnished the fingerprint, for example, Police Department, Albany, N.Y., will be identified and, if additional clarification is necessary, that agency can be contacted.

EFFECTIVE: 01/31/78

XXXXXX
XXXXXX
XXXXXXFEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET13

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 552Section 552a☐ (b)(1)☐ (b)(7)(A)☐ (d)(5)☒ (b)(2)☐ (b)(7)(B)☐ (j)(2)☐ (b)(3)☐ (b)(7)(C)☐ (k)(1)☐ (b)(7)(D)☐ (k)(2)☒ (b)(7)(E)☐ (k)(3)☐ (b)(7)(F)☐ (k)(4)☐ (b)(4)☐ (b)(8)☐ (k)(5)☐ (b)(5)☐ (b)(9)☐ (k)(6)☐ (b)(6)☐ (k)(7)

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

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

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

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

Pages were not considered for release as they are duplicative of _____

Page(s) withheld for the following reason(s): _____

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

MIOG Pt II Sec 9

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

XXXXXX
XXXXXX
XXXXXX

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 10 - 1

SECTION 10. RECORDS AVAILABLE AND INVESTIGATIVE TECHNIQUES

10-1 INTRODUCTION

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

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

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

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

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

EFFECTIVE: 01/21/86

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 10 - 2

10-2 RECORDS AVAILABLE

[REDACTED]
Biographic Directories
[REDACTED]
[REDACTED]
[REDACTED]

City Directory
Closed and Pending Files
Court System
[REDACTED]

|| Department of Veterans Affairs |
[REDACTED]
[REDACTED]

Field Office Special Services List
[REDACTED]
[REDACTED]

b2, b7E

Government Agencies
[REDACTED]
[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]
[REDACTED]

Probation and Parole Offices

Public Libraries
[REDACTED]
[REDACTED]

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 10 - 3

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

Telephone Directory

Unemployment Agencies, Federal and State

Voter Records

b2, b7E

EFFECTIVE: 05/25/90

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

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

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 10 - 4

Collection of Evidence in
Rape Cases

see MIOG, Part II, 13-8.2.5

Fluorescent Powders
and Other Marking Materials

see MIOG, Part II, 13-15.2

Plastic Cast Impression of
Stamped Numbers in Metal

see MIOG, Part II, 13-13.3.1

Restoration of Obliterated
Markings

see MIOG, Part II, 13-14.2
(10)

Shoe/Tire Tread Cast and Lifts

see MIOG, Part II, 13-19

Hypnosis

see MIOG, Part II, 10-12

Identification Orders

see MIOG, Part II, 21-25

Informants

see MIOG, Part I, 137

Investigative Information Services
Data Bases For Use In Investigations

see MIOG, Part II, 10-17

Mail Covers

see MIOG, Part II, 10-6

National Crime Information Center

see MAOP, Part II, 7

Pen Registers

see MIOG, Part II, 10-10.7

| Photographic Examinations

see MIOG, Part II, |13-7.6|

Photographic Surveillances

see MIOG, Part II, 13-7.5

Polygraph Examinations

see MIOG, Part II, 13-22

Stop Notices

see MIOG, Part II, 10-7

Surveillance Techniques

see MIOG, Part II, 9

Telephone Toll Records

see MIOG, Part II, 10-8

Title III Coverage

see MIOG, Part II, 10-9.10

Undercover Activities

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 10 - 5

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

EFFECTIVE: 07/25/97

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

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

EFFECTIVE: 06/01/94

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

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

(2) Detailed instructions for conducting name searches

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 10 - 6

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

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

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

EFFECTIVE: 05/13/96

10-6 MAIL COVERS

EFFECTIVE: 03/09/81

10-6.1 United States Postal Service (USPS) Regulations

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

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

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

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 10 - 7

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

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

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

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

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

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 10 - 8

EFFECTIVE: 03/09/81

10-6.2 Policy

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

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

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

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

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

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

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

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 10 - 9

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

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

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

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

EFFECTIVE: 05/09/95

10-6.3 Requesting Approval

EFFECTIVE: 05/09/95

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 10 - 10

10-6.3.1 Fugitive or Criminal Cases

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

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

(a) Brief background of the case.

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

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

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

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

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

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

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

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

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

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

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 10 - 11

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

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

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

EFFECTIVE: 05/09/95

10-6.3.2 National Security Cases

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

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

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

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

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 10 - 12

Room 3417

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

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

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

EFFECTIVE: 02/16/89

10-7 STOP NOTICES

EFFECTIVE: 06/10/88

10-7.1 Definition

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

EFFECTIVE: 06/10/88

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 10 - 13

10-7.2 Placement of Stops

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

b2, b7E

EFFECTIVE: 06/10/88

10-7.3 Indexing Stops

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

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

EFFECTIVE: 06/10/88

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 10 - 14

10-7.4 Removal of Stops

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

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

EFFECTIVE: 06/10/88

10-7.5 Types of Stops

EFFECTIVE: 06/10/88

10-7.5.1 [REDACTED]

Stop notices are placed by letter to [REDACTED]

b2, b7E

EFFECTIVE: 06/10/88

10-7.5.2 Immigration and Naturalization Service (INS)

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

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

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE - 10 - 15

areas open to travelers.

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

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

b7E per INS

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

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

b7E per INS

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

The FD-315 lists [REDACTED]

(a) [REDACTED]

(b) [REDACTED]

(c) [REDACTED]

b7E
per
INS

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 10 - 16

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

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

EFFECTIVE: 05/25/90

[REDACTED]

[REDACTED]

[REDACTED]

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 10 - 17

[REDACTED]

[REDACTED]

[REDACTED]

EFFECTIVE: 04/08/96

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

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

EFFECTIVE: 01/22/90

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 10 - 18

10-8.1 Contents of Electronic Communications in Electronic Storage

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

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

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

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

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 10 - 19

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

EFFECTIVE: 10/23/95

10-8.2 Access to Transactional Information

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

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

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

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

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

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

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 10 - 20

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

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

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

(c) Notification to Telephone Subscriber

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

| (2) | On-line Computer Network Records

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

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 10 - 21

USC, Section 2703(c)).

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

(3) Video Tape Rental or Sales Records

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

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

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

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

This type of information was specifically not included in the

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 10 - 22

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

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

EFFECTIVE: 10/23/95

10-9 ELECTRONIC SURVEILLANCE (ELSUR) PROCEDURES AND
REQUIREMENTS

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

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

EFFECTIVE: 04/24/89

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 10 - 23

10-9.1 Definitions

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

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 10 - 24

matters.

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

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

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

EFFECTIVE: 04/24/89

10-9.2 Instructions for Maintaining ELSUR Indices

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

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

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 10 - 25

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

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

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

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

EFFECTIVE: 02/16/89

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 10 - 26

10-9.3 Requests for ELSUR Checks

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

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

EFFECTIVE: 04/18/85

10-9.4 ELSUR Searching Procedures

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

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

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 10 - 27

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

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

(4) Where the 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 relating to consensual monitoring ELSURs, the field division should always advise if the ELSUR coverage in question is still pending or a covert operation not yet disclosed.

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

EFFECTIVE: 04/18/85

10-9.5 Transmitting ELSUR Material to FBIHQ

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

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 10 - 28

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

Director, FBI
ELSUR Index
FBIHQ

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

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

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

EFFECTIVE: 06/18/87

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 10 - 29

10-9.6 Retention of ELSUR Files and Related Records

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

EFFECTIVE: 06/18/87

10-9.7 Marking File Cover "ELSUR"

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

EFFECTIVE: 12/10/93

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

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

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 10 - 30

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

EFFECTIVE: 12/21/94

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

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

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

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

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

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

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

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

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 10 - 31

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

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

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

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

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

CHAIN OF CUSTODY

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

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

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

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

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 10 - 32

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

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

EFFECTIVE: 10/16/96

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

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

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

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

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 10 - 33

EFFECTIVE: 10/18/88

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

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

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

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

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

(c) Presidential assassination, kidnapping, or assault;

(d) Obstruction of justice;

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

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

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

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

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 10 - 34

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

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

(3) Title III Applications - Approval Levels

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

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 10 - 35

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

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

1. applications requesting Title III interceptions based upon "relaxed specificity" (i.e., applications in which the requirement to specify those facilities from which, or the place where, the communication is to be intercepted has been eliminated--so called "roving" interceptions) under provisions of Title 18, USC, Section 2518(11) (a) and (b);
2. situations involving significant privilege issues or First Amendment concerns (e.g., attorney-client privilege or other privileged conversations, or interception of news media representatives);
3. situations involving significant privacy concerns (e.g., interceptions of conversations in a bedroom or bathroom, etc.);
4. applications concerning Domestic Terrorism, International Terrorism, or Espionage cases;
5. in any other situation deemed appropriate by either the Assistant Director, CID, or Assistant Director, NSD.

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

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

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 10 - 36

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

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

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

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

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

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

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

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 10 - 37

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

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

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

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

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

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 10 - 38

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

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

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

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

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 10 - 39

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

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

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

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

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

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 10 - 40

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

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

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

b2
b7E

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

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

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 10 - 41

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

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

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

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 10 - 42

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

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

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

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

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 10 - 43

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

EFFECTIVE: 02/28/97

10-9.11 Emergency Provisions, Title III Criminal Matters

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

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

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

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

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

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

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 10 - 44

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

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

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

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

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 10 - 45

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

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

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

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

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 10 - 46

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

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

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 10 - 47

surveillance.

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

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

b2
b7E

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

EFFECTIVE: 02/28/97

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 10 - 48

10-9.11.1 Form 2 Report

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

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

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

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

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

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 10 - 49

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

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

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

EFFECTIVE: 06/18/87

10-9.11.2 Completion of Form 2 Report

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

(1) "COURT AUTHORIZING OR DENYING THE INTERCEPT"

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

(2) "SOURCE OF APPLICATION"

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

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

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 10 - 50

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

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

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

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

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

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

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

(4) "DURATION OF INTERCEPT"

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

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 10 - 51

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

(5) "TYPE OF INTERCEPT"

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

(6) "PLACE"

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

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

(7) "INSTALLATION"

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

(8) "DESCRIPTION OF INTERCEPTS"

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

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

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

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

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

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 10 - 52

if intercepted more often);

(e) the estimated number of communications intercepted, and

(f) the estimated number of incriminating communications intercepted.

(9) "COST"

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

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

(10) "RESULTS"

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

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 10 - 53

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

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

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

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

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

(11) "COMMENTS AND ASSESSMENT"

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

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

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 10 - 54

EFFECTIVE: 06/18/87

10-9.11.3 Submissions of Form 2 Report to FBIHQ

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

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

Director, FBI
ELSUR Index
FBIHQ

The airtel will include the following information:

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

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

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

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

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

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 10 - 55

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

EFFECTIVE: 06/18/87

10-9.11.4 Supplemental Form 2 Reports

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

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

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

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

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 10 - 56

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

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

EFFECTIVE: 06/18/87

10-9.12 ELSUR Indexing in Title III Criminal Matters

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

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

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 10 - 57

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

Example of Principal Card

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

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

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

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 10 - 58

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

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

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

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

2. Proprietary Interest card for filing by
telephone number.

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

3. Proprietary Interest card for filing by
address.

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

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 10 - 59

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

4. Proprietary Interest card for filing by
facility.

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

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

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

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

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 10 - 60

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

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

3. Proprietary Interest card for filing by telephone number.

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

4. Proprietary Interest card for filing by address.

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

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 10 - 61

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

facility. 5. Proprietary Interest card for filing by

- 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

name. 1. Proprietary Interest card for filing by

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

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 10 - 62

address

2. Proprietary Interest card for filing by the

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

facility.

3. Proprietary Interest Card for filing by

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

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

name.

1. Proprietary Interest card for filing by

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

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 10 - 63

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

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

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

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

1. Proprietary Interest card for filing by
name.

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

2. Proprietary Interest card for filing by the
address.

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

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 10 - 64

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

3. Proprietary Interest card for filing by the facility.

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

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

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

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 10 - 65

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

Example of Overhear Card in Title III Matters

Overhear Title III, TESUR or MISUR coverage.

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

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

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

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 10 - 66

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

EFFECTIVE: 06/06/86

10-9.13 Marking of Recordings for Identification

See Part II, 16-8.2.3 of this manual.

EFFECTIVE: 09/22/87

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

See Part II, 16-7.3.4 of this manual.

EFFECTIVE: 09/22/87

10-9.15 Submission of Recordings

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

EFFECTIVE: 10/16/96

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 10 - 67

10-9.16 Transcription of Recordings

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

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

EFFECTIVE: 04/19/91

10-10 CONSENSUAL MONITORING - CRIMINAL MATTERS

EFFECTIVE: 04/19/91

10-10.1 Use of Consensual Monitoring in Criminal Matters

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

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

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

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 10 - 68

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

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

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

EFFECTIVE: 02/28/97

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

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

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

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

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 10 - 69

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

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

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

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

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

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 10 - 70

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

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

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

EFFECTIVE: 09/17/97

Sensitive
PRINTED: 02/18/98

Manual of Investigative Operations and Guidelines
Part II

[illegible]

Sensitive
PRINTED: 02/18/98

XXXXXX
XXXXXX
XXXXXXFEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

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

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

Section 552Section 552a☐ (b)(1)☐ (b)(7)(A)☐ (d)(5)☐ (b)(2)☐ (b)(7)(B)☐ (j)(2)☐ (b)(3)☐ (b)(7)(C)☐ (k)(1)☐ (b)(7)(D)☐ (k)(2)☐ (b)(7)(E)☐ (k)(3)☐ (b)(7)(F)☐ (k)(4)☐ (b)(4)☐ (b)(8)☐ (k)(5)☐ (b)(5)☐ (b)(9)☐ (k)(6)☐ (b)(6)☐ (k)(7)

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

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

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

Pages were not considered for release as they are duplicative of

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

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

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

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 10 - 73

[REDACTED]

[REDACTED]

[REDACTED]

EFFECTIVE: 05/10/96

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

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

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 10 - 74

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

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

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

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

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

(c) The interception relates to an investigation of

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 10 - 75

a federal law enforcement official;

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

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

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

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

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 10 - 76

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

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

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

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

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

(3) The Director has delegated authority to the SAC to approve NTCM of verbal communications except when the circumstances listed in MIOG, Part II, 10-10.3 (1) above, are present. SACs may authorize NTCM usage for the duration of nonsensitive investigations so long as the circumstances under which the authority was granted (i.e., the subject matter, the consenting party or parties to the interception, and the judicial district wherein monitoring will take place) do not substantially change--the authorization will remain valid. Where such changes are noted, consideration should be given by the SAC to determine whether or not the NTCM authority should continue or new authority obtained. Where new authority is obtained, a new FD-759 must be completed.

(4) Consensual monitoring conducted outside the division

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 10 - 77

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

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

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

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

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

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

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 10 - 78

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

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

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

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

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

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

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 10 - 79

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

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

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

EFFECTIVE: 09/17/97

10-10.4 Deleted

EFFECTIVE: 12/16/88

10-10.5 ELSUR Indexing in Consensual Monitoring Matters

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

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 10 - 80

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

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

Examples of Overhear Card in Consensual Monitoring
Matters

(a) Overhear Consensual Monitoring - Telephone

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 10 - 81

- | |
|---|
| <ul style="list-style-type: none">a. SMITH, JOHNb. 12-7-82c. AL CM# 10 (Telephone) or Consensual (Telephone)d. 182-111e. AL 182-1 |
|---|

(b) Overhear Consensual Monitoring - Nontelephone

- | |
|--|
| <ul style="list-style-type: none">a. SMITH, JOHNb. 12-7-82c. AL CM# 11 (Nontelephone) or Consensual
Nontelephone)d. 182-111e. 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:

- | |
|--|
| <ul style="list-style-type: none">a. SMITH, JOHNb. 12-7-82c. AL CM # 12 (Nontelephone) or Consensual
(Nontelephone)d. 182-111e. AL 182-11f. 00: BS 182-12 |
|--|

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

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 10 - 82

EFFECTIVE: 12/16/88

10-10.5.1 Administration of ELSUR Records Regarding Informants and Assets

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

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

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

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

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

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

(d) Neither the true name nor the informant symbol

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 10 - 83

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

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

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

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

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

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

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 10 - 84

EFFECTIVE: 10/16/96

10-10.6 Use of Consensual Monitoring in National Security Matters

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

EFFECTIVE: 12/05/85

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

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

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

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

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 10 - 85

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

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

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

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

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 10 - 86

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

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

EFFECTIVE: 10/23/95

10-10.7.1 Emergency Provisions

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

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

(a) an emergency situation exists that involves -

1. immediate danger of death or serious bodily injury to any person; or
2. conspiratorial activities characteristic of organized crime,

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

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 10 - 87

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

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

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

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

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

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 10 - 88

| not be obtained. |

EFFECTIVE: 01/22/90

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

b2
b7E
Electronic tracking devices, [REDACTED]
are called beepers. The two devices must be distinguished from each
other. This section addresses electronic tracking devices. [REDACTED]
[REDACTED] Generally speaking, tracking
devices are specifically excluded from Title III requirements because
of the manner in which they function and the limited privacy
implications related to their use (Title 18, USC, Section
2510(12)(D)). However, in those circumstances where a court order is
required, Title 18, USC, Section 3117 provides for extrajurisdictional
effect. That is, a court order issued by a judge or magistrate may
authorize the use of the device within the jurisdiction of the court
and outside that jurisdiction if the device is installed in that
jurisdiction. The Department of Justice has interpreted this section
to mean that such use is valid outside of the court's jurisdiction
both inside and outside the jurisdiction of the United States.

(1) On Vehicles

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

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

(2) Other Personal Property

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 10 - 89

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

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

EFFECTIVE: 02/27/95

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

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

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

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 10 - 90

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

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

EFFECTIVE: 05/08/95

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

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

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

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

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

b2
b7E

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 10 - 91

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

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

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

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

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

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

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

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

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 10 - 92

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

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

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

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

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

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 10 - 93

(5) Documentation of Consent

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

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

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

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

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

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 10 - 94

EFFECTIVE: 09/17/97

10-10.9.2 CCTV - ELSUR Records - Criminal Matters

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

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

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

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

EFFECTIVE: 12/10/93

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

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

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

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

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 10 - 95

| examples of | intercept records. |

EFFECTIVE: 05/08/95

10-10.9.4 CCTV - Preservation of the Original Tape Recording

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

EFFECTIVE: 09/22/87

10-10.10 Tape Recorders

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

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

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

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

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

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 10 - 96

or coerce; and

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

EFFECTIVE: 09/22/87

10-10.11 Radio Monitoring

EFFECTIVE: 09/22/87

10-10.11.1 [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Sensitive
PRINTED: 02/18/98

XXXXXX
XXXXXX
XXXXXXFEDERAL 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 552Section 552a☐ (b)(1)☐ (b)(7)(A)☐ (d)(5)☒ (b)(2)☐ (b)(7)(B)☐ (j)(2)☐ (b)(3)☐ (b)(7)(C)☐ (k)(1)☐ (b)(7)(D)☐ (k)(2)☒ (b)(7)(E)☐ (k)(3)☐ (b)(7)(F)☐ (k)(4)☐ (b)(4)☐ (b)(8)☐ (k)(5)☐ (b)(5)☐ (b)(9)☐ (k)(6)☐ (b)(6)☐ (k)(7)

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

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

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

Pages were not considered for release as they are duplicative of _____

Page(s) withheld for the following reason(s): _____

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

M106-Part II Page 10-97

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

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 10 - 98

b2
b7E
[REDACTED]
ELSUR indexing is required.

EFFECTIVE: 02/14/97

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

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

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

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

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 10 - 99

General Counsel, FBIHQ.

EFFECTIVE: 06/03/96

10-10.11.3 Cellular Telephones

Both the wire and radio portions of a cellular telephone conversation are specifically covered by Title III and a Title III court order must be obtained to intercept cellular communications. Noncontent information, such as cellular telephone ESN or MIN, cell site sector information, or other location type information may be considered "a record or other information pertaining to a subscriber" and, therefore, obtained from a telecommunications carrier pursuant to a court order under Title 18, USC, Section 2703(d), or pursuant to a warrant or consent of the subscriber or customer.

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

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

EFFECTIVE: 10/23/95

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 10 - 100

10-10.12 Approval for the Use of Technical Equipment

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

EFFECTIVE: 10/18/88

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

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

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

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

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

EFFECTIVE: 10/18/88

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 10 - 101

10-10.14 Review by Technical Advisor (TA)

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

EFFECTIVE: 10/18/88

10-10.15 Training for TTAs

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

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

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

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

EFFECTIVE: 10/18/88

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 10 - 102

10-10.16 [REDACTED]

(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

b2
b7E

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 10 - 103

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

(6) Further details as to [REDACTED] b2 b7E

EFFECTIVE: 01/22/90

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

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

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

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

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

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 10 - 104

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

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

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

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

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

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

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

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 10 - 105

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

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

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

EFFECTIVE: 02/14/97

10-10.17.1 Emergency Provisions

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

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

(a) an emergency situation exists that involves-

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

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

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 10 - 106

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

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

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

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

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 10 - 107

EFFECTIVE: 03/23/92

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

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

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

EFFECTIVE: 12/07/93

| 10-11.1 | Deleted |

EFFECTIVE: 10/18/93

| 10-11.2 | Deleted |

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 10 - 108

EFFECTIVE: 10/18/93

| 10-11.3 | Deleted |

EFFECTIVE: 10/18/93

| 10-11.4 | Deleted |

EFFECTIVE: 10/18/93

| 10-11.5 | Deleted |

EFFECTIVE: 10/18/93

| 10-11.6 | Deleted |

EFFECTIVE: 08/28/91

10-11.7 | Deleted |

EFFECTIVE: 08/28/91

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

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 10 - 109

EFFECTIVE: 08/28/91

| 10-11.9 | Deleted |

EFFECTIVE: 08/28/91

10-12 USE OF HYPNOSIS AS AN INVESTIGATIVE AID

EFFECTIVE: 02/16/89

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

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

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 10 - 110

participate in hypnotic interviews in non-Bureau cases.

EFFECTIVE: 03/21/96

10-12.2 Hypnotic Session

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

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

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

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

EFFECTIVE: 02/16/89

10-12.3 Role of Case Agent in Hypnotic Session

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

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 10 - 111

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

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

EFFECTIVE: 07/17/95

10-12.4 Hypnosis Evaluation

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

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

EFFECTIVE: 07/17/95

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 10 - 112

10-13 VISUAL INVESTIGATIVE ANALYSIS (VIA)

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

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

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

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

EFFECTIVE: 11/20/90

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 10 - 113

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

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

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

EFFECTIVE: 12/07/93

10-14.1 Types of Advance Funding Authority

Funds may be requested for the following investigative purposes:

EFFECTIVE: 11/23/87

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 10 - 114

10-14.1.1 Case Authority

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

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

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

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

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 10 - 115

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

EFFECTIVE: 12/07/93

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

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

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

EFFECTIVE: 12/07/93

10-14.1.3 FCI/Terrorist Informant Authority

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

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 10 - 116

EFFECTIVE: 12/07/93

10-14.1.4 Bribe of Public Officials Authority

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

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

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

EFFECTIVE: 12/07/93

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

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

EFFECTIVE: 02/14/97

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 10 - 117

10-14.1.6 Show and Buy-Bust Money Funding Authority

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

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

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

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

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

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

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

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

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

b2 b7E
(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.

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 10 - 118

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

b2, b7E

EFFECTIVE: 12/07/93

10-14.1.7 Deleted

EFFECTIVE: 05/25/90

10-14.2 Delivery of Advance

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

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

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

b2,
b7E

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

(b) Name and title of bank contact

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

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 10 - 119

| 194-5.6(1.) |

EFFECTIVE: 12/07/93

10-14.3 Accountability/Vouchering Requirements

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

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

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

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

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

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

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 10 - 120

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

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

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

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

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

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

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

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

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

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

Department of the Treasury - Federal Reserve Bank,

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 10 - 121

New York City, Treasury Department Code [REDACTED]
for credit to [REDACTED] b2

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

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

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

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

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

EFFECTIVE: 12/07/93

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

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

Sensitive

Manual of Investigative Operations and Guidelines
Part II.

PAGE 10 - 122

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

EFFECTIVE: 12/07/93

10-15 TRACING OF FIREARMS

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

EFFECTIVE: 08/28/91

10-16

2
NE



Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 10 - 123

62
b7E
EFFECTIVE: 08/28/91

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

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

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

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 10 - 124

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

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

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

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

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

(c) ASSET INFORMATION - Information concerning

b2
b7E

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

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

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

(e) [REDACTED]

b7D

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 10 - 125

b7D

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

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

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

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

(i) [REDACTED]

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

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

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 10 - 126

EFFECTIVE: 03/13/97

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 11 - 1

SECTION 11. TECHNIQUES AND MECHANICS OF ARREST

11-1 ARREST TECHNIQUES

EFFECTIVE: 05/10/82

11-1.1 General

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

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

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

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

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

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 11 - 2

EFFECTIVE: 05/10/82

11-1.2 Initial Approach

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

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

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

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

EFFECTIVE: 05/26/89

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 11 - 3

11-1.3 Search of the Person

EFFECTIVE: 05/26/89

11-1.3.1 Preliminary Search

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

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

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

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

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

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 11 - 4

them.

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

EFFECTIVE: 05/26/89

11-1.3.2 Final Search and Collection of Evidence

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

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

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

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 11 - 5

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

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

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

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

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

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

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

EFFECTIVE: 05/26/89

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 11 - 6

11-1.4 Transportation of Arrested Persons

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

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

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

EFFECTIVE: 05/26/89

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 11 - 7

11-1.5 Handcuffing

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

EFFECTIVE: 05/26/89

11-2 PROCEDURES FOR ARREST

EFFECTIVE: 05/26/89

11-2.1 Arrests and Searches

EFFECTIVE: 05/26/89

11-2.1.1 Types of Arrest Warrants

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

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

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

EFFECTIVE: 05/26/89

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 11 - 8

11-2.1.2 Authority to Serve Arrest Warrants

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

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

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

EFFECTIVE: 05/26/89

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 11 - 9

11-2.1.3 Summons and Subpoenas

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

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

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

EFFECTIVE: 05/26/89

11-2.1.4 Arrests Without Warrants

(1) Authority and Notification -

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

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

(2) Emergency Situations -

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

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 11 - 10

reasonable cause is the same as "probable cause."

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

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

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

EFFECTIVE: 05/26/89

11-2.1.5 Forcible Entry

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

EFFECTIVE: 01/31/78

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 11 - 11

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

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

EFFECTIVE: 06/28/94

11-2.2 Custody of Prisoners

EFFECTIVE: 01/31/78

11-2.2.1 Other Than District of Prosecution

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

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

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 11 - 12

necessary action.

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

EFFECTIVE: 01/31/78

11-2.2.2 Property of Prisoner

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

EFFECTIVE: 01/31/78

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

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

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

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

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

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 11 - 13

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

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

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

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

REPORT OF TEMPORARY RELEASE OF PRISONER

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

(U.S. Marshal or Deputy) _____

(Jud. Dist.) _____

EFFECTIVE: 05/10/82

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 11 - 14

11-2.3 Miscellaneous

EFFECTIVE: 05/10/82

11-2.3.1 Requests of Incarcerated Subjects

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

EFFECTIVE: 05/10/82

11-2.3.2 Medical Attention for Bureau Subjects

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

EFFECTIVE: 05/10/82

11-2.3.3 Arrest of Foreign Nationals

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

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 11 - 15

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

EFFECTIVE: 05/10/82

11-3 ROADBLOCKS

EFFECTIVE: 05/10/82

11-3.1 General

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

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

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

EFFECTIVE: 05/10/82

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 11 - 16

11-3.2 Roadblock Methods

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

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

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

b2
b7E

(2)

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

b2
b7E

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

b2
b7E

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 11 - 17

[REDACTED]

[REDACTED] (4) [REDACTED]

b2
b7E

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

EFFECTIVE: 05/10/82

11-4 RAIDS

EFFECTIVE: 05/10/82

11-4.1 SAC Responsibility

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

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 11 - 18

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

EFFECTIVE: 05/10/82

11-4.2 Elements of a Raid

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

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

EFFECTIVE: 05/10/82

11-4.3 Planning Raids

EFFECTIVE: 05/10/82

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 11 - 19

11-4.3.1 Raid Commander and Responsibilities

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

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

(3)

(4)

(5)

b2
b7E

EFFECTIVE: 05/10/82

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 11 - 20

11-4.3.2 Selection and Composition of the Raid Party

[REDACTED]

(1) [REDACTED]

b2
b7E

(2) [REDACTED]

EFFECTIVE: 05/10/82

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 11 - 21

11-4.3.3 Raid Orders

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

EFFECTIVE: 05/10/82

11-4.3.4 Equipment

[REDACTED]

b2
b7E

EFFECTIVE: 11/26/84

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 11 - 22

11-4.3.5 Assembly Location

(1)



(2)



b2
b7E

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

EFFECTIVE: 11/26/84

11-4.4 Approach to Raid Site

(1)



Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 11 - 23

[REDACTED]
(2) [REDACTED]
[REDACTED]

b2
b7E

EFFECTIVE: 02/20/90

11-4.5 Entering the Place to be Raided

EFFECTIVE: 02/20/90

11-4.5.1 Identification of Raid Party

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

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

(a) [REDACTED]
[REDACTED]

(b) [REDACTED]
[REDACTED]

b2
b7E

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 11 - 24

(c) [REDACTED]

b2
b7E

EFFECTIVE: 02/20/90

11-4.5.2 [REDACTED]

EFFECTIVE: 02/20/90

11-4.5.3 [REDACTED]

EFFECTIVE: 05/20/94

11-4.6 The Covering Party

EFFECTIVE: 02/20/90

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 11 - 25

11-4.6.1 Duties of the Covering Agents

(1) [REDACTED]

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

(3) [REDACTED]

(4) [REDACTED]

(5) [REDACTED]

b2
b7E

EFFECTIVE: 02/20/90

11-4.7 Post Raid Responsibilities

EFFECTIVE: 02/20/90

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 11 - 26

11-4.7.1 Arrest of Subjects

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

EFFECTIVE: 02/20/90

11-4.7.2 Raid Site Security

b2
b7E

EFFECTIVE: 02/20/90

11-4.7.3 Publicity

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

EFFECTIVE: 01/22/90

11-4.8 Miscellaneous

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

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 11 - 27

EFFECTIVE: 01/22/90

11-4.9 Photograph of Subjects

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

EFFECTIVE: 04/08/96

11-5 EMERGENCY AND PURSUIT DRIVING

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

(2) FBI vehicles responding to emergency or pursuit

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 11 - 28

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

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

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

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

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

EFFECTIVE: 01/22/90

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 12 - 1

SECTION 12. FIREARMS

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

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

EFFECTIVE: 04/07/97

12-1.1 SAC Responsibility

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

EFFECTIVE: 04/07/97

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

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

EFFECTIVE: 04/07/97

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 12 - 2

12-2 UTILIZATION OF FIREARMS

EFFECTIVE: 05/20/94

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

(1) POLICY TEXT:

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

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

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

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

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

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

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

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 12 - 3

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

(3) DEFINITIONS

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

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

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

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

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

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

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

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

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 12 - 4

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

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

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

(3) APPLICATION OF DEADLY FORCE

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

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

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

EFFECTIVE: 04/07/97

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

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 12 - 5

EFFECTIVE: 04/07/97

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

EFFECTIVE: 04/07/97

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

EFFECTIVE: 04/07/97

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

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

b2
b1E
SAs are authorized to be armed when off-duty.

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

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

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 12 - 6

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

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

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

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

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

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

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

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

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

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

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 12 - 7

EFFECTIVE: 04/07/97

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

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

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

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

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

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

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

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

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

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

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 12 - 8

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

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

EFFECTIVE: 04/07/97

12-3 ISSUED WEAPONS

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

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

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

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

b2
b7E

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

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 12 - 9

EFFECTIVE: 04/07/97

12-3.1 Distribution of Firearms

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

(1) Handguns -

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

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

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

(2) Shotguns

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

b2
b7E

(3) Rifles

(a) Sniper rifles and rifles capable of fully automatic fire are authorized for use only by current firearms instructors, [REDACTED] who are qualified in the weapon's use. Any exception to this requirement must be requested in writing and approved by the Unit Chief, FTU.

b2
b7E

(b) Any SA qualified in the use of a rifle may use a

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 12 - 10

rifle capable of automatic fire if it is equipped with a fire selector lock to prevent fully automatic fire.

(c) The SAC or designee may authorize the removal of the selector locks during emergency situations. This authority may not be delegated. Upon termination of the emergency situation the SAC must ensure the selector locks are properly reattached to the weapons.

(d) Bureau rifles should be sighted in during firearms training sessions to ensure accuracy at operationally appropriate distances.

(4) Submachine Guns

(a) The Bureau is generally equipped with Heckler and Koch (H&K) submachine guns.

(b) Submachine guns may only be used operationally by current firearms instructors, [REDACTED] currently qualified in their use. The MP5-10/A2 which is capable of a two-shot burst may be utilized by any Agent who is currently qualified on that weapon.

b2
b7E

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

(5) Carbines

(a) The Bureau is equipped with Heckler and Koch (H&K) and Colt carbines.

(b) All SAs are authorized to use the H&K MP5SF and Colt M16 series of carbines, provided they are currently qualified with the weapon. The weapon must be equipped with a fire control selector lock if capable of fully automatic fire.

EFFECTIVE: 04/07/97

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 12 - 11

12-4 PERSONALLY OWNED WEAPONS

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

(2) SAs are authorized up to two POW handguns in addition to a Bureau-issued pistol or revolver. Agents may elect to have three POW handguns but the Bureau-issued handgun must be returned to the FBI Academy Gun Vault and the Bureau-issued gun removed from the SA's property record. POW handguns authorized for duty may be any combination of pistols and/or revolvers.

(3) SAs are authorized one POW 12-gauge shotgun with a barrel length between 18 and 20 inches and fixed stock, provided the SA is qualified with that weapon.

(5) The Firearms Training Unit (FTU) and FBI Academy Gun Vault maintain an up-to-date list of firearms approved for official use as well as accessories authorized for these firearms. Additionally, the FTU will provide the list of approved handguns, shotguns and rifles/carbines with approved accessories to the field division PFIs in the Annual Field Firearms Program communication. Agents should consult with the PFI or the FTU BEFORE purchasing a firearm for official use.

(6) Before approval of a POW is granted, the weapon must be inspected by the FBI Academy Gun Vault for functional reliability, accuracy and serviceability.

(7) Approval for POWs will only be granted for currently manufactured models. Once a weapon is discontinued by a manufacturer, that model will no longer be approved. Previously approved weapons in this category will continue to be approved until removed by submission of FD-431. Likewise, once a weapon no longer approved is removed from an Agent's FD-431, that weapon will not be approved for official use by another Agent.

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

(9) No POW will be approved for use which requires an application for National Firearms Act (NFA) approval from the Bureau of Alcohol, Tobacco and Firearms (ATF). Those weapons that apply as listed in Title 18, Section 5845 are as follows:

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 12 - 12

- (a) A shotgun having a barrel or barrels of less than 18 inches in length;
- (b) A rifle having a barrel or barrels of less than 16 inches in length;
- (c) Any weapon mentioned in (a) or (b) above which has an overall length of less than 26 inches;
- (d) Any machine gun (fully automatic weapon);
- (e) Any silencer or suppressed weapon.

(10) |POWs must have a factory finish from the manufacturer. The Gun Vault will be responsible for blued or parkerized finishes only. If the condition of the finish renders the weapon unserviceable, authority to carry that weapon may be withdrawn. Refinishing other than bluing or parkerizing must be completed by the manufacturer at the Agent's own expense.

| (11) | Approval Procedure

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

(b) An SA seeking weapon approval will submit |an| FD-431 in quadruplicate to PFI with the weapon for |inspection and initial| approval.

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

(d) |The|PFI (or|a designated|firearms instructor), after signing the FD-431, will submit the forms for SAC approval and transmittal, returning three copies of the FD-431 to|the|FBI Academy Gun Vault WITH THE WEAPON. |The submitted FD-431 MUST contain the PFI's signature and SAC or designee's initials. |One copy of the FD-431 should be maintained as a field office tickler copy. Pistols must be accompanied by four factory|magazines. Rifles|must be submitted with a minimum of two factory magazines.

(e) |The aforementioned approval process may be modified when an Agent purchases an approved firearm directly from a manufacturer who will ship the weapon directly to the FBI Academy Gun

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 12 - 13

Vault. The FD-431 is completed by the requesting Agent, approved by the PFI and SAC, and three copies forwarded to the FBI Academy Gun Vault. The FD-431 will then be matched with the gun received from the manufacturer.

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

(g) The Gun Vault will inspect the firearm for physical condition and test fire the weapon for functional integrity.

(h) If the weapon meets all necessary inspection prerequisites, the firearm will be returned to the submitting PFI with the FD-431 marked "approved." The Bureau will not supply parts needed to make a weapon acceptable for approval.

(i) SAs must fire a qualifying score on the current qualification course for the weapon in question and appropriately record scores BEFORE authority to carry the weapon will be granted by the PFI.

(j) Once the approval procedure is complete, the SA is authorized to carry this POW. The approval copy of FD-431 should be placed in the SA's personnel file.

(k) Any reason for disapproval of a weapon will be explained in full on the FD-431 which will be returned with the weapon to the submitting PFI.

(12) To remove a POW from Bureau-approved status, properly execute Form FD-431 in quadruplicate and forward three copies to Quantico. Upon receipt of the return copy from Quantico, the PFI will delete this weapon from the Agent's firearms training records.

(13) No firearm is authorized for official use unless it is physically inspected and authorized by the Gun Vault (i.e., seized weapons, personal purchases, etc.).

EFFECTIVE: 04/07/97

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 12 - 14

| 12-4.1 | Revised and Moved to 12-4 |

EFFECTIVE: 04/07/97

12-5 MAINTENANCE AND REPAIRS

(1) SAs are personally responsible for security and maintenance of all firearms and other expendable and nonexpendable related equipment assigned to them.

(2) Alterations, repairs, and refinishing of assigned firearms must be conducted by FBI gunsmiths. Exceptions include refinishing by manufacturers or other contractors whose use has been requested in writing and approved by the Firearms Training Unit (FTU) in advance.

(3) After-market parts or options will not be approved unless authority is requested in writing and approved by the FTU Unit Chief. Questions regarding the installation of after-market parts on a Bureau-approved firearm should be resolved PRIOR to purchase of these parts or modifications by contacting the FTU.

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

(5) Firearms must be unloaded, cleaned, and properly packaged before shipment via Federal Express, or other appropriate means. When returning a firearm to the FBI Academy Gun Vault for service or turn-in, a cover communication should be included which states the reason the firearm is being returned. Firearms being returned should be addressed: FBI Academy, Room 110, Building DN, Quantico, Virginia 22135. (DO NOT MAIL WEAPONS ADDRESSED "ATTENTION: GUN VAULT.") (See MAOP, Part I, 17-1.7.1; Part II, 2-2.2.2, 6-2.3.9, and 6-10.2.)

(6) When it becomes necessary to render a weapon inoperable during the course of an investigation, this procedure must be accomplished by an FBI gunsmith.

(7) Field offices intending to use seized guns for

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 12 - 15

demonstrations or teaching purposes must first submit those weapons to the Gun Vault for inspection, approval, and possible modifications to render them safe.

EFFECTIVE: 04/07/97

12-5.1 Care of Firearms

(1) After being used, and periodically during storage, all weapons should be carefully cleaned and lubricated per the manufacturer's recommendations. Care should be taken to prevent excess solvent and oil from entering inaccessible areas of the firearm.

(2) Excess oil and solvent must be completely wiped off wood stocks. Do not allow any oil or solvent to come in contact with the lenses of any telescopic sights or night sights.

(3) Due to the fact that handguns are almost continually encased in leather holsters, regular inspection and lubrication should be conducted to prevent rusting.

(4) Questions pertaining to the care, cleaning and maintenance of firearms should be addressed to the PFI or FBI Academy gunsmiths.

EFFECTIVE: 04/07/97

12-5.2 Deleted

EFFECTIVE: 04/07/97

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 12 - 16

12-6 SECURITY OF WEAPONS | (See also MIOG, Part II, 12-2.2.) |

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

(2) SACs must provide |secure| storage areas for Bureau-assigned firearms in Bureau office space.

(3) When on duty and out of the office, handguns should be kept on the SA's person unless operational considerations or good judgment dictate otherwise.

(4) [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. |This recommended action is made to minimize unnecessary unloading/loading of weapons within Bureau office space. |

(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 - |magazine removed, slide closed, hammer released and chamber plug inserted if available. |

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

(d) Colt Model |M16/AR-15 series of |rifles or carbines - magazine removed, action closed, trigger snapped, fire selector on "SEMI."

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 12 - 17

(e) Winchester/Remington rifles - action closed, trigger snapped, safety off.

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

(g) H&K MP5 (all models) - magazine removed, action closed, trigger snapped, safety on.

(h) M79 Grenade Launcher - action closed, trigger snapped, safety on.

(i) Federal Gas Gun - action closed.

EFFECTIVE: 04/07/97

12-6.1 Security of Weapons at Residence or Nongovernment Space

(1) SAs are personally responsible for security of all assigned firearms to prevent unauthorized handling or unintentional discharge.

(2) When devices or containers are provided by the Bureau for the storage of weapons away from Bureau space, SAs should make use of this equipment whenever possible.

(3) When unattended, each firearm must be made inoperable by one or more of the following methods:

(a) Remove and separate the source of ammunition.

(b) Install commercially available pistol lock, trigger lock, or cable lock.

(c) Contain in a commercially available lock box or other container which will provide appropriate security.

(4) Bureau personnel authorized to carry a firearm must use the utmost caution when storing and securing their firearm at home when children are present. In addition to great personal grief, many states have laws providing for severe criminal and civil penalties when anyone is injured or killed as a result of a child

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 12 - 18

obtaining access to a firearm. Bureau employees are to ensure the security and storage of their firearm(s) complies with pertinent state and local laws.

EFFECTIVE: 04/07/97

12-6.2 Vehicles (See MAOP, Part I, 1-3.2.)

(1) No Bureau-assigned firearm may be left in the passenger compartment of an unattended Bureau vehicle or vehicle authorized for official use unless the vehicle doors are locked and the firearm is secured in a locked vehicle weapons mount or other secure device or container which cannot be readily removed from the vehicle, and circumstances prevent more secure storage.

(2) [REDACTED] Even when properly secured, firearms should not be left in unattended vehicles overnight unless required by operational circumstances.

(3) Other nonexpendable Bureau equipment related to Agent safety may be maintained in the passenger compartment of an unattended Bureau vehicle or vehicle authorized for official use for short periods of time only if required by operational necessity or good judgment, and only if properly concealed and with the vehicle doors locked. "Properly concealed" means placed in an appropriate container and/or secreted within the vehicle to prevent observation and identification of the item from the vehicle exterior.

(4) Any nonexpendable Bureau equipment not related to SA safety should be maintained in the locked trunk of an unattended Bureau vehicle or vehicle authorized for official use, but should not be left overnight unless operational circumstances dictate otherwise.

(5) [REDACTED]

(6) [REDACTED]

(7) [REDACTED]

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 12 - 19

b2
b7E

(8) The standards set forth above are MINIMUM standards. Employees are expected to exercise good judgment in providing adequate security to all such equipment and firearms. Personal inconvenience is not considered an adequate reason for deviation from these minimum standards.

(9) Reports of lost/stolen firearms related Bureau property should be submitted to the Firearms Training Unit AND the Adjudication Unit, Office of Professional Responsibility, for replacement and possible administrative action.

EFFECTIVE: 04/07/97

12-7 AMMUNITION

(1) SAs and other Bureau employees authorized to carry firearms may load their Bureau-assigned weapon(s) only with ammunition provided or approved by the FBI.

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

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

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

(5) During training, any ammunition authorized for FBI use may be fired. At all other times outside of training sessions, FBI authorized service ammunition must be used.

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

(7) 9 mm 124 grain ball "training" ammunition may be used

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 12 - 20

operationally in the suppressed MP5 SD only. This round is limited to training use only in all other Bureau-issued/approved 9 mm weapons.

(8) The Firearms Training Unit is the procurement point for all ammunition used by Bureau personnel for official purposes.

EFFECTIVE: 04/07/97

12-7.1 Deleted

EFFECTIVE: 04/07/97

12-8 FIREARMS PROCUREMENT

(1) The acquisition of firearms as Bureau property must be (1) approved by the FTU, and (2) administered by the FBI Academy Gun Vault.

(2) All firearms purchased or obtained by a field office as Bureau property must be shipped directly to the FBI Academy Gun Vault for inspection and test firing before use.

(3) Any exceptions to this policy must first be requested in writing and approved by the FTU before procurement.

EFFECTIVE: 04/07/97

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 12 - 21

12-9 FIREARMS IN RESIDENT AGENCIES

(1) Firearms may be maintained in resident agencies.

(2) All handguns and shoulder fired weapons should be stored in a secure safe, vault or safe-type cabinet. Reasonable security precautions such as weapons locked and stored in locked cabinets or closets within alarmed Bureau space may suffice in lieu of storage in a safe.

(3) Field offices are authorized to purchase safes, vaults, or safe-type cabinets in order to provide secure storage of firearms.

(4) All other policies cited herein that govern the use and maintenance of Bureau-assigned firearms and ammunition also apply.

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

EFFECTIVE: 04/07/97

12-10 FIREARMS TRAINING

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

(2) The objective of the FBI firearms training program is to provide four MANDATORY qualification sessions annually. Since firearms training is a perishable skill, however, the FTU encourages field offices to provide additional training opportunities. Field offices whose range availability and ammunition supply will not support mandated training should submit a proposed training plan to the Training Division, FTU, for approval. This plan should include the number of sessions, courses to be used, and the number of rounds to be fired.

(3) The SAC is ultimately responsible for all firearms training, weapons and ammunition inventories, and execution of the Field Firearms Program.

(4) SAs and all other personnel authorized to carry

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 12 - 22

firearms must meet or exceed the minimum proficiency and safety standards set forth in the Annual Field Firearms Program.

(5) PFIs are responsible for all transition training either from revolver to pistol or pistol to revolver. The PFI must be satisfied that an SA has successfully completed the requirements of transition training and proficiency checklist as specified in training curricula provided by the FTU and is qualified to carry that weapon. The PFI must verify this training by documentation on or attached to the SA's FD-40.

(6) Each PFI should adhere to the format of the calendar year Field Firearms Program provided by the FTU. Any changes must be submitted via written communication and approved in advance by the Unit Chief, FTU.

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

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

(9) The Defensive Tactics Training Course will be managed by the Principal Defensive Tactics Instructor in each field division. This program is submitted to each office as part of the annual Field Firearms Training Program.

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

(a) Dates of training sessions

(b) Ranges utilized

(c) Names of instructors assisting each session. These names should also be listed at the bottom of FD-39 score cards.

(d) Names of Bureau personnel who have missed ANY mandatory training sessions, with the reason for each delinquency specified. ALL delinquencies must be reported.

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

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 12 - 23

qualified.

(11) The PFI is to ensure that ranges used for field firearms training are inspected and contain no safety hazards that would endanger FBI personnel or others.

(12) PFIs are to make every effort to ensure that the air quality of indoor ranges used for training complies with the Occupational Safety and Health Administration (OSHA) standards. A certificate of compliance with these standards should be available for review at the range facility. If an indoor range does not comply with OSHA standards, this facility should not be used for training.

(13) The authority in charge of a particular range should be advised of any safety deficiencies noted.

EFFECTIVE: 04/07/97

12-10.1 Firearms Delinquencies

(1) Any employee authorized to carry firearms who does not attend firearms training during a firearms training period is considered delinquent. To ensure compliance with this requirement, the SAC (or AD in the case of FBIHQ) may, at their discretion, require delinquent individuals to surrender their firearms and make any necessary recommendations to the Adjudication Unit, Office of Professional Responsibility (OPR), FBIHQ, for administrative action if appropriate. The individual's authority to carry a firearm is rescinded and the weapon should only be issued for training purposes until the delinquency is corrected. No SA should be permitted to become delinquent for any firearms training period unless documented medical circumstances dictate otherwise AND the SA has been placed on medical mandate by FBIHQ Health Care Programs Unit. The FTU is to be advised of each delinquency in the "Annual Field Firearms Training Report."

(2) Those Agents who were unable to attend firearms training on their regularly scheduled days should be rescheduled at the earliest convenience during the training period. Delinquencies must be corrected as soon as possible.

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

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 12 - 24

EFFECTIVE: 04/07/97

12-10.2 Firearms Qualification

EFFECTIVE: 05/20/94

12-10.2.1 Firearms Qualification Policy (See MIOG, Part II,
12-10.4; MAOP, Part I, 20-28.3.)

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

(2) SAs must qualify a minimum of four times per calendar year.

(3) SAs must qualify with each assigned handgun a minimum of once per year. It is recommended that weapons regularly carried on duty be fired for qualification at each firearms session.

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

(5) Agents will qualify within their assigned division. Agents assigned to FBIHQ, the Engineering Research Facility, and the FBI Academy will qualify with the FTU at Quantico.

Exceptions:

(a) Agents assigned on a temporary duty basis to another division which would preclude their qualification in their assigned division, may qualify with the host division. It is the responsibility of the PFI in the host division to ensure the TDY

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 12 - 25

Agent's scores are recorded and forwarded to the PFI of the Agent's assigned division.

(b) Agents wishing to qualify with another division for convenience must have the concurrence of the PFI from their assigned division and the host division. The PFI of the host division must record the visiting Agent's scores and forward these to the PFI of the Agent's assigned division.

(c) Agents assigned to FBIHQ, the Engineering Research Facility and the FBI Academy wishing to qualify with another division must have the concurrence of the FTU and host PFI. The PFI of the host division is responsible to ensure the visiting Agent's scores are recorded and reported to the FTU.

EFFECTIVE: 04/07/97

12-10.2.2 Recording Firearms Scores

(1) The names of SAs receiving firearms training should be indicated on the Form FD-39 or an approved automated system.

(2) The individual scores shall be entered in the appropriate column of Form FD-39. This form shall contain the names of all SAs attending firearms training and the make and model of issue/approved firearm(s) used for qualification. Supervising firearms instructors shall be listed at the bottom of FD-39.

(3) After completion of a training period, scores are to be transferred from the FD-39 to each SA's FD-40 or automated form. FD-39s are retained for one year, then destroyed; FD-40 is a permanent record and must accompany the SA's personnel file upon transfer.

(4) The PFI or designated firearms instructor will score the targets on qualifying courses.

EFFECTIVE: 04/07/97

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 12 - 26

12-10.2.3 Failure to Qualify

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

(2) After opportunities have been provided for qualification and failures continue to exist, the PFI must advise the FTU in the Annual Field Firearms Training Report.

(3) Employees must demonstrate proficiency to be permitted to carry firearms. If the employee cannot qualify after remedial training on two out of three qualification attempts, the SAC must require the employee to surrender his/her firearm. The Agent will be issued his/her weapon only for training until such a time as a qualifying score is shot. When an Agent's authority to carry a firearm is rescinded, this action must be noted on the Agent's FD-40.

(4) Chronic unexcused delinquency or failure to qualify should be reported to the FTU and Adjudication Unit, Office of Professional Responsibility, with recommendations for administrative action, if appropriate.

EFFECTIVE: 04/07/97

12-10.2.4 Shoulder Weapons - Qualification

SAs will qualify with each assigned shoulder weapon at least twice per year. Agents are encouraged to train with weapons they regularly carry at EVERY training session. SAs with an assigned shoulder weapon will use that specific weapon when qualifying. Agents not assigned a specific shoulder weapon will, at a minimum, demonstrate proficiency with the shotgun and MP5 at least once per year as specified in the Annual Field Firearms Program.

EFFECTIVE: 04/07/97

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 12 - 27

12-10.3 Firearms Safety Rules

(1) Cardinal Rules:

- (a) Treat all firearms as if they are loaded.
- (b) Never point a weapon at anyone unless you are justified in doing so.
- (c) Keep your finger off the trigger unless you intend to shoot.

(2) General Rules:

- (a) All live-fire FBI firearms training must be supervised by an FBI Firearms Instructor.
- (b) When transporting weapons on your person to and from the range, handguns should be holstered; shoulder weapons should be in a safe condition and carried with the muzzle pointed straight up.
- (c) Safety precautions must be adhered to and enforced. Discipline must be maintained. Unsafe and careless behavior will not be tolerated, should be reported, and may result in recommendations for administrative action.
- (d) Immediately upon picking up a firearm, face a safe direction, activate the safety if present, remove any ammunition, open the action and check to see that the weapon is unloaded. Check it again.
- (e) Never give to or receive a firearm from anyone, unless the weapon is unloaded and the action is open allowing the person receiving the weapon to see that it is unloaded. Always present the weapon BUTT first.
- (f) Never anticipate a command. Avoid unnecessary conversation, and pay attention to instructors. You will be told exactly what to do.
- (g) Perform a safety check on the weapon before a training session. Make sure the weapon is unloaded. After training, you also need to ensure the weapon is unloaded before cleaning.

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 12 - 28

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

(i) Keep the firearm pointed down range or in a safe direction at all times and ALWAYS be aware of potential dangers in any direction your weapon may be pointed.

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

(k) No smoking, eating or drinking on the firing line because of health risks associated with lead residue.

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

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

(n) After firing a shot that does not sound as loud as it should, clear the weapon and check to see if a bullet is lodged in the barrel.

(o) Never leave your firing position unless instructed to do so.

(p) Never remove a weapon from the holster in training, unless instructed to do so.

(q) Never dry fire on the range unless under direct supervision of a Firearms Instructor. Exceptions will be specifically identified by the lead Firearms Instructor.

(r) Eye and ear protection are mandatory when firing on the range. Ear plugs should be worn ONLY IN CONJUNCTION with proper sound barriers and are NOT a substitute for issued or equivalent hearing protection.

(s) Everyone is responsible for range safety. Immediately report any safety violations you see to a Firearms Instructor.

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 12 - 29

EFFECTIVE: 04/07/97

12-10.4 Firearms Training of Non-Agent Employees

As a rule, only Agents receive firearms training from the Bureau. Exceptions are:

(1) Electronics technicians and security patrol clerks specifically authorized by FBIHQ.

(2) Uniformed Police Officers of the FBI.

(3) Other non-Agent personnel with special authority to carry firearms (e.g., Special Deputy U.S. Marshal).

(4) Non-Agent personnel authorized to carry firearms must:

(a) be approved by their SAC or Section Chief

(b) comply with deputation requirements established by the USMS, and

(c) be engaged in official activities for which the carrying of a firearm has been authorized.

(5) All non-Agent personnel who are authorized to carry firearms will comply with all regulations in this section that normally apply to SAs (see MIOG, Part II, 12-10.2.1). In addition, they must also attend annual legal training, quarterly defensive tactics training, and participate in the Fitness Indicator Test (FIT).

EFFECTIVE: 04/07/97

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 12 - 30

12-10.5 Police Firearms Training

(1) FBI firearms instructors may conduct police firearms schools.

(2) Firearms training is to be given only to law enforcement groups unless an exception is authorized by the SAC (e.g., safety training for Bureau employees and their family).

(3) The primary firearms instructor must ensure that ranges used for firearms training are inspected and contain no safety hazards that would endanger FBI or police personnel.

EFFECTIVE: 04/07/97

12-10.6 Firearms Instructors Policy (Formerly 12-10.6.1)

(1) To qualify as a Bureau firearms instructor, candidates must attend the Firearms Instructor In-Service (FAIS) presented by the FTU.

(2) To maintain instructor status, employees must qualify quarterly and obtain the following minimum scores when these courses are fired:

(a) 30 round bulls-eye course

1. One-hand score 240, or

2. Two-hand (optional) score 260

(b) Double Action Course score 90

(c) PQC score 90

(d) Shotgun 10A score 90

(e) MP5 (qualification course) score 90

(3) To maintain instructor status, in addition to shooting instructor level scores on courses listed in (2) above, each instructor must participate in at least one documented Bureau firearms

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 12 - 31

training session per year.

(4) Firearms instructors must attend a Recertification Program with the FTU at least once every four years. Agents transferring out of the FTU are considered recertified for a period of four years.

(5) Failure to comply with instructor requirements will result in the loss of current status. The employee will be listed officially as firearms instructor - inactive.

(6) To regain active firearms instructor status, the employee must attend a Recertification Program at the FBI Academy and demonstrate proficiency as noted in (2) above.

EFFECTIVE: 07/17/97

| 12-10.6.1 | Revised and Moved to 12-10.6 |

EFFECTIVE: 04/07/97

| 12-10.7 | Target Guidelines |

| (1) | STEEL TARGET POLICY

| (a) - Standard | service and training ammunition | may not be used on steel targets | at distances less than ten yards. Some types of frangible ammunition may | be used on | steel targets at closer distances.

| (b) | To minimize | potential injury from | ricochets, firing positions should be perpendicular to the target line.

| (c) | Construction of any steel targets MUST be coordinated through the | FTU to ensure targets meet minimum hardness and safety standards.

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 12 - 32

(d) PFIs are responsible for permitting only the use of proper weapons and ammunition on steel targets to prevent damage or destruction to the target, reduce ricochet and prevent injury to personnel.

(e) Steel targets must be inspected before each training session.

(f) All personnel on the steel course site must stand behind the shooter. In multiple courses, the shooter must not be ahead of another shooter.

(g) All personnel on the steel course site must continuously wear eye and ear protection. Personnel on a steel course should also wear issued body armor.

(h) Damaged targets, i.e., dimpled, punctured, or bowed, are unsafe and should not be used.

EFFECTIVE: 04/07/97

12-11 SHOOTING INCIDENTS (See MAOP, Part II, 8-1.3.2.)

EFFECTIVE: 10/17/95

12-11.1 Reporting of Shootings (See MIOG, Part II, 12-11.8; MAOP, Part II, 8-1.3.2.)

(1) In all shooting incidents involving the intentional use of force by FBI personnel and in all incidents, intentional or otherwise, WHERE INJURY OCCURS, notify the Violent Crimes and Major Offenders Section (VCMOS) Chief, CID, FBIHQ by telephone, followed by teletype. Similarly, in all shooting incidents occurring in joint investigations or FBI led/controlled task forces where a non-FBI participant fires a weapon, notify the VCMOS, CID, FBIHQ by telephone, followed by an airtel within seven days.

(2) Other instances involving the discharge of a firearm

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 12 - 33

| by FBI personnel | must be reported as soon as time permits by teletype to the Chairperson, Shooting Incident Review Group (SIRG), with a copy to the Firearms Training Unit (FTU). FD-418 (Shooting Incident Report), in triplicate, is to be submitted to the FTU by airtel within five working days. SA's FD-40 (Firearms Record) should be attached to the FD-418.

(3) If an FBI employee is injured, designate one copy of teletype for the Office of | Public | and | Congressional Affairs. |

(4) SAC must personally ensure that investigations | related | to Agent-involved shooting incidents are handled quickly and properly.

(5) | If the SAC or ASAC was involved in the planning or execution of events, FBIHQ should be advised during initial contact. |

(6) | Initial teletype should include the SAC's recommendation whether the shooting inquiry should be conducted by the field division under the direction of the SAC, or by a Shooting Incident Response Team (SIRT) under the direction of an Inspector or Inspector-in-Place (IIP). Generally, this determination is based on the extent of SAC or ASAC participation in the planning and operational events of the incident. |

(7) | The Assistant Director, Inspection Division (INSD), in consultation with the SAC and Assistant Director, CID, will make the determination whether a shooting inquiry will be conducted under the direction of the SAC or an Inspector/IIP. |

(8) | If an Inspector/IIP is not dispatched to the scene, the SAC will advise and confirm by teletype that he/she is directing the necessary required shooting inquiry investigation, UACB. |

(9) | A shooting inquiry must be conducted under the direction of the SAC when a weapon is discharged by FBI personnel unless circumstances necessitate the inquiry be conducted under the direction of an Inspector/IIP. |

(10) | In joint or task force investigations wherein a local, state, or other federal law enforcement officer fires a weapon or is shot, but no shots are fired by FBI personnel who are present:

(a) Joint investigation - SAC or ASAC will notify FBIHQ by telephone, followed by an airtel delineating the following:

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 12 - 34

1. Activities of accompanying officer and circumstances which led to the shooting.
2. Details of raid/arrest plan.
3. Instructions given to accompanying officer.
4. Results of local shooting inquiry conducted, if available; records of interview(s), and analysis.

(b) FBI led/controlled task force:

1. Include all of (a) above, plus:
 - a. Degree of FBI supervision exercised over the officer's day-to-day investigative activities (generally reflected in implementing Memorandum of Understanding (MOU)).
 - b. Chain of command within the task force.
 - c. A copy of any MOU delineating task force responsibilities of non-FBI personnel.

(c) Submit within seven days, an original and 12 copies of the shooting incident airtel to the Assistant Director, INSD, Rm. 7129, Attention: SIRG, with one copy designated to the FTU.

(11) through (22) Moved to MIOG, Part II, 12-11.7, 12-11.8, and 12-11.9.

EFFECTIVE: 10/17/95

12-11.2 Guidelines for Intervention at the Shooting Scene (See MAOP, Part II, 8-1.3.2.)

(1) After the shooting scene has been secured, the first concern expressed and acted upon will be that all Bureau personnel are well cared for both physically and mentally.

(2) The Agent(s) involved in the shooting incident will be permitted and encouraged to immediately contact his/her spouse

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 12 - 35

and/or family. If the Agent has been injured, or if he/she feels it would be useful, the Agent's family will be contacted immediately in person by a designated Agent who knows the family personally. The field office will also be notified of the Agent's condition so that there will be a response to the family who called the office. It is particularly important that family notification occur before press and/or media accounts appear.

(3) Agents who have been personally involved in the shooting incident will be removed from the scene as soon as possible and not assigned further duties in the investigation of that incident.

(4) If the Agent's weapon is secured for evidence or ballistics tests, another will be issued immediately unless there is cause not to issue a weapon. The Principal Legal Advisor, Office of General Counsel, FBIHQ, or the United States Attorney's Office should be consulted if questions arise regarding whether an Agent's weapon should be surrendered to local authorities.

(5) The SAC or ASAC will initiate a personal contact with the Agent(s) and his/her family in a supportive role and offer assistance, if needed. This contact will be made as soon as possible following the incident (within the first 24 hours).

(6) The current Bureau procedure of not releasing the identity of Agents involved in investigations or incidents is especially important in post-shooting matters and will be maintained.

(7) An SAC should communicate with FBIHQ if any of the established procedures appear to be inappropriate for a specific incident.

(8) SACs and/or ASACs should hold an office conference, as soon as practical, after a shooting incident and as often as necessary to keep all personnel advised of pertinent details concerning the shooting incident. This should substantially reduce rumors and distorted accounts of the incident. (See MAOP, Part II, 8-1.3.2.)

EFFECTIVE: 05/20/94

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 12 - 36

12-11.3 Guidelines For Intervention During The First Week (See
MAOP, Part II, 8-1.3.2.)

(1) The Critical Incident Program consists of several specifically trained Agents and support employees located at the FBI Academy, Quantico, Virginia, and throughout the field offices administered from Personnel Division (PD), FBIHQ.

(2) The Critical Incident Program also includes FBI Chaplains in each field office who have been trained to respond to Agents and support employees who have been involved in critical incidents including shootings.

(3) Bureau policy establishes confidentiality for any conversations between employees and peer support employees or FBI Chaplains.

(4) There are exceptions to this Bureau policy of confidentiality which could require disclosure. These exceptions might include, but are not limited to, risk of death or injury, perspective criminal acts, or interference with Bureau investigations. A decision to disclose must first be discussed with the Critical Incident Program Manager, PD, FBIHQ. No assurance can be given that the courts will recognize the confidential relationships established by this policy. In a criminal or civil action arising from a critical incident, the court could conceivably order disclosure notwithstanding Bureau policy.

(5) The SAC or ASAC will advise the office FBI Chaplain(s) of the critical incident and coordinate a request for peer support with the PD, FBIHQ.

(6) A brochure is available to Agents/employees who have been involved in shooting incidents covering:

- (a) The symptoms to be expected and their normal course.
- (b) Administrative handling of the post-shooting investigation.
- (c) Legal aspects of the shooting incident.
- (d) Counseling services available.

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 12 - 37

(7) An official from FBIHQ will contact the Agent personally by telephone. The scope and direction of this call is to express concern for the welfare of the Agent and his/her family. The Assistant Director, PD, will coordinate the personal phone contacts.

(8) A total of five optional days of administrative leave are available to be taken (at sole discretion of) persons directly involved in the shooting incident. The use of that administrative leave will be strongly encouraged by the SAC. This leave may be taken at any time at the discretion of the Agent and should be coordinated with his/her supervisor. The Health Care Programs Unit (HCPU), PD, will furnish guidance concerning individuals eligible for leave and authority to grant leave. (Also see LEAVE ADMINISTRATION GUIDE.)

(9) An Agent directly involved in the shooting incident should be advised by the SAC that the Agent can be reassigned from his/her squad for a period of time if the Agent so desires.

(10) The SAC will immediately coordinate with HCPU, PD, FBIHQ, if an Agent directly involved in the shooting incident requires other special attention, to initiate the utilization of the mental health professional resources of the Employee Assistance Program (EAP).

(11) If an Inspector has been assigned to conduct the shooting inquiry, he/she will review these intervention guidelines with appropriate field office managers.

(12) In the event of an incident which involves the death of an employee or a line-of-duty injury that results in the hospitalization of the employee for serious injuries, the Director desires to personally contact the employee or family and offer comments that will contribute, even if in only a small fashion, to the healing process that lies ahead. To facilitate these contacts the following information should be relayed to the Director expeditiously, usually by teletype.

(a) A brief description of the incident and the nature of the injuries sustained.

(b) The name(s) and age(s) of the employee's immediate family.

(c) Where and when the employee or family may be reached.

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 12 - 38

(d) Any other information that would be helpful during the Director's contact with employee or family.

(13) Recognizing that the FBI's continuing concern can significantly help the recovery of our employees and their families, it may be beneficial for the Director to recontact them. The timing of this recontact is left to the discretion of the SAC. Recontact requests should be submitted by teletype to the Director's personal attention and include the following information:

(a) The information requested above.

(b) An update on the condition of the employee or family.

(14) More periodic expressions of concern by the immediate FBI family will be led by the SAC. SACs should be aware of the extensive support structure that exists in the HCPU of the PD. This includes peer support, contract mental health professionals, FBI Chaplains and the EAP. These resources should be used as appropriate to provide our employees and their families with the support and assistance they need during times of extreme trauma and sorrow.

EFFECTIVE: 05/20/94

12-11.4 Guidelines for Long-Term Issues (See MAOP, Part II, 8-1.3.2.)

(1) SAC or ASAC will personally make every effort to facilitate the administrative investigation of a shooting incident.

(2) If a group of Inspectors from FBIHQ is required to conduct an investigation of the shooting incident, an effort will be made to ensure that at least one of the Inspectors has received training in the effects of post-shooting trauma and, if possible, has personally experienced a shooting incident.

(3) Agents should be allowed to pace their own return to work following shooting incidents. The Personnel Division (PD) will furnish guidelines concerning use of administrative leave. The SAC and supervisor will be involved in this decision-making process.

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 12 - 39

(4) If a transfer of an Agent to another squad following a shooting incident is contemplated, consideration will be given to the effects of the transfer on the adjustment period and the Agent should be involved in the decision.

(5) The letter announcing the conclusion of a Bureau investigation of a shooting incident will be phrased in a way that takes into account the emotional impact on the Agent who has been involved in a life-threatening situation and may have suffered post-shooting trauma.

(6) SACs and/or ASACs or the Principal Firearms Instructor should personally and individually provide the necessary positive and/or negative feedback to Agents after the administrative inquiry has been completed. This will also afford an opportunity to ascertain if the involved Agent(s) is amenable to any formal recognition, as warranted. Medals or incentive awards following a shooting incident in which subjects have been seriously injured or killed can have a negative psychological impact and/or be perceived as a reward. However, medals or incentive awards may be appropriate, and will be authorized if recommended and justified. Emphasis will be on the effort to save lives.

(7) Agents who have been involved in a shooting incident will not immediately be assigned to duties likely to involve armed confrontations. This is even more important when a given Agent has already been involved in a previous shooting incident. This consideration should take precedence over other action, including transfers.

(8) Employees who have been involved in shooting incidents will be afforded an opportunity to attend a Post-Critical Incident Seminar at the FBI Academy. These group sessions will be the basis for future modifications in policy and training and will also provide a pool of employees able to provide meaningful peer support. The group sessions provide a therapeutic understanding of the shooting event. These conferences will be coordinated by the Training Division's Behavioral Science Services Unit (BSSU).

(9) PD's Employee Benefits Unit has prepared a booklet captioned "Your Worker Compensation Benefits" for questions relating to work-related illnesses and injuries.

(10) The PD Transfer Ombudsman had been designated to serve as a single point of contact at FBIHQ concerning insurance and compensation matters following a shooting incident. The Ombudsman

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 12 - 40

will be available on a case-by-case basis to respond following a critical incident and offer assistance to victims and survivors of that incident concerning insurance and compensation matters. The Ombudsman attends Post-Critical Incident Seminars and maintains contact with the Critical Incident Program Manager.

(11) Six months after the shooting incident, HCPU, PD, FBIHQ, will contact the SAC of the Agent involved in the shooting incident to determine if follow-up counseling is necessary.

EFFECTIVE: 05/20/94

12-11.5 Guidelines For Training (See MAOP, Part II, 8-1.3.2.)

(1) Training related to post-shooting trauma and its management will be made available to Bureau administrative personnel. A training block of this type will be presented by the Behavioral Science Services Unit, (BSSU), Firearms Training Unit, and the Management Science Unit, Training Division. A presentation in this area should also be incorporated into upcoming SAC Conferences, Senior Executive Programs, and Executive Development Institute sessions.

(2) An orientation session by the BSSU on an introduction to post-shooting trauma will be provided to students during New Agents training.

(3) In the planning of operations which have a high risk of armed confrontations and/or may involve the use of deadly force, if the SAC, ASAC or supervisor is aware of an Agent who is experiencing high levels of personal and/or family stress or health problems, consideration should be given to temporarily excuse the SA from participating in the exercise in order to minimize the risk of cumulative stress or trauma incidental thereto.

EFFECTIVE: 05/20/94

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 12 - 41

12-11.6 Nondisclosure of Agents' Names in Shooting Incidents (See MAOP, Part II, 5-2 (4) and 8-1.3.2.)

Names of Agents involved in shooting incidents in performance of duty should not be volunteered to outsiders since experience has shown that once their identities become a matter of public knowledge, the potential that they and their families will be subjected to harassment and possible retaliation substantially increases. If identities of Agents involved in shooting incidents have been made public through inclusion in public records or disclosure at public proceedings, SACs may verify the Agents' identities in response to inquiries by news media representatives or others.

EFFECTIVE: 04/07/97

12-11.7 Investigation of Shootings Involving FBI Personnel (Formerly 12-11.1.) (See MAOP, Part II, 8-1.3.2.)

(1) An investigative inquiry of the shooting incident will be conducted under the direction of the SAC or Inspector/Inspector in Place (IIP), as appropriate, and a comprehensive report issued.

(a) The SAC is responsible for preserving evidence and instituting a logical investigation. SAC or SAC's designee should personally coordinate investigation if an Inspector/IIP is not dispatched to the scene.

(b) The SAC will designate an investigative team to conduct those shooting inquiries under his/her direction. The SAC should use appropriate personnel and resources (Evidence Response Team (ERT), Photographer, etc.) to conduct a thorough, factual investigation of the shooting incident and to submit a comprehensive report to the Shooting Incident Review Group (SIRG). The SAC should consider Laboratory Division assistance in appropriate circumstances.

(c) In the event an Inspector/IIP is dispatched to the scene, the Shooting Incident Response Team (SIRT) will be comprised of an Inspector or IIP and two or more Assistant Inspectors-in-Place (AIIP) selected by the Chief Inspector, Inspection Division

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 12 - 42

(INSD), and a forensic team comprised of a firearms examiner, visual information specialist, and photographer selected by the Laboratory Division.

(d) The SIRT under the direction of the Inspector or IIP will report directly to the Chief Inspector, Office of Inspections, during the shooting inquiry and be tasked with completion of a thorough, factual investigation of the shooting incident and submission of a comprehensive report to the SIRG, along with any observations regarding safety and/or training issues identified through the inquiry.

(2) Local authorities are to be contacted to clarify jurisdiction and investigative responsibilities.

(3) All personnel and witnesses at the scene are to be identified, located and interviewed.

(4) Agents involved in a shooting must be given sufficient time to regain composure before being requested to provide any statements. The official conducting the inquiry will consult with the SAC or other appropriate personnel and consider such factors as physical injuries or trauma experienced by the Agent involved in a shooting to determine when an interview should take place.

(5) Avoid having involved Agent(s) conduct any investigation and/or interviews relevant to the shooting. Do not, however, delay substantive investigation to accomplish this. Separate and remove involved Agent(s) from the scene as soon as practical.

(6) Forms FD-644 (Warning and Assurance to Employee Requested to Provide Information on a Voluntary Basis) and FD-645 (Warning and Assurance to Employee Required to Provide Information) are not to be used in investigations concerning shooting incidents in the absence of specific, compelling reasons. Such a determination will be made by the SAC or Inspector/IIP in consultation with the appropriate FBIHQ officials. Prior to the use of the FD-645 in cases where there is potential for criminal prosecution of the employee to be interviewed, OPR, Inspection Division, must present the facts of the case to OPR, DOJ, and obtain an initial opinion that the matter in question should be handled administratively rather than criminally. (See MAOP, Part I, 13-6 (3) and MIOG, Part I, 263-5 (3).)

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 12 - 43

EFFECTIVE: 10/17/95

12-11.8 Shooting Inquiry Report (See MIOG, Part II, 12-11.1;
MAOP, Part II, 8-1.3.2.)

(1) Results of an inquiry in all shooting incidents involving the intentional use of force by FBI personnel and in all incidents, intentional or otherwise, WHERE INJURY OCCURS, are to be submitted to FBIHQ within two weeks in the form of an investigative report. The shooting inquiry is primarily a fact-finding effort and must be objective, thorough, and factual. Observations regarding safety and/or training issues identified during the inquiry should be included in the report.

(2) Report should be captioned "Shooting Inquiry, Report of Shooting Incident; (name of Reporting) Division; (date of shooting incident); Admin Matters; (66F classification)." The report should specifically reference, using case caption, the substantive violation, if any, involving the shooting incident, e.g., "John Doe; First Savings Bank; 3/6/95; BR; OO: NY; UCFN #." Reference should also be made to the teletype that initially advised FBIHQ of the shooting and the communication which forwarded the FD-418s.

(3) The report should contain appropriate enclosures and exhibits, to include but not limited to: medical reports, coroner or autopsy reports, police reports, crime scene diagrams, radio logs, criminal record and NCIC checks, military records of subjects if pertinent, weather information, firearms and ballistic information (include Laboratory Reports if available or FD-302 summary of laboratory analysis), videos from local news media, shooting incident reconstructions, and crime scene photographs.

(4) No accomplishments should be claimed in the Shooting Inquiry report. Any accomplishments achieved at the time of the shooting incident should be claimed by a communication under the substantive title.

(5) The Administrative section of the report should include information concerning decisions regarding interview of subject(s), pertinent administratively controlled material, informant information, and observations regarding training and/or safety issues. SAC analysis and recommendation(s) for administrative action, if deemed warranted, should be set forth in this section of the report.

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 12 - 44

(6) A table of contents should be utilized to organize and identify report contents. Following is an example of items which might normally be included:

(a) Interviews of personnel involved - include signed, sworn statements of all Bureau employees principally involved in the shooting incident. Interview all Bureau personnel directly involved in the investigation and/or planning leading to the shooting incident. Any arrest or raid plans pertinent to the incident should be carefully spelled out in statements obtained from the person(s) in charge of the raid/arrest.

Interviews in shooting inquiries should be handled without the use of Forms FD-644 and FD-645, unless there are specific factual situations or complaints which might raise concerns about the shooting. Should these arise, the details should be discussed with the Chief Inspector, Inspection Division (INSD), prior to conducting any interview of Bureau personnel.

(b) Interviews of witnesses - include FD-302s of all witnesses to the shooting incident. Persons interviewed should be apprised of the access provisions of the Privacy Act and afforded the opportunity to request confidentiality in accordance with MIOG, Part I, 190-7 and SAC Memo 51-77 (C) dated 11/15/77.

(c) Investigation regarding subject(s) - include such information as criminal records, if available, and interviews of associates which are germane to shooting (i.e., individuals involved in circumstances surrounding the shooting incident, co-arrestee, etc.). If possible, include interview of subject(s) regarding the shooting. Such an interview is often quite productive in obtaining admissions from the subject(s) directly pertinent to the shooting incident. Statements made by subject(s) contemporaneous to the shooting oftentimes may be important to the overall evaluation of the incident by the SIRG.

Apprehension FD-302 should be included. Prepare FD-302 reporting that subject did not, was not known to have, or refused to comment on the shooting, if applicable.

(d) Medical reports - include medical reports and interviews with medical personnel clarifying the nature and gravity of all wounds or injuries as a result of the shooting. Indicate weapon, entry and exit of individual shots, if determinable. If fatalities involved, include coroner or autopsy reports.

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 12 - 45

(e) Vehicles involved - describe all pertinent vehicles and indicate damage incurred. Describe any other property damage.

(f) Weapons involved - include FD-302s reflecting weapons and ammunition used by Agent(s), officer(s) and subject(s) involved and disposition or custody of weapons following the shooting.

(g) Maps, diagrams, photographs, and other graphic depictions or representations of shooting incident scene and/or scenario.

(h) Police reports - include copies of reports, if available, plus any statements made regarding possible prosecutive action against Bureau personnel. Include copy of communications with local prosecuting attorney.

(i) Prosecutive status of subjects.

(j) Laboratory reports - laboratory reports should be included in the Shooting Inquiry report, if they are available. If laboratory examinations have not been completed, preliminary results should be reported by a summary FD-302. Results of forensic processing conducted at the scene may be included in the form of a laboratory report or an FD-302, whichever is deemed most suitable by the forensic expert(s).

(7) To assure accuracy and completeness of the Shooting Inquiry report, SAC or Inspector/IIP should confer with the Chief Inspector, Office of Inspections, INSD.

(8) Submit an original and 12 copies of the report to the Assistant Director, INSD, Rm. 7129, Attention: SIRG, with one copy designated to the FTU. The INSD will distribute copies to members of the SIRG.

EFFECTIVE: 10/17/95

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 12 - 46

12-11.9 Shooting Incident Review Group (Formerly 12-11.1.) (See
MAOP, Part II, 8-1.3.2.)

(1) The Shooting Incident Review Group (SIRG) is an independent review committee established to analyze all shooting incidents involving Bureau personnel and to evaluate the application of deadly force in such incidents. The SIRG is to provide the Director with an evaluative analysis, observations, and recommendations for corrective actions from an operational standpoint, if any, as well as recommendations concerning training issues, safety issues and administrative action, if deemed necessary.

(2) Scope and Purpose: The SIRG will review all shooting incidents wherein Bureau personnel employ deadly force, as well as all incidents where a firearm is discharged in a nontraining setting.

(a) The SIRG will determine if the shooting under review was intentional or unintentional. This will govern the standards applied in the review as the FBI's Deadly Force Policy will only be applied where the shooting was intentional.

(b) The SIRG will deliberate and determine if the shooting incident falls within the application of the FBI's Deadly Force Policy and the law.

(c) The SIRG will review operational plans, procedures, tactics and circumstances leading to the shooting incident.

(d) The SIRG will review issues associated with safety, training, and management oversight and make recommendations for administrative action, if deemed necessary.

(3) The SIRG will be comprised of representatives from the following:

(a) Inspection Division (INSD) - Deputy Assistant Director, (Chairperson) and Chief Inspector, Office of Inspections, (Alternate Chairperson);

(b) Criminal Investigative Division;

(c) National Security Division;

(d) Training Division;

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 12 - 47

(e) Personnel Division;

(f) Office of the General Counsel;

(g) Laboratory Division;

(h) Field Supervisor (preferably one who has been involved in a shooting incident) from the Washington, D.C. Metropolitan area.

(i) Department of Justice Attorney(s) as delegated by the Deputy Attorney General.

(4) The SIRG will deliberate and report its analysis by issuing a memorandum of findings and recommendations to the Director. This memorandum will be reviewed by the SIRG members, each of whom may provide additional comments, observations, or recommendations by attaching an addendum to the memorandum.

(5) The findings and recommendations will be submitted from the SIRG by the Chairperson to the Assistant Director, INSD, for approval and forwarding to the Director. An information copy of the SIRG memorandum of findings will be disseminated to the substantive Assistant Director (CID or NSD) as appropriate, and to other appropriate entities (Training, Personnel, etc.).

EFFECTIVE: 10/17/95

12-12 HOLSTER/ACCESSORY EQUIPMENT

(1) SAs must train with holsters and related equipment normally used on duty at each firearms training session.

(2) Holsters are not provided for personally owned weapons.

(3) Personally owned holsters must be approved through the PFI before use.

(4) Alterations of any holster, such as removing a thumb brake, is not permitted.

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 12 - 48

(5) Accessory equipment, i.e., magazine or speed loader pouches, ammunition pouches, etc., must be maintained and inspected in the same manner as a holster.

(6) Each SA is responsible for the proper maintenance of all holsters and accessory equipment under his/her control.

(7) Bureau-issued holsters/accessories, when worn or damaged beyond repair may be replaced through the FBI Academy Gun Vault.

(8) All strong side belt holsters will meet the following requirements:

(a) Must be able to draw and reholster the handgun with one hand.

(b) The holster must not require the trigger finger to pass through the trigger guard to release the weapon.

(c) the holster must secure the weapon during strenuous physical activity (running, climbing, upside down, etc.).

(9) "Miscellaneous holsters" refers to shoulder holsters, belly bands, ankle holsters, inside pants holsters, cross-draw holsters, fanny (butt) packs, etc.

(a) All regulations that exist for strong side hip holsters apply with the exception that it is permissible for the weak hand to steady the holster while returning the weapon. However, no holster will be approved that REQUIRES using both hands to draw the weapon.

(b) Firearms instructors are to ensure that proper safety is exercised during training with any miscellaneous holster.

(10) SAs should use both Bureau-issued and personally owned holsters and other firearms equipment during firearms training sessions to ensure familiarity.

EFFECTIVE: 04/07/97

Sensitive
PRINTED: 02/18/98

XXXXXX
XXXXXX
XXXXXXFEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

9

Page(s) withheld entirely at this location in the file. One or more of the following statements, where indicated, explain this deletion.

- ☒ Deletions were made pursuant to the exemptions indicated below with no segregable material available for release to you.

Section 552Section 552a☐ (b)(1)☐ (b)(7)(A)☐ (d)(5)☒ (b)(2)☐ (b)(7)(B)☐ (j)(2)☐ (b)(3)☐ (b)(7)(C)☐ (k)(1)☐ (b)(7)(D)☐ (k)(2)☒ (b)(7)(E)☐ (k)(3)☐ (b)(7)(F)☐ (k)(4)☐ (b)(4)☐ (b)(8)☐ (k)(5)☐ (b)(5)☐ (b)(9)☐ (k)(6)☐ (b)(6)☐ (k)(7)

- ☐ Information pertained only to a third party with no reference to the subject of your request or the subject of your request is listed in the title only.

- ☐ Documents originated with another Government agency(ies). These documents were referred to that agency(ies) for review and direct response to you.

Pages contain information furnished by another Government agency(ies). You will be advised by the FBI as to the releasability of this information following our consultation with the other agency(ies).

Page(s) withheld inasmuch as a final release determination has not been made. You will be advised as to the disposition at a later date.

Pages were not considered for release as they are duplicative of _____

Page(s) withheld for the following reason(s): _____

- ☒ The following number is to be used for reference regarding these pages:

MIOG DE II Sec 12 p49 thru 57

XXXXXXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X for this page X
XXXXXXXXXXXXXXXXXXXX

XXXXXX
XXXXXX
XXXXXX

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 12 - 58

12-15 DEMONSTRATIONS AND TOURS

(1) Only authorized firearms instructors may present "live fire" demonstrations, and then only with the express consent of the SAC or designee.

(2) Any other SA may present Bureau firearms for demonstration using "red-handle" weaponry or live weapons equipped with trigger guard locks or similar devices which prevent the weapon from firing.

(3) The safe condition of all weapons used for demonstration should be verified by a Bureau firearms instructor BEFORE use. (The general safe condition of firearms is action open, safety on, and weapon free of any live ammunition.) Demonstration weapons should never be pointed at another person.

EFFECTIVE: 04/07/97

12-16 MEDICAL PROFILE SYSTEM - MEDICAL MANDATES (RESTRICTIONS)

(1) Agents on medical mandates are to be permitted to participate in firearms training, including defensive tactics, PROVIDED the Agent's evaluating physician is fully familiar with the Agent's condition, the nature of the training to be undertaken, and furnishes a written statement that, in the physician's opinion, such participation would not be injurious to the Agent's health or dangerous to others. (See MAOP, Part I, 20-5.2.1 (2).)

(2) In instances where the evaluating physician does not certify the Agent to attend training and the prospects for future participation are remote due to the Agent's condition, authority to carry a firearm will be rescinded and any Bureau-issued weapon turned in. (See MAOP, Part I, 20-5.2.1 (3).)

EFFECTIVE: 04/07/97

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 12 - 59

12-17 TRAINING SAFETY

(1) All training exercises or scenarios which incorporate the use of loaded or unloaded firearms must be supervised by a currently qualified Bureau firearms instructor.

(2) The supervising firearms instructor must ensure that:

(a) all necessary firearms and ammunition safety checks are conducted prior to commencement of training.

(b) all firearms safety rules and precautions are adhered to by all participants.

(c) all facilities and training props are safe and absent of potential hazards to all personnel.

(3) The primary instructor may designate assistants as required; however, the ultimate responsibility for safety rests with the primary instructor.

(4) Under no circumstances will the primary or assistant instructors become active participants or role players during the training exercise or scenarios.

EFFECTIVE: 04/07/97

12-17.1 Deleted

EFFECTIVE: 04/07/97

12-17.1.1 Deleted

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 12 - 60

EFFECTIVE: 04/07/97

| 12-17.1.2 | Deleted |

EFFECTIVE: 04/07/97

| 12-17.1.3 | Deleted |

EFFECTIVE: 04/07/97

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 1

SECTION 13. LABORATORY DIVISION AIDS TO INVESTIGATIONS

13-1 INTRODUCTION TO FBI LABORATORY DIVISION

EFFECTIVE: 05/25/90

| 13-1.1 | Deleted |

EFFECTIVE: 04/07/97

13-2 AVAILABILITY AND USE OF LABORATORY FACILITIES

EFFECTIVE: 05/25/90

13-2.1 Availability of the FBI Laboratory

As a general rule, services of the FBI Laboratory are available to:

(1) U.S. Attorneys, military tribunals, and all other Federal agencies in both civil and criminal matters. (Requests from USAs for any Laboratory services (including trial charts), examinations and testimony of FBI Laboratory experts should be made through FBI field offices.)

(2) All duly constituted state, county, and municipal law enforcement agencies in the United States and territorial possessions in connection with their official investigations, but in criminal matters only.

EFFECTIVE: 05/25/90

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 2

13-2.1.1 Stipulations

All Laboratory services, including expert witnesses, are rendered free of all cost to the requesting agency, but in offering these services, experience has dictated the following limitations in the interest of economy to avoid duplication of effort and to ensure the proper administration of justice:

(1) No examination will be conducted on any evidence which has been previously subjected to the same type of technical examination. This requirement is intended to eliminate duplication of effort and ensure the integrity of the evidence is maintained. An exception may be granted by the Laboratory Division to this policy when there exist compelling reasons that a reexamination be conducted. These reasons should be set forth in individual letters from the director of the laboratory which conducted the original examination, the prosecuting attorney, and the investigating agency which collected and submitted the evidence for laboratory analysis. (Note: A check will be searched through the National Fraudulent Check File even though it has been technically examined by or searched through a check file maintained by another agency.)

(2) No testimony will be furnished if testimony on the same technical subject and in the same case is to be given for the prosecution by another expert.

(3) No request for examination will be accepted from a nonfederal law enforcement agency in connection with criminal cases if it is indicated that only a civil case will grow out of it.

(4) No requests for examination will be accepted from other laboratories which have the capability of conducting the requested examinations. (Exceptions to this policy may be made, in extenuating circumstances, upon approval of the Assistant Director of the Laboratory.)

EFFECTIVE: 04/07/97

| 13-2.1.2 | Deleted |

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 3

EFFECTIVE: 09/09/93

13-2.2 Use of Other Laboratories or Other Forensic Experts

Since materials of evidentiary value located at a crime scene or otherwise obtained during FBI investigative activities offer invaluable potential for investigative information and probative results, these materials should be submitted, except in circumstances detailed in subsection 13-2.2.2 below, to the FBI Laboratory in lieu of other laboratories or other forensic experts because

(1) The facilities of and the expertise within the FBI Laboratory provide the best in available scientific analyses and technical services

(2) The FBI is appropriated money yearly by Congress to operate its own Laboratory to provide laboratory services in matters of interest to the Bureau.

EFFECTIVE: 04/07/97

13-2.2.1 Cases Involving Joint Jurisdiction

Diplomacy and good judgment must be exercised in the instances which arise in cases of joint jurisdiction where state, local, and/or other Federal laboratories either handle or maintain custody of materials of evidentiary value obtained by their personnel either prior to or after FBI involvement so as to:

(1) Protect the integrity and "chain of custody" of these materials of evidentiary value in the event the final mutual agreement is that the matter under investigation is to be prosecuted in the Federal judicial system with the FBI having the responsibility of primary jurisdiction and

(2) Demonstrate the FBI has the proper professional respect for the technical and scientific competence of these other laboratories and the investigative efforts of their law enforcement personnel.

(3) In matters where physical evidence has been

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 4

previously examined by a state or local crime laboratory and the FBI Laboratory is directed by the Department of Justice to conduct a reexamination, the head of the laboratory which conducted the original analysis will be promptly notified of this action by the Laboratory Division.

EFFECTIVE: 05/25/90

13-2.2.2 Cases Involving Sole FBI Jurisdiction (See MIOG, Part II, 13-2.2.)

When circumstances dictate, FBIHQ will consider requests for the use of non-Bureau forensic experts. The following conditions must be observed:

(1) Only the FBI Laboratory should conduct forensic examinations of evidence in FBI investigations. Only under extenuating circumstances should other laboratories or forensic experts in private practice be consulted or their services requested. This should only occur after prior contact, and with the approval of, the FBI Laboratory by electronic communication (EC), teletype, or telephone and then confirmed by EC or teletype. Such communications should include:

(a) A synopsis of the circumstances necessitating the use of an outside forensic expert.

(b) The name of the local expert(s) and their local laboratory affiliation, if any,

(c) The name and office telephone number of the case Agent, and

(d) The personal endorsement of the SAC that such action is needed.

(2) This procedure is necessary to ensure:

(a) That the needed services or examinations cannot be performed in a timely fashion by submitting the evidence to the FBI Laboratory due to extreme urgency of the situation, or that FBI Laboratory personnel could not travel to the requesting location and perform the services or examinations;

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 5

(b) That when circumstances so warrant, and FBI Laboratory approval is given, only competent and reputable forensic experts be utilized who are recognized as reliable within the forensic science community.

(3) If FBI Laboratory approval is obtained for the use of non-FBI Laboratory experts, those experts must assure that all necessary examinations are being performed since federal violations frequently require different elements of proof than do state or local violations of the same or similar nature and,

(a) That nothing will be done which will destroy the usefulness of the evidentiary material;

(b) That the local expert be advised of the willingness of the FBI Laboratory to be consulted on the scientific and technical aspects of the examination(s) and to provide additional examinations which may not be possible locally;

(c) That a copy of the local expert's examinations report be promptly furnished to the FBI Laboratory.

(4) Under no circumstances should "curbstone" opinions be sought of local scientific or technical personnel to assess the potential value of evidentiary materials prior to submitting these items to the FBI Laboratory for examination. Preliminary local analyses could

(a) Cause alteration and/or contamination of these materials,

(b) Create a conflict of opinion due to variations in testing procedures,

(c) Unduly complicate the "chain of custody,"

(d) Severely hamper the effectiveness of the Bureau's efforts, and

(e) Create unnecessary legal issues which could arise subsequently in the prosecution process.

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 6

EFFECTIVE: 04/07/97

13-3 REQUESTING LABORATORY ASSISTANCE

The information under this caption as well as that contained elsewhere in this section under the particular type of examination or assistance desired should be consulted to facilitate the submission of requests to the Laboratory Division.

EFFECTIVE: 05/25/90

13-3.1 Requests for Examination(s) of Evidence (See MIOG, Part I, 9-7; II, 13-17.3.)

A request for an examination must be in written form and forwarded with the evidence. A telephonic request must be followed with a written official communication. The incoming communication must be sent with each case and should include a listing of the suspect/subject, victim, violation, location and date of offense, case file number, a brief description of the case, a detailed description of the evidence enclosed, the request of the Laboratory and a contact name and number. A written request for Laboratory Division services must bear a single title and a single Universal Case File Number. If additional cases need to be intercompared with the listed title, that request should be in the body of the incoming communication, not identified by additional titles. All requests should be addressed to the Director, Federal Bureau of Investigation, with an attention line in accordance with 13-3.1.1 below and contain the following information:

- (1) Reference to any previous correspondence submitted to the Laboratory in the case.
- (2) The nature of and the basic facts concerning the violation insofar as they pertain to the laboratory examination.
- (3) The name(s) and sufficient descriptive data of any subject, suspect, or victim.
- (4) Each case submitted to the Laboratory must be individually packaged and placed in an appropriate evidence container. The evidence container must be placed under proper seal, labeled with

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 7

appropriate warning labels, contain a single titled communication, and shipped via trackable carrier. Lab exam requests should contain a list of the evidence being submitted either "herewith" or "under separate cover." (Note: Due to evidential "chain of custody" requirements, all evidence sent through the U.S. Postal Service (USPS) system must be registered mail and not by parcel post or regular mail. If United Parcel Service, Federal Express, or air freight is used, utilize their "acknowledgment of delivery," "protective signature," "security signature," or any other such service which provides the same protection as USPS registered mail.) Only evidence for the first captioned case should be submitted with each communication. (See MIOG, Part II, 13-3.1.2 (9), 13-6.7 and 13-6.7.1.)

(a) "Herewith": This method is limited to certain small items of evidence which are not endangered by transmission in an envelope. Utilize the specially designed evidence envelope (Form FD-632). Execute written portion of envelope BEFORE placing evidence inside to preclude damaging or altering evidence and to prevent addition of indented writing. Insert the evidence and securely seal the envelope. Fold up the flap marked "PLEASE STAPLE CORRESPONDENCE TO THIS FLAP" and securely attach the written communication which should state "Submitted herewith are the following items of evidence."

(b) "Under separate cover": This method is generally used for shipment of numerous and/or bulky items of evidence. The written communication should state "Submitted under separate cover by (list the method of shipment be it USPS, United Parcel Service, Federal Express, or air freight) are the following items of evidence." For further information concerning the preparation of packages sent under separate cover see 13-3.1.2 below as well as 13-6.6 (Packaging Chart) illustrated in the "Electronic Reference Library Searching Guide" Appendix.

(c) "Packaging": An evidence container is defined as any container that houses items of evidence in a manner which maintains the integrity of those items. To further this definition, a primary container is the container that is in direct contact with the evidence. For example, an envelope housing a fraudulent document or a vial containing blood would be considered a primary container. A primary container must be placed in a secondary container which must be leakproof and puncture-resistant, when the evidence so warrants additional protections. A secondary container is needed only when wet evidence, such as liquid blood, or a sharp item, such as a needle or a knife, is submitted to the Laboratory for examination. Each item of evidence must be packaged separately to avoid contamination. Each case must be submitted individually. The Laboratory Division will

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 8

strictly endorse the related portions of MIOG, Part II, 13-3.1.2(3) and 13-3.1.2(4).

(d) "Sealing": All containers must be properly sealed with tamper-evident tape. A container is properly sealed only if its contents cannot readily escape and if entering the container results in obvious damage/alteration to the container or its seal. A proper seal consists of taping the evidence container over or along the opening with tamper-evident tape and placing the initials of the person creating the seal over the tape. A proper seal is not created by simply stapling the evidence container closed, nor is it properly sealed when a container opening is exposed. Tamper-evident tape is available through FBI central supply or the Evidence Control Technician. (See 13-3.1.2.)

(e) "Warning Labels": A warning label alerts the recipient of the potential hazards of the evidence enclosed, therefore appropriate warning labels must be placed on an evidence container in a visible area. Biological hazards (biohazards) fall under the Bloodborne Pathogen guidelines. (See 13-3.1.2.)

Biohazardous evidence (evidence containing any biological material) must be labeled with a biohazard sticker. If the item is or contains dried body fluids, such as blood, semen, or saliva, a primary container is the only container needed and the biohazard sticker is placed on the outside of the primary container. If the item is or contains wet body fluids, the primary container must be placed in a secondary container and the secondary container must be labeled with a biohazard sticker. (See 13-12.4.1.)

Because of the importance of compliance with using proper warning labels, FBIHQ will remind the field of the policy when a noncompliant submission is received. If the case Agent or Evidence Control Technician neglects to affix appropriate warning labels, the examiner or examiner's Unit Chief will call the supervisor of the case Agent or Evidence Control Technician to alert that supervisor of the noncompliant submission. Pursuant to the contact, a letter describing the noncompliant submission will be sent to the Assistant Director in Charge (ADIC) or Special Agent in Charge (SAC).

(5) A request stating what types of examinations are desired. Include, if applicable, comparisons with other cases, listing captions of these cases and Bureau file numbers, if available.

(6) Information as to where the original evidence is to be returned as well as where the original Laboratory report is to be

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 9

sent.

(7) A statement, if applicable, as to whether

(a) The evidence has been examined previously by another expert in the same technical field (provide a copy of any report(s) generated by other experts, if available)

(b) Any local controversy is involved in the case,
or

(c) Any non-Bureau law enforcement agencies have an interest in the case.

(8) Notification of the need and reason(s) for an expeditious examination bearing in mind this treatment should not be routinely requested.

(9) If damage occurs in the mail system or evidence is improperly packaged and the integrity of the evidence has been jeopardized as a result, the case Agent will be notified. If the integrity of the evidence has been compromised, a decision will be made by appropriate laboratory personnel as to what, if any, forensic examinations can or will be conducted. This policy is imperative to preserve the integrity of the evidence and to protect the safety and well being of the persons handling these submitted materials.

EFFECTIVE: 11/21/97

13-3.1.1 Attention Lines for Communications and Packages (See MIOG, Part II, 13-3.1, 13-3.1.2(8) and (10).)

The following guidelines should be adhered to as closely as possible to avoid any unnecessary delay in the routing of mail at FBI Headquarters.

(1) All requests for a laboratory examination should be marked "Attention: FBI Laboratory, Evidence Control Center."

(2) Deleted

(3) Deleted

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 10

(4) Requests for photographic processing ONLY should be submitted on the FD-523. (Note: Whenever a package containing exposed film is sent to the Laboratory the word "FILM" should be clearly marked on the outside of the package.)

(5) Requests for photographic laboratory examination of any kind should be marked "Attention: FBI Laboratory, Special Photographic Unit."

(6) Requests for BOTH photographic processing and a fingerprint examination should be submitted on the FD-523 and, in the area for request, marked "Attention: Laboratory Division, Evidence Control Center."

(7) Requests for the enhancement, processing and examination of video imagery where no comparison with known photographs or items of clothing are required or requests for the production of video tape demonstrative evidence should be marked "Attention: FBI Laboratory, Special Photographic Unit."

EFFECTIVE: 07/25/97

13-3.1.2 Shipment of Evidence "Under Separate Cover" (See MIOG, Part II, 13-3.1(4)(b).)

The following steps should be followed to properly prepare a package for shipment of numerous and/or bulky items of evidence apart from the original written request for the examination(s). For additional guidance and instructions see 13-3.1(4)(b), (c), (d), and (e) above and 13-6.6 (Packaging Chart) below. (Note: Comply with the following steps (1) through (9) if a cardboard box is used and step (10) if a wooden box is used):

(1) Take every precaution to preserve the items of evidence as outlined in the applicable sections of the Evidence Chart (13-6.7) as well as afford appropriate physical protection of the latent fingerprints thereon to include identification with the word "LATENT." (See (10) below.)

(2) Choose a cardboard box suitable in size.

(3) Place nonporous items of evidence in a separate container to avoid contamination and for preservation of latent

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 11

prints. (See Part II, 13-3.1(4)(c) and 13-3.1.2 (10) below.)

(4) Do not place evidence from more than one case in the same box. (See Part II, 13-3.1(4)(c) and 13-3.1.2 (10) below.)

(5) Pack the evidence securely within the box to avoid damage in transit or puncture of box and protrusions/loss of evidence. (See (10) below.)

(6) Seal the box with gummed tape and clearly mark the outer portions of the box with the word "EVIDENCE." (Note: If any of the evidence in the box is to be subjected to a latent fingerprint examination, also clearly mark the outer portions of the box with the word "LATENT.")

(7) Place a copy of the original written request for the examination(s) in an envelope marked "INVOICE" and securely affix this envelope to the outside of the sealed box.

(8) Enclose the sealed box in wrapping paper and seal the wrapping paper with gummed tape. Prepare the address label, addressing the package to the Director, Federal Bureau of Investigation, 935 Pennsylvania Avenue, NW, Washington, D.C. 20535-0001, with the proper attention line as outlined above in 13-3.1.1. Cover the label with yellow transparent tape to identify the shipment as evidence and place it securely on the package.

(9) Ship the package by U.S. Postal Service, United Parcel Service, Federal Express, or air freight in accordance with the note in 13-3.1(4) above and the Evidence Chart (13-6.7).

(10) Choose a durable wooden box suitable in size and

(5). (a) Comply with the above steps (1), (3), (4), and

(b) Securely fasten the lid on the box and address it to the Director, Federal Bureau of Investigation, 935 Pennsylvania Avenue, NW, Washington, D.C. 20535-0001, with the proper attention line as outlined above in 13-3.1.1.

(c) Place a copy of the original written request for the examination(s) in an envelope marked "INVOICE." Place the invoice envelope in a clear plastic cover, and tack it to the box.

(d) Comply with step (9) above.

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 12

EFFECTIVE: 07/25/97

13-3.2 Requests for Other Laboratory Assistance

Requests for artist conceptions should be submitted on Form FD-383. Requests for photographic processing, printing, enlargements, etc., where no examination is involved must be submitted on an FD-523. Requests for other Special Projects Section services should be submitted on an FD-790. Requests for translations, trial exhibits, and on-the-scene Laboratory assistance in photographic surveillances, evidence examinations, or crime scene searches (e.g., bombings) and questions concerning photographic, polygraphic, forensic training, or other Laboratory matters should be submitted in a written communication, in triplicate, directed to the FBI Laboratory. However, if time is of the essence or the exigencies of the case are such, telephonically contact the Laboratory Division, referring to the "FBI Laboratory Directory of Support Services," for the unit which provides the desired assistance. If after consulting the Directory, problems or questions still exist, call the office of the Assistant Director, extension 4410.

EFFECTIVE: 09/03/93

13-4 RESULTS OF EXAMINATION(S) OF EVIDENCE

The results of evidential examinations conducted in the Laboratory are recorded in a written report.

EFFECTIVE: 11/23/87

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 13

13-4.1 Dissemination of Laboratory Report (See MAOP, Part II, 10-13.13.)

Normally three copies of each laboratory report are furnished to the

- (1) Office(s) contributing evidence,
- (2) Office of origin,
- (3) Offices designated by the contributor(s), and

(4) Those offices determined by the Laboratory to have an interest in the case depending on the results of the examination(s).

(a) The original and two copies of the report will usually be sent to the office of origin in those instances where there are several offices contributing evidence, as well as those instances in which a contributing office makes such a request.

(b) If evidence is submitted to the Laboratory by a non-Bureau agency in a case in which the Bureau has or may have a joint jurisdiction, a report will be furnished the contributor with three copies of the report designated for interested Bureau offices, to include the office of origin.

EFFECTIVE: 09/24/93

13-4.2 Inclusion of Laboratory Report in Other Reports

A copy of a laboratory report may be included in other reports prepared in the field. Some laboratory reports are sent to the field under the cover of a Laboratory Transmittal Form (7-72) commonly referred to as the Administrative Page(s). These Administrative Pages are not part of the laboratory report and therefore should not be included in any reports prepared in the field.

EFFECTIVE: 01/26/83

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 14

13-4.3 Rule 16. (Discovery and Inspection)

A portion of Rule 16 of the Federal Rules of Criminal Procedure states "Reports of Examinations and Tests. Upon request of a defendant the government shall permit the defendant to inspect and copy or photograph any results or reports of physical or mental examinations, and of scientific tests or experiments, or copies thereof, which are within the possession, custody, or control of the government, the existence of which is known, or by the exercise of due diligence may become known, to the attorney for the government, and which are material to the preparation of the defense or are intended for use by the government as evidence in chief at the trial." This request must be made before the court and "Upon a sufficient showing the court may at any time order that the discovery or inspection be denied, restricted, or deferred, or make such other order as is appropriate."

EFFECTIVE: 01/26/83

13-4.4 Laboratory Reports and the Disposition of Submitted Evidence

(1) Each laboratory report will normally contain a statement concerning the original evidence being returned herewith, under separate cover, or with the results of another examination such as a latent fingerprint examination.

(2) Whenever original evidence is returned by the Laboratory to the contributing office(s) or to the office of origin, upon the request of the contributor(s), it should be checked against those items listed in the written request as well as in the laboratory report to ensure all the evidence has been returned.

(a) If any discrepancies exist, extreme care should be exercised in examining all of the packing material utilized in the shipment of the evidence in order that the missing items will not be inadvertently disposed of with this material. The FBI Laboratory should be advised immediately of any discrepancies.

(b) |Deleted|

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 15

EFFECTIVE: 04/07/97

13-5 TESTIMONY OF LABORATORY EXAMINERS

EFFECTIVE: 01/26/83

13-5.1 Availability of Service

Laboratory examiners are available for expert testimony concerning their examinations provided no other expert is used by the prosecution in the same scientific field. (Note: This restriction is generally used in the interest of economy and to avoid duplication of effort.)

EFFECTIVE: 01/26/83

13-5.1.1 Testimony at Trials

The absence of examiners from FBIHQ should be kept to a minimum; therefore,

(1) Every effort should be made to utilize the services of these witnesses as quickly as possible, consistent with good trial procedures.

(2) Whenever practical, arrange for their immediate release following court appearance.

(3) In most cases the presence of an expert witness is NOT required by the court during the jury selection and, consequently, he/she need not be present when the case is called.

(4) Whenever it is possible to anticipate when the expert testimony will be required, arrangements should then be made to have the witness present at that time, rather than earlier in the trial.

(5) Laboratory should be notified of the trial dates or other judicial deadlines as soon as they are known or set.

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II.

PAGE 13 - 16

EFFECTIVE: 07/25/97

13-5.1.2 Grand Juries and Preliminary Hearings

(1) Laboratory experts are available to testify at such hearings but requests for their appearance should not be made unless absolutely necessary because in most cases the laboratory report, an affidavit, or the testimony of the case Agent will suffice.

(2) If all attempts to obviate the appearance of a Laboratory expert have been exhausted, the FBI Laboratory should be advised in detail of the unusual circumstances which make the presence of an expert absolutely necessary.

EFFECTIVE: 01/26/83

13-6 HANDLING OF PHYSICAL EVIDENCE

EFFECTIVE: 01/26/83

13-6.1 Definitions of Evidence

(1) That which is legally submitted to a competent tribunal as a means of ascertaining the truth of any alleged matter of fact under investigation before it.

(2) Anything which a suspect leaves at a crime scene or takes from the scene or which may be otherwise connected with the crime.

EFFECTIVE: 01/26/83

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 17

13-6.1.1 Terminology

"Physical," "real," "tangible," "laboratory," and "latent," are all adjectives to describe the types of evidence which the FBI Laboratory Division examines.

EFFECTIVE: 09/24/93

13-6.2 Purpose of Physical Evidence

- (1) Aids in the solution of the case because it can
 - (a) Develop M.O.'s or show similar M.O.'s.
 - (b) Develop or identify suspects.
 - (c) Prove or disprove an alibi.
 - (d) Connect or eliminate suspects.
 - (e) Identify loot or contraband.
 - (f) Provide leads.
- (2) Proves an element of the offense, for example.
 - (a) Safe insulation, glass or building materials on suspect's clothing may prove entry.
 - (b) Stomach contents, bullets, residue at scene of fire, semen, blood, toolmarks may all prove elements of certain offenses.
 - (c) Safe insulation on tools may be sufficient to prove violation of possession of burglary tools statutes.
- (3) Proves theory of a case, for example,
 - (a) Footprints may show how many were at scene.
 - (b) Auto paint on clothing may show that a person was hit by car instead of otherwise injured.

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 18

EFFECTIVE: 01/26/83

13-6.3 Nature of Physical Evidence

For the most part, physical evidence falls into two classifications.

EFFECTIVE: 01/26/83

13-6.3.1 Evidence with Individual Identifying Characteristics

This evidence can be positively identified as having come from a specific source or person if sufficient identifying characteristics, or sufficient microscopic or accidental markings are present. (Examples are: fingerprints, handwriting, bullets, toolmarks, shoe prints, pieces of glass and plastic where the broken edges can be matched, and wood where broken/cut surfaces can be matched and fabric and tape (torn ends).)

EFFECTIVE: 04/01/96

13-6.3.2 Evidence With Class Characteristics Only

(1) This evidence, no matter how thoroughly examined, can only be placed into a class. A definite identification as to its source can never be made since there is the possibility of more than one source for the evidence found. (Examples are: soil, blood, hairs, fibers, paint from a safe or car, glass fragments too small to match broken edges, and toolmarks, shoe prints, or bullets, in those instances where the microscopic or accidental markings are insufficient for positive identification.)

(2) It is desirable to have evidence that can be positively identified, but the value of evidence with class characteristics only should not be minimized. In cases involving evidence with class characteristics only, the following are desirable:

- (a) A preponderance of such evidence.

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 19

(b) A preponderance of class characteristics within a single item of evidence such as paint with many layers all matching or soil with foreign matter such as paint chips, odd seeds, and safe insulation.

(c) Elimination specimens such as soil from where a suspect claims he/she was or where he/she claims a car was; soil from the surrounding areas to show that a variation does exist; and paint or other materials from a source mentioned in an alibi.

EFFECTIVE: 09/24/93

13-6.4 Crime Scene Search

A crime scene search is a planned, coordinated, legal search by competent law enforcement officials to locate physical evidence or witnesses to the crime under investigation. In order to be effective a crime scene search should include the steps outlined in paragraphs 13-6.4.1 through 13-6.4.8 below. (Note: For additional information concerning a bombing crime scene search see paragraph 13-6.5 below.)

EFFECTIVE: 02/12/92

13-6.4.1 Protect and Secure the Crime Scene

Only persons who have a legitimate investigative interest should be allowed into the crime scene. This number should be kept to a minimum. Too many people in a crime scene can lead to evidence being moved or destroyed before its value as evidence is recognized. Once the scene is established, it should be protected diligently.

EFFECTIVE: 02/12/92

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 20

13-6.4.2 Conduct a Preliminary Survey of the Crime Scene for the
Purposes of Establishing Firm Organizational and Planning
Guidelines

This is the planning stage of the search. The plans
should include:

- (1) Form objectives of the search - what is to be found.
- (2) Take special note of evidence that may be easily
destroyed such as shoe prints in dust, footprints, etc.
- (3) Organize the search.
 - (a) Make assignments for photographs, fingerprints,
plaster casts, and evidence handling.
 - (b) Decide on search pattern, i.e., lane, grid,
spiral or zone searches.
 - (c) Issue instructions to assisting personnel.
- (4) Write a narrative description of the general
conditions of the crime scene. These are the investigator's original
notes which will be used to refresh his/her memory at the trial. They
should be an accurate description of the crime scene and should
include:
 - (a) Date, time, and location of the search.
 - (b) Weather and lighting conditions.
 - (c) Identity of others participating in the search.
 - (d) Assignments given other personnel.
 - (e) Condition and position of evidence found.

EFFECTIVE: 02/12/92

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 21

13-6.4.3 Photograph the Crime Scene

(1) Crime scenes will not remain undisturbed for very long, and therefore should be photographed as soon as possible, preferably before anyone is allowed into the scene.

(2) When possible, a medium-format (120-roll film) camera such as the Mamiya 645 should be used. If not available, then the 35mm camera should be used. Crime-scene photographs will be taken in daylight or with electronic flash; therefore, the best film choice is either Kodacolor Gold 100 or Vericolor Professional III Type S (VPS). If using VPS, set camera and flash ISO settings at 80 instead of 160 which is indicated on the film instructions. It is noted that numerous stages of a crime scene investigation will involve photography. A constant awareness must be maintained in order to ensure that the original crime scene is photographically recorded. As discoveries are made, these also should be photographed.

(a) Exterior crime scene:

1. Establish the location of the scene by taking a series of overall photographs to include a landmark. (360 degrees coverage if possible)

2. Establish the location of the building through a series of overall photographs. (Aerial photographs obtained at a later date may be useful.) Oblique and verticals.

3. Any item of importance should have two additional photographs made of it. A MEDIUM-distance photograph that depicts the item and shows its relative position to other items in the immediate area and a CLOSE-UP photograph with a scale if possible.

4. Take a series of close-up photographs of individual items of evidence to include filling the film frame, showing proper perspective and avoiding oblique angles if possible. (Black and white slow-speed film should be used as needed to record shoe prints in dust, documents, fingerprints, etc.)

5. All entrances/exits into the crime scene area should be photographed.

(b) Interior crime scene:

1. Utilizing a series of overall photographs, photograph rooms and other interior areas from all sides in an

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 22

overlapping series. It may be useful to make some photographs with a wide-angle lens, but, as mentioned before, these should be noted on the "photo log," Form FD-674.

2. Any item of importance should have two additional photographs made of it. A MEDIUM-distance photograph that depicts the item and shows its relative position to other items in the immediate area and a CLOSE-UP photograph with a scale if possible.

3. Deleted

4. Deleted

(c) Evidence photographs are needed to:

1. Record the condition of individual items of evidence before recovery. (Photographs must show the evidence in detail and should include a scale, photographer's initials, and the date.)

2. Conduct laboratory examinations of evidence such as shoe prints, tire impressions, and that obtained from bank robberies. (Photography should be performed before any attempts to lift or cast. Photographs should show identifying data as indicated above.)

3. Support testimony given in court.
(Photographs should be of professional quality and very detailed.)

(3) The sequence of photographs varies with each scene. Logic should dictate what order to proceed with photography based on the fragility of a given area and your ability to maintain control of the scene. If you feel that exterior areas are in danger of being contaminated, then start with those. As long as all the needed photographs are made, the order in which they are made is not critical.

(4) Crime-scene photographs should be made with the "normal" lens for the camera in use (80mm lens with the 120-roll film camera, 50mm lens with the 35mm camera) whenever possible. The "normal" lens maintains the same perspective that your eye gives you looking at the scene. A series of overlapping photographs can be made so that all areas of given space are recorded. If using a lens other than the "normal" lens, such as a "wide-angle" lens, to be able to photograph a larger area in a single photograph, it should be noted in the photo log (FD-674). (See paragraph (5).)

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 23

(5) A record of photographs taken should be kept on a "photo log," Form FD-674. It is not necessary to record the shutter speed and f/stop used. It will be very useful to record the item description and, in some cases, the location of an item and/or the photographer may be significant. A quick drawing showing this should be done in the provided space on the form. (This drawing in no way is a substitute for the crime scene sketch.) This information can then be used later for identifying photographs and as an aid in testimony.

EFFECTIVE: 02/12/92

13-6.4.4 Sketch the Crime Scene

A crime scene sketch is a handmade pictorial representation of conditions at a crime scene. (Floor plans are sometimes available from commercial concerns to aid in sketching.) It is useful in clarifying investigative data and to make the situation easier to understand by eliminating unnecessary detail. A sketch does not replace photographs at the crime scene and should be used to show:

- (1) Dimensions of rooms, furniture, doors, windows, etc.
- (2) Distances from objects to entrances and exits
- (3) Distances between objects (including persons/bodies)
- (4) Measurements showing the exact location of items of evidence. Each object should be located by two measurements from nonmovable items, such as doors, walls, etc.
- (5) Point-of-view locations of photographs

EFFECTIVE: 02/12/92

13-6.4.5 Process for Fingerprints

See Part II, Section 15, of this manual for instructions on fingerprinting a crime scene.

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 24

EFFECTIVE: 02/12/92

13-6.4.6 Make Shoe Print/Tire Tread Casts and/or Lifts

See paragraphs 13-19.1 through 13-19.1.3 elsewhere in this section for instructions on the making of shoe print/tire tread cases and/or lifts.

EFFECTIVE: 02/12/92

13-6.4.7 Collect, Identify and Preserve the Evidence

For additional information on the collection, identification, and preservation of items of evidence, see paragraph 13-6.7 (Evidence Chart) and/or the appropriate paragraphs elsewhere in this section concerning the type of examination desired.

(1) Collection.

(a) All evidence must be collected legally in order to be admissible in court at a later date. For further instructions on the legality of crime scene searches, refer to the Legal Handbook for Special Agents.

(b) Evidence found during a search should be displayed immediately to another Special Agent so that both Agents can testify to its source.

(c) All evidence should be fully described in the searcher's notes and photographed in place prior to being picked up.

(d) If appropriate, Form FD-597 (Receipt for Property Received/Returned/Released/Seized) should be properly executed and the copy furnished to the contributor and/or the person(s) to whom the property is being surrendered. The original of Form FD-597 is to be placed in the 1-A exhibit envelope of the case file.

(2) Identification.

All articles of an evidentiary nature should be carefully marked for identification, preferably on the article itself,

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 25

in a manner not to injure the evidence itself and not to be obliterated. These markings, to include initials, date and case number, enable the person finding the evidence to testify, at a later date, to the finding of it.

(3) Preservation.

(a) Each item of evidence should be placed in a suitable container, such as pillboxes, plastic vials or strong cardboard boxes. The container should be suitably identified and sealed.

(b) Prepare appropriate 1-A envelopes (FD-340a and/or FD-340b) and/or Forms FD-192 and store the evidence in designated areas.

(c) For submission of evidence to the laboratory for examination see 13-3 (Requesting Laboratory Assistance), 13-6.6 (Packaging Chart), and 13-6.7 (Evidence Chart).

(d) The legal "chain of custody" must be maintained at all times.

EFFECTIVE: 02/12/92

13-6.5 Bombing Crime Scene Search

Bombing crime scenes, in spite of their massive destruction, must be conducted on the theory that everything at the scene prior to the explosion is still in existence unless it has been vaporized by the explosion. Locating and identifying items is the problem. The often-used statement that so much is destroyed by the explosion that the cause must remain unknown is rarely true. Due to various factors, the exact amount of explosives used cannot normally be determined based on an evaluation of the damage at the scene. (Note: The information contained in 13-6.4 through 13-6.4.7 concerning a crime scene search also applies to a bombing crime scene search.)

EFFECTIVE: 12/05/85

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 26

13-6.5.1 Purpose of Bombing Crime Scene Search

(1) The purpose of a bombing crime scene search is to determine what happened, how it happened, and gather evidence to identify bomb components, reconstruct the explosive device and compare it with items of evidence identifiable to a suspect or to previous bombings.

(2) The office of origin should contact the Laboratory as soon as feasible to advise of the bombing and pertinent details. The Laboratory will search its archives in order to advise the field office of any similar bombing incidents from the past.

EFFECTIVE: 04/07/97

13-6.5.2 Special Considerations for a Bombing Crime Scene Search

The following steps are to assist in the preparation, supervision, and evaluation activity connected with the scene of a bombing. The topics covered are not meant to be all inclusive and no attempt has been made to comment on the many aspects of the bombing investigation.

(1) Plan of action: Formulate a plan adapted to the particulars of the bombing crime scene. This plan will include consideration of the creation of an on-scene command post; establishment of lines of supervision; assignment of various tasks such as photographing, fingerprint processing, crowd control, collection of evidence, etc.; protection of the crime scene; obtainment of needed equipment; periodic evaluation of progress; providing of pertinent information to the public; safety; etc.

(2) Command post: Consider establishing an on-scene command post, separate from the investigative command post, particularly at a large bombing which may require days or weeks to complete the crime scene search. The command post should coordinate efforts amongst Bureau personnel and between representatives of other agencies and utilities as well as handle inquiries from sightseers, persons associated with the scene, relatives of the victims, and the press.

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 27

One person should be in overall charge of the bombing investigation, another over the actual crime scene search, and another over the collection of the evidence. These three individuals must maintain close coordination and expeditiously exchange information on a continual basis. The evidence coordinator will report directly to the crime scene coordinator who in turn will report directly to the individual responsible for the overall bombing investigation.

(3) Safety: Evaluate safety conditions at the outset of the crime scene search and on a continual basis throughout the search consider the possibility of a second bomb, a "jammed" bomb, or live explosives being in the debris and the safety of crowds, nearby residents, and personnel at the crime scene not only from additional explosions but also from such dangers created by utilities, weakened walls, etc.

(a) Ensure all crime scene personnel are current with Tetanus and Hepatitis B vaccine.

(b) Dust masks should be worn at all times while present at the crime scene, especially when death occurs and suspect carcinogens are present.

(c) Annual physical for potential crime scene personnel and individuals which have worked on major crime scenes is recommended.

(d) All crime scene clothing should be detoxified prior to leaving the crime scene, even if the crime scene personnel are returning the following day. Caution should be exercised when storing soiled crime scene clothing in a hotel room or at the searcher's residence. Many contaminants may be adhering to this clothing and could cause illness to an individual not associated with the crime scene.

(e) Prior to allowing the search team access to the crime scene, especially in the event of a large bombing, the crime scene should be examined for the presence of a radioactive residue, either associated with the bomb or the bombing scene.

NOTE: Bureau bomb technicians, Laboratory explosive specialists, public safety bomb squad or military EOD personnel should be contacted if a bomb is located.

(4) Protection of crime scene: Take adequate safeguards to protect the crime scene from fire, law enforcement, utility, and

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 28

rescue personnel as well as others such as sightseers, victims, and individuals with a personal interest in the property. Also, since most residues remaining after an initiation of an explosive are water soluble, the crime scene, as much as possible, should be protected against exposure to excessive moisture be it from rain, snow, broken water pipes, or any other source.

(5) Photographs: Take appropriate photographs to give a photographic representation of the crime scene (see 13-6.4.3 as a guide). These photographs should be made immediately before, periodically during, and at the completion of the crime scene activity. Properly identify each photograph, coordinate the photographs with diagrams and/or blueprints or maps, and consider the advisability of aerial photographs.

(6) Bomb scene specialists: Have some specialists trained in handling and processing bomb scenes or make arrangements for obtaining such individuals from the Laboratory Materials and Devices Unit. Although the basic principles of conducting a crime scene search apply in a bomb scene search, individuals with specialized knowledge of explosives, improvised explosive devices, damage produced by explosive charges, and other facets associated with bomb scene searches, such as the search and collection of physical bombing evidence, are extremely valuable to the processing of a bomb scene effectively and efficiently. These specialists need not be qualified bomb disposal specialists. They should be the first persons, if possible, to be selected for the evidence and crime scene search coordinator positions.

(7) Equipment: Promptly make arrangements to obtain the necessary equipment to move the debris and material at the scene. Although the equipment needed at the scene varies, the following have been used:

(a) Hand tools: Shovels, rakes, brooms, boltcutters, wire cutters, sledgehammer, hammer, screwdrivers, wrenches, chisels, hacksaw, magnet, flashlights, knife, 50-foot measuring tape, and traffic wheel measuring device.

(b) Other light equipment: Screens for sifting debris, wheelbarrows, metal trash cans, power saw, cutting torch equipment, ladders, portable lighting equipment, metal detector, large plastic sheets, photographic equipment, and parachute harness with related rope and pulleys.

(c) Heavy equipment: Truck, front-end loader,

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 29

bulldozer, crane, and shoring materials.

(d) Personal equipment: Hard hats, safety goggles, gloves (work and rubber types), foul weather clothing, coveralls, and work shoes.

(e) Crime scene kit: Usual equipment used for the collection, preservation, and identification of physical evidence.

(f) Vehicle: If the bombed target was a vehicle, bring an identical vehicle, if possible, to the scene to assist in identifying fragmented and mutilated items.

(8) Search for evidence: Bear in mind the search for evidence at a bombing crime scene is important because the crime may contain principal evidence which will lead to the identification of the bomber(s) and/or assist in the successful prosecution of the matter. The following guidelines are general in nature as the exact method of searching depends on various uncontrollable factors:

(a) Place one person in overall charge of the collection of the evidence from the various collectors as valuable evidence may not be admissible in court if a proper "chain of custody" cannot be established.

(b) Do not stop the search after a few items of evidence have been found. Experience has shown that a thorough, persistent search will locate remains of most of the bomb components.

(c) Avoid the tendency to concentrate only on physical evidence, such as safety fuse, detonating cord, blasting caps, leg (electrical) wire, dynamite wrappers, batteries, clock and timing devices, electronic and electrical components, metal end cap from a TNT block, plastic end cap from a C4 block, explosive residues, and unconsumed explosives, which may represent a bomb as this can result in overlooking other valuable evidence, such as fingerprints, hair, fibers, soil, blood, paint, plastic, tape, tools, toolmarks, metals, writing, paper, printing, cardboard, wood, leather, and tire tread-shoe print impressions.

(d) Conduct a well organized, thorough, and careful search to prevent the necessity of a second search. However, have a secure "dump" area for debris in the event a second search is necessary.

(e) | Simultaneously commence the scene search from

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 30

both the site of the explosion and from the extreme perimeter toward the center. If the bomb crater is in earth, obtain soil samples from the perimeter of the crater, as well as from the sides and bottom, making sure to dig into the substrata. If the crater is in another material, obtain similar samples.

(f) Sift small debris through a 1/4-inch wire screen onto an insect-type wire screen. Usually these screens are placed on 2-foot square wooden frames constructed from 2- by 4-inch lumber. NO more than three workers should work on a screen.

(g) X-ray the bodies of living and deceased victims who were in close proximity of the explosion site for possible physical evidence and if possible, have the evidence removed. Their clothing should be retained as it may contain explosive residues. Also, obtain all medical reports concerning the victims' injuries/circumstances of death.

(h) Search a sufficient distance from the site of the explosion as evidence has been found several blocks from the sites of large explosions.

(i) Determine the possible flight paths of bomb components to prevent needless searching.

(j) Search trees, shrubbery, telephone poles, and the roofs, ledges, and gutters of buildings.

(k) Establish a search pattern for large areas. A line of searchers moving forward has been found to be a satisfactory method. A bomb scene specialist should follow the line of searchers to evaluate the items found, control the searchers, and furnish guidance. If a second search is desired, the positions of the searchers on the line should be rotated.

(l) Retain all items foreign to the scene and items which the searchers cannot identify after seeking the assistance of those familiar with the bombed target.

(m) Obtain known standards of wire and building material from the bomb scene to be submitted to the Laboratory for elimination purposes.

(n) Collect and preserve street signs, such as no parking or stop signs that may have captured explosives residue following the bombing. If it is not possible to remove and collect

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 31

the sign immediately, a plastic bag should be placed over the sign until explosives residues can be removed and packaged for analysis.

(o) Have a chemist screen each crime scene worker for possible contamination with explosives in accordance with existing policy.

(p) Do not wear crime scene clothing that has been used for explosive training, research with explosives, clothing normally used for firearms practice or has been worn at other bombing crime scene searches or the search of a bombing suspect or bomb factory unless the clothing has been thoroughly cleaned by a commercial laundry.

EFFECTIVE: 04/07/97

13-6.6 Packaging Chart (See MIOG, Part II, 13-3.1(4)(b), 13-3.1.2, 13-6.4.7(3)(c), 13-6.7(20)(d); NFIP Manual, Part I, 5-6.3(14)(b).)

The following chart should be followed to properly prepare a package for shipment of numerous and/or bulky items of evidence apart from the original written request for an examination(s). For additional guidance and instructions see 13-3.1.2 (Shipment of Evidence "Under Separate Cover") above.

ILLUSTRATION NOT SHOWN - SEE "ERL SEARCHING GUIDE," APPENDIX

1. Pack bulk evidence securely in box.
2. SEAL box and mark as evidence. Mark "Latent" if necessary.
3. Place copy of transmittal letter in envelope and mark "Invoice."
4. Stick envelope to OUTSIDE of sealed box.
5. Wrap sealed box in outside wrapper and SEAL with gummed paper.
6. Address to: Director

Federal Bureau of Investigation
935 Pennsylvania Avenue, NW
Washington, D.C. 20535-0001
"Attention FBI Laboratory, Evidence
Control Center."

Cover label with yellow transparent tape and attach

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 32

- it securely to the package.
7. If packing box is wooden--tack invoice envelope to top under a transparent yellow cover.

EFFECTIVE: 04/01/96

13-6.7 Evidence Chart (See MIOG, Part I, 91-8(11), 139-3; Part II, 13-3.1(4), 13-3.1.2 (1), (9), 13-6.4.7 (3)(c).)

The following chart is provided to give assistance in the collection, identification, preservation, packaging, and sending of evidence to the Laboratory. This chart should be used in conjunction with similar evidence information contained elsewhere in this section under each type of examination desired. This evidence information and chart are not intended to be all inclusive, and does not pertain to latent fingerprint evidence.

(1) SPECIMEN - ABRASIVES, INCLUDING CARBORUNDUM, EMERY, SAND, ETC.:

- ounce
- (a) STANDARD (AMOUNT DESIRED) - Not less than one
- (b) EVIDENCE (AMOUNT DESIRED) - All
- (c) SEND BY - Registered mail or Federal Express
- (d) IDENTIFICATION - On outside of container: Type of material, date obtained, name or initials
- (e) WRAPPING AND PACKING - Use sturdy containers, such as 35 mm film canister or pharmaceutical container. Seal to prevent any loss.
- (f) REMARKS - Avoid use of envelopes

(2) SPECIMEN - ACIDS:

- (ml.)
- (a) STANDARD (AMOUNT DESIRED) - 100 milliliters
- (b) EVIDENCE (AMOUNT DESIRED) - All to 100 ml.

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 33

Service

(c) SEND BY - Federal Express or United Parcel

(d) IDENTIFICATION - On outside of container: Type of material, date obtained, name or initials

(e) WRAPPING AND PACKING - Plastic or all-glass bottle. Tape stopper. Pack in vermiculite or other absorbent material.

(f) REMARKS - Label "acids-corrosive."

(3) SPECIMEN - ADHESIVE TAPE:

(a) STANDARD (AMOUNT DESIRED) - Recovered roll

(b) EVIDENCE (AMOUNT DESIRED) - All

(c) SEND BY - Registered mail

(d) IDENTIFICATION - On outside of container: Type of material, date obtained, name or initials

(e) WRAPPING AND PACKING - Place on waxed paper cellophane.

(f) REMARKS - Do not cut, wad or distort.

(4) SPECIMEN - ALKALIES - CAUSTIC SODA, POTASH, AMMONIA, ETC.:

(a) STANDARD (AMOUNT DESIRED) - 100 ml., 100 grams (gm.)

(b) EVIDENCE (AMOUNT DESIRED) - All to 100 ml., All to 100 gm.

(c) SEND BY - Federal Express or United Parcel Service

(d) IDENTIFICATION - On outside of container: Type of material, date obtained, name or initials

(e) WRAPPING AND PACKING - Plastic or glass bottle with rubber stopper held with adhesive tape. Pack in sawdust or vermiculite. Label "Corrosive Material-Alkali" and volume.

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 34

(f) REMARKS - Label alkali-corrosive.

(5) SPECIMEN - AMMUNITION (CARTRIDGES): (See (29).)

(a) SEND BY - For instructions re: shipping live ammunition, see 13-12.4.2 in this section.

(b) IDENTIFICATION - On outside of container: Type of material, date obtained, name or initials

(c) WRAPPING AND PACKING - For instructions re: shipping of live ammunition, see 13-12.4.2 in this section. (See also 13-12.4.3.)

(d) REMARKS - Unless specific examination of cartridge is essential, do not submit.

(6) SPECIMEN - ANONYMOUS LETTERS, EXTORTION LETTERS, BANK ROBBERY NOTES: (See (19), (20), (22), (23), (43), (52), (65))

(a) EVIDENCE (AMOUNT DESIRED) - All (Original documents, not copies, whenever possible)

(b) SEND BY - Registered mail

(c) IDENTIFICATION - Initial and date each unless legal aspects or good judgment dictates otherwise.

(d) WRAPPING AND PACKING - Place in proper enclosure envelope and seal with "Evidence" tape or transparent cellophane tape. Flap side of envelope should show (1) wording "Enclosure(s) to FBIHQ from (name of submitting office)," (2) title of case, (3) brief description of contents, and (4) file number, if known. Staple to original letter of transmittal.

(e) REMARKS - Do not handle with bare hands. Advise if evidence should be treated for latent fingerprints.

(7) SPECIMEN - BILE:

(a) STANDARD (AMOUNT DESIRED) - 10 milliliters

(b) SEND BY - Most expeditious means available

(c) IDENTIFICATION - Label container identifying

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 35

sample name of subject, date taken, initials of Agent.

(d) WRAPPING AND PACKING - Container in cardboard box with paper or styrofoam packing.

(e) REMARKS - Hold in freezer until personally delivered or pack in dry ice for mailing by most expeditious means available. Attach autopsy report.

(8) SPECIMEN - BLASTING CAPS (CONTACT MATERIALS AND DEVICES UNIT FOR INSTRUCTIONS.)

(9) SPECIMEN - BLOOD - LIQUID KNOWN SAMPLES: (See 13-8.1.4, 13-8.2.5 (3) & 13-8.4 (5).)

(a) STANDARD (AMOUNT DESIRED) - 1 red top (no preservative) vacutainer vial for serological analysis and 1 purple top (EDTA) vacutainer vial for DNA analysis

(b) EVIDENCE (AMOUNT DESIRED) - All

(c) SEND BY - Air mail special delivery - air freight or similar rapid transit method

(d) IDENTIFICATION - Use adhesive tape on outside of test tube. Name of donor, date taken, doctor's name, name or initials of Agent.

(e) WRAPPING AND PACKING - Wrap in cotton, soft paper. Place in mailing tube or suitably strong mailing carton.

(f) REMARKS - Submit immediately. Don't hold awaiting additional items for comparison. Keep under refrigeration, NOT freezing, until mailing. NO refrigerants and/or dry ice should be added to sample during transit. Fragile label.

(10) SPECIMEN - BLOOD - SMALL QUANTITIES (LIQUID QUESTIONED SAMPLES): (See MIOG, Part II, 13-8.1.4.)

(a) EVIDENCE (AMOUNT DESIRED) - All

(b) SEND BY - Air mail special delivery - air freight or similar rapid transit method

(c) IDENTIFICATION - Use adhesive tape on outside of test tube. Name of donor, date taken, doctor's name, name or initials

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 36

of Agent.

(d) WRAPPING AND PACKING - Wrap in cotton, soft paper. Place in mailing tube or suitably strong mailing carton.

(e) REMARKS - If unable to EXPEDITIOUSLY furnish sample, allow to dry thoroughly on the nonporous surface, and scrape off; or collect by using eyedropper or clean spoon, transfer to nonporous surface and let dry; or absorb in sterile gauze and let dry.

(11) SPECIMEN - BLOOD - SMALL QUANTITIES (DRY STAINS NOT ON FABRICS): (See MIOG, Part II, 13-8.1.4.)

(a) EVIDENCE (AMOUNT DESIRED) - As much as possible

(b) SEND BY - Registered mail

(c) IDENTIFICATION - On outside of pillbox or plastic vial. Type of specimen date secured, name or initials.

(d) WRAPPING AND PACKING - Seal to prevent leakage.

(e) REMARKS - Keep dry. Avoid use of envelopes for scrapings.

(12) SPECIMEN - BLOOD - SMALL QUANTITIES (FOR TOXICOLOGICAL USE): (See MIOG, Part II, 13-8.1.4, 13-8.2.4 (3).)

(a) EVIDENCE (AMOUNT DESIRED) - 20 cc. (Blood and preservative mixture)

(b) SEND BY - Air mail special delivery - air freight or similar rapid transit method

(c) IDENTIFICATION - Use adhesive tape on outside of test tube. Name of donor, date taken, doctor's name, name or initials of Agent.

(d) WRAPPING AND PACKING - Medical examiner should use a standard blood collection kit.

(e) REMARKS - Preservative desired (identify preservation used). Refrigerate. CAN freeze.

(13) SPECIMEN - BLOOD - STAINED CLOTHING, FABRIC, ETC.: (See MIOG, Part II, 13-8.1.4.)

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 37

(a) EVIDENCE (AMOUNT DESIRED) - As found

(b) SEND BY - Registered mail, Federal Express,
United Parcel Service (UPS)

(c) IDENTIFICATION - Use tag or mark directly on
clothes. Type of specimens, date secured, name or initials.

(d) WRAPPING AND PACKING - Each article wrapped
separately and identified on outside of package. Place in strong box
placed to prevent shifting of contents. Brown paper bags should be
used for air-dried, blood-stained clothing items.

(e) REMARKS - If wet when found, DRY BY HANGING.
USE NO HEAT TO DRY. Avoid direct sunlight while drying. Use no
preservatives.

(14) SPECIMEN - BODY ORGANS (BRAIN, KIDNEY, LIVER, LUNG):
(See (33) and (70) below, and MIOG, Part II, 13-10.1.5.)

(a) EVIDENCE (AMOUNT DESIRED) - 75 grams of each

(b) SEND BY - Most expeditious means available

(c) IDENTIFICATION - Label container indicating
organ, name of subject, date taken, initials of Agent

(d) WRAPPING AND PACKING - Styrofoam container
preferred to keep specimens frozen

(e) REMARKS - Hold in freezer until personally
delivered or pack in dry ice for mailing by most expeditious means
available. Attach autopsy report.

(15) SPECIMEN - BULLETS (NOT CARTRIDGES): (See MIOG, Part
II, 13-12.4.3.)

(a) EVIDENCE (AMOUNT DESIRED) - All found

(b) SEND BY - Registered mail

(c) IDENTIFICATION - Initial or otherwise mark
primary container only

(d) WRAPPING AND PACKING - Pack tightly in cotton or

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 38

soft paper in pill, match or powder box. Label outside of box as to contents.

(e) REMARKS - Unnecessary handling obliterates marks

(16) SPECIMEN - CARTRIDGES (LIVE AMMUNITION):

(a) EVIDENCE (AMOUNT DESIRED) - All found

(b) SEND BY - For instructions re: shipping live ammunition, see paragraph 13-12.4.2 in this section.

(c) IDENTIFICATION - Initial or otherwise mark
primary container only

(d) WRAPPING AND PACKING - Pack tightly in cotton or soft paper in pill, match or powder box. Label outside of box as to contents.

(17) SPECIMEN - CARTRIDGE CASES (SHELLS): (See MIOG, Part II, 13-12.4.3.)

(a) EVIDENCE (AMOUNT DESIRED) - All

(b) SEND BY - Registered mail

(c) IDENTIFICATION - Initial or otherwise mark
primary container only

(d) WRAPPING AND PACKING - Pack tightly in cotton or soft paper in pill, match or powder box. Label outside of box as to contents.

(13.) (18) SPECIMEN - CHARRED OR BURNED DOCUMENTS: (See 13-17.4)

(a) EVIDENCE (AMOUNT DESIRED) - All

(b) SEND BY - Registered mail

(c) IDENTIFICATION - On outside of container indicate fragile nature of evidence, date obtained, name or initials.

(d) WRAPPING AND PACKING - Utilize polyester film encapsulation technique (contact Investigative Operations and Support Section for instructions) OR Ship charred paper in original container

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 39

in which it was burned at crime scene OR Pack in rigid container between layers of cotton. Do not compress layers.

(e) REMARKS - Added moisture, with atomizer or otherwise, NOT RECOMMENDED.

(19) SPECIMEN - CHECKS (FRAUDULENT):

(a) EVIDENCE (AMOUNT DESIRED) - All (Original documents, not copies, whenever possible)

(b) SEND BY - Registered mail

(c) IDENTIFICATION - See Anonymous Letters (6) above

(d) WRAPPING AND PACKING - See Anonymous Letters (6) above

(e) REMARKS - Advise what parts questioned or known. Furnish physical description of subject.

(20) SPECIMEN - CHECK PROTECTOR, RUBBER STAMP AND/OR DATER STAMP KNOWN STANDARDS (NOTE: SEND ACTUAL DEVICE WHEN POSSIBLE)

(a) STANDARD (AMOUNT DESIRED) - Obtain several copies in full word-for-word order of each questioned check-writer impression. If unable to forward rubber stamps, prepare numerous samples with different degrees of pressure.

(b) SEND BY - Registered mail

(c) IDENTIFICATION - Place name or initials, date, name of make and model, etc., on sample impressions.

(d) WRAPPING AND PACKING - See Anonymous Letters (6) above and/or Packaging Chart (paragraph 13-6.6) above

(e) REMARKS - Do not disturb inking mechanisms on printing devices

(21) SPECIMEN - CLOTHING:

(a) EVIDENCE (AMOUNT DESIRED) - All

(b) SEND BY - Registered mail, or Federal Express or United Parcel Service (UPS)

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 40

(c) IDENTIFICATION - Mark directly on garment or use string tag. Type of evidence, name or initials, date.

(d) WRAPPING AND PACKING - Each article individually wrapped with identification written on outside of package. Place in strong container. Clothing items should be individually packaged in paper bags.

(e) REMARKS - Leave clothing whole. Do not cut out stains. If wet, HANG IN ROOM TO DRY before packing.

(22) SPECIMEN - CODES, CIPHERS AND FOREIGN LANGUAGE

MATERIAL:

(a) EVIDENCE (AMOUNT DESIRED) - All

(b) SEND BY - Registered mail

above (c) IDENTIFICATION - Same as Anonymous Letters (6)

(6) above (d) WRAPPING AND PACKING - Same as Anonymous Letters

(e) REMARKS - Furnish pertinent background and technical information.

(46)) (23) SPECIMEN - COMPUTER AND COMPUTER-RELATED ITEMS: (See

(a) EVIDENCE (AMOUNT DESIRED) - All

(b) SEND BY - Floppy disks - registered mail; hard disks - by overnight express.

(c) IDENTIFICATION - Label container indicating date taken and initials of Agent.

(d) WRAPPING AND PACKING - See Anonymous Letters (6) above. Package or envelope should be marked "Magnetic Media Evidence Enclosed. Do not X-ray."

(e) REMARKS - If computer diskettes are submitted, accompanying communication should, if possible, contain information regarding the make and model of computer used in their preparation.

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 41

(24) SPECIMEN - DRUGS - LIQUIDS: (See (35), (36), (49))

- (a) EVIDENCE (AMOUNT DESIRED) - All
- (b) SEND BY - Registered mail, UPS or air express
- (c) IDENTIFICATION - Affix label to bottle in which found, including name or initials and date.
- (d) WRAPPING AND PACKING - Bottle with sealable top.

(e) REMARKS - Determine alleged normal use of drug and if prescription, check with druggist for supposed ingredients.

(25) SPECIMEN - DRUGS - POWDERS, PILLS, SOLIDS: (See (35), (49))

- (a) EVIDENCE (AMOUNT DESIRED) - All
- (b) SEND BY - Registered mail, UPS or air express
- (c) IDENTIFICATION - On outside of pillbox, name or initials and date
- (d) WRAPPING AND PACKING - Seal to prevent any loss by use of tape

(26) SPECIMEN - DYNAMITE AND OTHER EXPLOSIVES OR SUSPECTED EXPLOSIVES (CONTACT MATERIALS AND DEVICES UNIT FOR INSTRUCTIONS AND SHIPPING CONTAINERS.)

(27) SPECIMEN - FIBERS:

- (a) STANDARD (AMOUNT DESIRED) - Entire garment or other cloth item
- (b) EVIDENCE (AMOUNT DESIRED) - All
- (c) SEND BY - Registered mail
- (d) IDENTIFICATION - On outside of sealed container or on object to which fibers are adhering.
- (e) WRAPPING AND PACKING - Folded paper or pillbox. Seal edges and openings with tape.

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 42

(f) REMARKS - Do not place loose in envelope.

(28) SPECIMEN - FILM:

(a) EVIDENCE (AMOUNT DESIRED) - All

(b) SEND BY - Registered mail

(c) IDENTIFICATION - If not developed mark outside
"DO NOT X-RAY."

(d) WRAPPING AND PACKING - If not developed wrap in
lightproof container.

(29) SPECIMEN - FIREARMS: (See MIOG, Part II, 13-12.4.3,
13-12.5; MAOP, Part II, 2-2.2.2, 6-2.3.9.)

(a) EVIDENCE (AMOUNT DESIRED) - All

(b) SEND BY - Registered mail or Federal Express

(c) IDENTIFICATION - Mark inconspicuously as if it
were your own. Investigative notes should reflect how and where gun
marked.

(d) WRAPPING AND PACKING - Wrap in paper and
identify contents of package. Place in cardboard box or wooden box.

(e) REMARKS - Unload all weapons before shipping.
Keep from rusting. See Ammunition (5) above, if applicable.

(30) SPECIMEN - FLASH PAPER:

(a) SEND BY - Contact Investigative Operations and
Support Section for instructions

(b) IDENTIFICATION - Initials and date.

(c) WRAPPING AND PACKING - Individual polyethylene
envelopes double wrapped in manila envelopes. Inner wrapper sealed
with paper tape.

(d) REMARKS - Store between moistened sheets of
blotter paper, with dry ice. Refrigerate if extended storage is
necessary.

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 43

(31) SPECIMEN - FUSE (SAFETY) (CONTACT MATERIALS AND
DEVICES UNIT FOR COMPLETE INSTRUCTIONS)

(32) SPECIMEN - GASOLINE: (See MIOG, Part II, 13-10.3.4.)

(a) STANDARD (AMOUNT DESIRED) - 100 ml.

(b) EVIDENCE (AMOUNT DESIRED) - All to 100 ml.

(c) SEND BY - UPS or Federal Express

(d) IDENTIFICATION - On outside of container, label
with type of material, name or initials, and date.

(e) WRAPPING AND PACKING - Use sturdy box containing
break-proof bottles and absorbent packing.

(f) REMARKS - Shipping regulation - allow 4 oz.
maximum per bottle.

(33) SPECIMEN - GASTRIC CONTENTS:

(a) EVIDENCE (AMOUNT DESIRED) - All available

(b) SEND BY - Most expeditious means available

(c) IDENTIFICATION - Label container indicating
"gastric contents," name of subject, date taken, initials of Agent.

(d) WRAPPING AND PACKING - Bottle with sealable top
and pack as indicated under "Body organs," (14) above.

(e) REMARKS - Mark package "Keep Refrigerated."

(34) SPECIMEN - GEMS: (See MIOG, Part II, 13-11.7.)

(a) EVIDENCE (AMOUNT DESIRED) - All

(b) SEND BY - Registered mail

(c) IDENTIFICATION - On outside of container

(d) WRAPPING AND PACKING - Use 35 mm film canister
or pharmaceutical container.

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 44

(35) SPECIMEN - GENERAL UNKNOWN - SOLIDS (NONHAZARDOUS):

- (a) STANDARD (AMOUNT DESIRED) - 100 gms.
- (b) EVIDENCE (AMOUNT DESIRED) - All to 100 gms.
- (c) SEND BY - Registered mail
- (d) IDENTIFICATION - Name or initials, date on outside of sealed container.
- (e) WRAPPING AND PACKING - Same as Drugs, (24) and (25) above.

(f) REMARKS - If item is suspected of being a hazardous material, treat as such and contact Materials and Devices Unit for shipping instructions.

(36) SPECIMEN - GENERAL UNKNOWN - LIQUIDS (NONHAZARDOUS):

- (a) STANDARD (AMOUNT DESIRED) - 100 ml.
- (b) EVIDENCE (AMOUNT DESIRED) - All to 100 ml.
- (c) SEND BY - Registered mail
- (d) IDENTIFICATION - Same as for liquid drugs, (24) above.
- (e) WRAPPING AND PACKING - Same as drugs, (24) above.

(f) REMARKS - If item is suspected of being a hazardous material, treat as such and contact Materials and Devices Unit for shipping instructions.

(37) SPECIMEN - GLASS FRAGMENTS: (See MIOG, Part II, 13-11.1.3.)

- (a) EVIDENCE (AMOUNT DESIRED) - All
- (b) SEND BY - Registered mail, UPS or air express
- (c) IDENTIFICATION - Adhesive tape on each piece. Name or initials and date on tape. Separate questioned and known.

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 45

(d) WRAPPING AND PACKING - Wrap each piece separately in cotton. Pack in strong box to prevent shifting and breakage. Identify contents.

(e) REMARKS - Avoid chipping and mark "Fragile."

(38) SPECIMEN - GLASS PARTICLES: (See MIOG, Part II, 13-11.1.3.)

(a) STANDARD (AMOUNT DESIRED) - All of bottle or headlight. Small piece of each broken pane.

(b) EVIDENCE (AMOUNT DESIRED) - All

(c) SEND BY - Registered mail

(d) IDENTIFICATION - Name or initials, date on outside of sealed container

(e) WRAPPING AND PACKING - Use 35 mm film canister or pharmaceutical container.

(f) REMARKS - Do not use envelopes or bags which will tear.

(39) SPECIMEN - GLASS WOOL INSULATION: (See (45))

(a) STANDARD (AMOUNT DESIRED) - 1-inch mass from each suspect area

(b) EVIDENCE (AMOUNT DESIRED) - All

(c) SEND BY - Registered mail

(d) IDENTIFICATION - Name or initials, date on outside of sealed container

(e) WRAPPING AND PACKING - Sealed container

(40) DELETED

(41) SPECIMEN - GUNSHOT RESIDUES - ON CLOTH: (See (57) and MIOG, Part II, 13-12.4.1.)

(a) EVIDENCE (AMOUNT DESIRED) - All

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 46

(b) SEND BY - Registered mail

(c) IDENTIFICATION - Attach string tag or mark directly. Type of material, date, and name or initials.

(d) WRAPPING AND PACKING - Place fabric flat between layers of paper and then wrap so that no residue will be transferred or lost.

(e) REMARKS - Avoid shaking.

(42) SPECIMEN - HAIR:

(a) STANDARD (AMOUNT DESIRED) - 25 or more full length hairs randomly selected from head or pubic regions. Should include both pluckings and combings, separately enclosed in envelopes and marked accordingly.

(b) EVIDENCE (AMOUNT DESIRED) - All

(c) SEND BY - Registered mail

(d) IDENTIFICATION - On outside of container. Type of material, date, and name or initials.

(e) WRAPPING AND PACKING - Folded paper or pillbox. Seal edges and openings with tape.

(f) REMARKS - Do not place loose in envelope.

(43) SPECIMEN - HANDWRITING AND HAND PRINTING, KNOWN STANDARDS:

(a) STANDARD (AMOUNT DESIRED) - For instructions re: obtaining known standards, see paragraph 13-17.2.3 in this section

(b) SEND BY - Registered mail

(c) IDENTIFICATION - Name or initials, date, from whom obtained, and voluntary statement should be included in appropriate place.

(d) WRAPPING AND PACKING - Same as Anonymous Letters
(6) above.

(44) SPECIMEN - HOAX BOMB DEVICES AND/OR COMPONENTS (FOR

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 47

INSTRUCTIONS, CONTACT THE MATERIALS AND DEVICES UNIT.) (See also MIOG, Part I, 91-8; Part II, 13-16.6.)

(39) ABOVE.) (45) SPECIMEN - INSULATION (SEE GLASS WOOL INSULATION,

(46) SPECIMEN - MAGNETIC MEDIA (SEE COMPUTER, (23) ABOVE.)

(47) SPECIMEN - MAGNETIC TAPE RECORDINGS (SEE MIOG, PART I, 139-3(2) (d), PART II, SECTION 16, PARAGRAPHS 16-8 TO 16-8.2.4.)

(48) SPECIMEN - MATCHES:

(a) STANDARD (AMOUNT DESIRED) - One to two books of paper. One full box of wood.

(b) EVIDENCE (AMOUNT DESIRED) - All

(c) SEND BY - UPS or Federal Express

(d) IDENTIFICATION - On outside of container. Type of material, date, and name or initials.

(e) WRAPPING AND PACKING - Metal container and packed in larger package to prevent shifting. Matches in box or metal container packed to prevent friction between matches.

(f) REMARKS - Keep away from fire. "Keep away from fire" label

ABOVE.) (49) SPECIMEN - MEDICINES (SEE DRUGS, (24) AND (25)

(50) SPECIMEN - METAL:

(a) STANDARD (AMOUNT DESIRED) - One pound

(b) EVIDENCE (AMOUNT DESIRED) - All to one pound

(c) SEND BY - Registered mail, UPS or air express

(d) IDENTIFICATION - On outside of container. Type of material, date, and name or initials.

(e) WRAPPING AND PACKING - Use paper boxes or containers. Seal and use strong paper or wooden box.

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 48

(f) REMARKS - Melt number, heat treatment, and other specifications of foundry if available. Keep from rusting.

(51) SPECIMEN - OIL: (See MIOG, Part II, 13-10.3.4.)

(a) STANDARD (AMOUNT DESIRED) - 250 ml. together with specifications

(b) EVIDENCE (AMOUNT DESIRED) - All to 250 ml.

(c) SEND BY - Any method

(d) IDENTIFICATION - On outside of container. Type of material, date, and name or initials.

(e) WRAPPING AND PACKING - Container with tight screw top. Pack in strong box using excelsior or similar material.

(f) REMARKS - Keep away from fire.

(52) SPECIMEN - OBLITERATED, ERADICATED, OR INDENTED
WRITING:

(a) EVIDENCE (AMOUNT DESIRED) - All

(b) SEND BY - Registered mail

(c) IDENTIFICATION - Same as Anonymous Letters, (6)
above

(d) WRAPPING AND PACKING - Same as Anonymous Letters, (6) above

(e) REMARKS - Advise whether bleaching or staining methods may be used. Avoid folding.

(53) SPECIMEN - PAINT - LIQUID:

(a) STANDARD (AMOUNT DESIRED) - Original unopened container, up to 1 gallon if possible

(b) EVIDENCE (AMOUNT DESIRED) - All to 1/4 pint

(c) SEND BY - Registered mail, UPS or air express

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 49

(d) IDENTIFICATION - On outside of container. Type of material, origin if known, date, name or initials.

(e) WRAPPING AND PACKING - Friction-top paint can or large-mouth, screw-top jars. If glass, pack to prevent breakage. Use heavy corrugated paper or wooden box.

(54) SPECIMEN - PAINT - SOLID (PAINT CHIPS OR SCRAPINGS):

(a) STANDARD (AMOUNT DESIRED) - At least 1/2 square inch of painted area if possible, with all layers represented. Take representative samples from several areas of known source and secure separately.

(b) EVIDENCE (AMOUNT DESIRED) - All. If on small object, send object.

(c) SEND BY - Registered mail, UPS or air express

(d) IDENTIFICATION - On outside of container. Type of material, origin if known, date, name or initials.

(e) WRAPPING AND PACKING - Use 35 mm film canister or pharmaceutical container. Seal to prevent leakage. Paper and plastic envelopes are not satisfactory. Do not pack in cotton.

(f) REMARKS - Avoid contact with adhesive materials such as fingerprint lifting tape or other pressure sensitive tape. Wrap so as to protect smear.

(55) SPECIMEN - PHOTOGRAPHS:

(a) EVIDENCE (AMOUNT DESIRED) - All

(b) SEND BY - Registered mail

(c) IDENTIFICATION - If not developed mark outside
"DO NOT X-RAY"

(d) WRAPPING AND PACKING - If not developed wrap in lightproof container.

(56) SPECIMEN - DENTAL STONE CASTS OF TIRE TREADS AND SHOE PRINTS: (See 13-19.1.2.)

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 50

(41) ABOVE.) (57) SPECIMEN - POWDER PATTERNS (SEE GUN SHOT RESIDUES,

(58) SPECIMEN - ROPE, TWINE, AND CORDAGE:

- available
- (a) STANDARD (AMOUNT DESIRED) - One yard or amount
 - (b) EVIDENCE (AMOUNT DESIRED) - All
 - (c) SEND BY - Registered mail

(d) IDENTIFICATION - On tag or container. Type of material, date, name or initials.

(e) WRAPPING AND PACKING - Wrap securely.

11.3.2.) (59) SPECIMEN - SAFE INSULATION: (See MIOG, Part II, 13-

areas (a) STANDARD (AMOUNT DESIRED) - Sample all damaged

(b) EVIDENCE (AMOUNT DESIRED) - All

(c) SEND BY - Registered mail, UPS or air express

(d) IDENTIFICATION - On outside of container. Type of material, date, name or initials

(e) WRAPPING AND PACKING - Use 35 mm film canister or pharmaceutical container. Seal to prevent any loss.

(f) REMARKS - Avoid use of glass containers and envelopes.

13-8.2.4.) (60) SPECIMENS - SALIVA SAMPLES: (See MIOG, Part II,

(a) STANDARD (AMOUNT DESIRED) - Collect on saliva swab (cotton-tipped applicator), generally, five-inch long wooden stick with cotton tip.

(b) EVIDENCE (AMOUNT DESIRED) - All

(c) SEND BY - Registered mail

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 51

(d) IDENTIFICATION - On outside envelope put type of sample, date and place of collection and collector's initials.

(e) WRAPPING AND PACKING - Seal in envelope.

(f) REMARKS - Applicators can be purchased in individually wrapped sterile packets which contain a single sterile swab. Allow to dry before placing in envelope.

(61) SPECIMEN - SHOE PRINT LIFTS (IMPRESSIONS ON HARD SURFACES): (See MIOG, Part II, 13-19.1.3.)

(a) STANDARD (AMOUNT DESIRED) - Photograph before making of dust impression.

(b) EVIDENCE (AMOUNT DESIRED) - All

(c) SEND BY - Registered mail

(d) IDENTIFICATION - On lifting tape or paper attached to tape. Name or initials and date.

(e) WRAPPING AND PACKING - Prints in dust are easily damaged. Fasten print or lift to bottom of a box so that nothing will rub against it.

(f) REMARKS - Always rope off crime scene area until shoe prints or tire treads are located and preserved.

(62) SPECIMEN - SOILS AND MINERALS: (See MIOG, Part II, 13-11.2.2 and 13-11.2.3.)

(a) STANDARD (AMOUNT DESIRED) - Samples from areas near pertinent spot.

(b) EVIDENCE (AMOUNT DESIRED) - All

(c) SEND BY - Registered mail

(d) IDENTIFICATION - On outside of container. Type of material, date, name or initials.

(e) WRAPPING AND PACKING - Use 35 mm film canister or pharmaceutical container.

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 52

(f) REMARKS - Avoid glass containers and envelopes.

(63) SPECIMEN - TOOLS:

(a) EVIDENCE (AMOUNT DESIRED) - All

(b) SEND BY - Registered mail, UPS or air express

(c) IDENTIFICATION - On tools or use string tag.
Type of tool, identifying number, date, name or initials.

(d) WRAPPING AND PACKING - Wrap each tool in paper.
Use strong cardboard or wooden box with tools packed to prevent shifting.

(64) SPECIMEN - TOOLMARKS: (See (72) and MIOG, Part II, 13-13.3, 13-13.4.)

(a) STANDARD (AMOUNT DESIRED) - Send in the tool.
If impractical, call Firearms/Toolmarks Unit for instructions.

(b) EVIDENCE (AMOUNT DESIRED) - All

(c) SEND BY - Registered mail, UPS or air express

(d) IDENTIFICATION - On object or on tag attached to
or on opposite end from where toolmarks appear. Name or initials and date.

(e) WRAPPING AND PACKING - After marks have been
protected with soft paper, wrap in strong wrapping paper, place in strong box, and pack to prevent shifting.

(65) SPECIMEN - TYPEWRITING, KNOWN STANDARDS:

(a) STANDARD (AMOUNT DESIRED) - For instructions re:
obtaining known standards see paragraph 13-17.2.4 in this section

(b) SEND BY - Registered mail

(c) IDENTIFICATION - Place name or initials, date,
serial number, name of make and model, etc., on specimens.

(d) WRAPPING AND PACKING - Same as Anonymous
Letters, (6) above.

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 53

(e) REMARKS - Examine ribbon for evidence of questioned message thereon.

(66) SPECIMEN - URINE:

(a) STANDARD (AMOUNT DESIRED) - 50 cc minimum

(b) SEND BY - Registered mail

(c) IDENTIFICATION - Label container indicating "urine," name of subject, date taken, initials of Agent.

(d) WRAPPING AND PACKING - Bottle with sealable top, surrounded with absorbent material to prevent breakage. Strong cardboard or wooden box, refrigerate if possible.

(e) REMARKS - Mark package "Keep Refrigerated."

(67) SPECIMEN - VAGINAL SAMPLES - SLIDES (MICROSCOPE):
(See (68) and MIOG, Part II, 13-8.2.5.)

(a) EVIDENCE (AMOUNT DESIRED) - Minimum of two slides

(b) SEND BY - Registered mail

(c) IDENTIFICATION - Label with type of sample, name of donor, date and place of collection and collector's initials.

(d) WRAPPING AND PACKING - Use commercial slide box.

(e) REMARKS - Slide box available at hospitals. Doctor should not fix slides. No cover slips. Air dry.

(68) SPECIMEN - VAGINAL SAMPLES - SWABS: (See MIOG, Part II, 13-8.2.5.)

(a) STANDARD (AMOUNT DESIRED) - Two unstained swabs from same package as stained.

(b) EVIDENCE (AMOUNT DESIRED) - Minimum of two swabs

(c) SEND BY - Express mail

(d) IDENTIFICATION - Same as (67) above.

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II.

PAGE 13 - 54

(e) WRAPPING AND PACKING - Seal in envelope.

(f) REMARKS - Allow swabs to dry before packaging, refrigerate or freeze.

(69) SPECIMEN - VIDEO TAPES:

(a) EVIDENCE (AMOUNT DESIRED) - Always submit original

(b) SEND BY - Registered mail

(c) IDENTIFICATION - Place name or initials, date and identification number on cassette housing.

(d) WRAPPING AND PACKING - Wrap securely. Strong cardboard box with three inches of paper crumpled around all sides of the video tapes. Do not use foam packing material.

(e) REMARKS - Mark the package "Video Tape" or "Recorded Magnetic Medium."

(70) SPECIMEN - VITREOUS HUMOR:

(a) STANDARD (AMOUNT DESIRED) - All

(b) SEND BY - Most expeditious means available

(c) IDENTIFICATION - Label container indicating "vitreous humor," name of subject, date taken, initials of Agent

(d) WRAPPING AND PACKING - Glass bottle with sealable top and pack as indicated for "Body organs," (14) above.

(e) REMARKS - Refrigerate only (do not freeze) until personally delivered. Keep cool during delivery time. Attach autopsy report.

(71) SPECIMEN - WATER:

(a) STANDARD (AMOUNT DESIRED) - 1 Liter

(b) EVIDENCE (AMOUNT DESIRED) - 1 Liter

(c) SEND BY - Registered mail

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 55

(d) IDENTIFICATION - Date and initial

top.
(e) WRAPPING AND PACKING - Use bottle with sealable

(72) SPECIMEN - WIRE (SEE ALSO TOOLMARKS, (64) ABOVE.):

kink.)
(a) STANDARD (AMOUNT DESIRED) - Three feet (Do not

(b) EVIDENCE (AMOUNT DESIRED) - All (Do not kink.)

(c) SEND BY - Registered mail

(d) IDENTIFICATION - On label or tag. Type of
material, date, name or initials.

(e) WRAPPING AND PACKING - Wrap securely.

(f) REMARKS - Do not kink wire.

(73) SPECIMEN - WOOD:

available.
(a) STANDARD (AMOUNT DESIRED) - One foot or amount

(b) EVIDENCE (AMOUNT DESIRED) - All

(c) SEND BY - Registered mail

(d) IDENTIFICATION - On label or tag. Type of
material, date, name or initials.

(e) WRAPPING AND PACKING - Wrap securely

EFFECTIVE: 11/21/97

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 56

13-6.7.1 Hazardous Materials (See MIOG, Part II, 13-3.1(4) and
[13-15.1.6; MAOP, Part II, 2-4.4.3.]

Over 3,000 items, including flash paper, live ammunition, explosives, radioactive materials, flammable liquids and solids, flammable and nonflammable gases, spontaneously combustible substances, and oxidizing and corrosive materials are currently considered as hazardous materials. All require special packaging and the amount of each item which can be shipped is regulated. Therefore, the applicable action listed below is to be taken:

(1) Flash paper: Contact Investigative Operations and Support Section for shipping instructions EACH AND EVERY TIME this item is to be submitted to the Laboratory.

(2) Live ammunition: For shipping instructions see 13-12.4.2 elsewhere in this section.

(3) Other hazardous materials: Contact the Materials and Devices Unit for shipping instructions EACH AND EVERY TIME any hazardous material, except flash paper or live ammunition, is to be submitted to the Laboratory.

EFFECTIVE: 04/07/97

13-6.7.2 Nonhazardous Materials

If evidence of this type is not found in this chart or elsewhere in this section, locate a specimen which is most similar in nature and take the appropriate actions or call the Laboratory at 202-FBI-4410 for general instructions.

EFFECTIVE: 05/26/83

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 57

13-7 FIELD PHOTOGRAPHY

The purpose of the information under this caption is to provide some of the general guidelines pertaining to Bureau photographic matters and to list by name, description, and use the types of document copying, microfilming, general photographing, and surveillance equipment available to the various field offices. For information concerning photographic examinations conducted in the Laboratory see [MIOG, Part II, 13-7.6 and 13-7.6.1.)]

EFFECTIVE: 07/25/97

13-7.1 General Guidelines

EFFECTIVE: 04/19/91

13-7.1.1 Laboratory Photographic Responsibilities

ba

[(1) | The Special Photographic Unit (SPU) of the Laboratory (Room 3449, Extension [REDACTED] is responsible for all photographic matters to include surveillance photography, nonroutine requests, unusual processing requirements, examination of photographic evidence, and all other photographic equipment requests, repairs, problems, or other inquiries. SPU has been funded to supply the field with most photographic equipment; therefore, requests for routine photographic equipment should be directed to SPU through the field office Photographic Technician. SPU is the funding source for all photographic equipment (there is no other source available to the field). If there is any doubt regarding equipment, contact SPU, for assistance and clarification. SPU also handles all photographic tradecraft in FCI matters.

[(2) | The SPU also handles all general processing and mass production photographic work. This includes the capability of doing copy work on film of documents, objects, i.e., photographs, jewelry, etc., and duplication of slides and making of slides from original art work for training purposes. SPU handles equipment needs for darkroom and "mug shot" photography. This is defined as photographic processing and finishing, studio and "mug shot" areas to include those facilities in use within the field office and off-site facilities. SPU will also handle the design of field office darkrooms and those

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 58

related areas due to moves or renovations. All related equipment selection, procurement, inventory and distribution, including sinks, cabinets, enlargers, miscellaneous darkroom equipment, processing and finishing equipment, mug shot and copying equipment that relate to the darkroom areas will also be handled by SPU.

(3) The SPU is responsible for the processing of the video imagery where the image requires enhancement and the preparation of a photographic print. This video imagery may originate from time-lapse or full-motion video tapes of any format or from still video disks. SPU can provide photographic prints and/or video tapes of these enhanced images. Requests for comparisons of video imagery to known photographic prints or to other submitted evidence (guns, articles of clothing, bags, hats, etc.) should be forwarded directly to SPU. (See 13-7.6.1.)

(4) Submissions to the SPU should be by electronic communication under the case caption.

(5) The SPU of the Laboratory Division oversees the areas of film processing, color and black and white enlarging and camera copy work, and slide reproduction, all on a quantitative basis. These requests should be submitted with an FD-523.

(6) The film processing functions are inclusive of color negative (C-41), color positive (E-6), microfilms, and all black and white negatives.

(7) Color and black and white enlargements made from negatives are processed to specifications which can vary in dimensions of 3 1/2 by 5 inches to 40 by 60 inches. There is also the capability of processing color enlargements from slides; however, this involves the preparation of an internegative which can result in the loss of resolution and color reproduction in larger prints.

EFFECTIVE: 07/25/97

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 59

13-7.1.2 Personal Identification ("mug") Photographs
(See MIOG, Part II, 11-4.9.)

Personal identification color ("mug") photographs should include the head and shoulders in full face view and profile. If not otherwise equipped, use the Mamiya 645, with flash equipment or flood lamps and, if available, a white background. Include identifying data and a visible gray scale in all pictures. If the equipment for this purpose is not available, contact the Special Photographic Unit (Room 3449, Ext. [REDACTED])

b2

EFFECTIVE: 07/25/97

13-7.1.3 Polaroid Photographs

Polaroid cameras and 4- by 5-inch (Speed Graphic) polaroid film holders are available in many offices. The use of polaroid should be limited to those situations in which an immediate photographic print will definitely further the investigation. In other situations, conventional photography should be used.

EFFECTIVE: 04/19/91

13-7.1.4 Color Photography

The use of color photography should be considered during the course of all investigations where a record of the color or color contrast may be a factor in the evaluation of the evidence. Color photographs may be particularly helpful and important in recording the bloodstains in a crime scene; color negative processing should be used. When color photographs are to be made, 120 or 35mm film is preferred. Closely follow the instructions provided with the film as to lighting and exposure data. Good quality color prints can be made from a color negative. If projection slides are desired, color reversal (positive) properly exposed film, such as Ektachrome or 3M CS Type Film and FUJI can be used. (Under no circumstances should Kodachrome film be used.)

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 60

EFFECTIVE: 04/19/91

13-7.2 General Photographic Equipment

Name of Equipment	Description	Use
Mamiya 645	120mm roll film camera. Kit includes camera, motor drive, flash and lens.	Aerial, crime scene, "mug" and document photography.
Canon and Nikon Camera Systems	35mm camera. Lens available 24mm-2000mm. Numerous other special application accessories are supplied or are available on request.	Primarily intended for use as a surveillance system. Also used in some concealments and remote applications.

EFFECTIVE: 04/19/91

13-7.3 Microfilming Equipment

Name of Equipment	Description	Use
Attache photocopy units	Portable, completely self-contained, collapsible document copy equipment carried in an attache case, 18" by 12" by 4 3/4", weighing 16 lbs. Electronic photo-flash lights powered by self-contained 6-volt (four "C" cells) battery pack or AC/DC. Camera is standard 36 exposure 35mm Olympus with lens. Newer models will have AC/DC	Rapid photography of small number of documents including bound and large-size documents. Do not use color film.

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 61

operation and larger film
capacity options.

EFFECTIVE: 04/19/91

13-7.4 Deleted

EFFECTIVE: 02/12/92

13-7.5 Photographic Surveillance

The objective of surveillance photography is generally to obtain recognizable, identification images of individuals or items, or to record events as they occur, or over a long period of time. Conventional still photography should be used in all instances where recognition or identifiable detail is required. Still video is not to be used unless the immediate electronic transmission of the image is of prime importance and quality is secondary. Motion pictures (if detail is of high importance) or closed circuit TV (CCTV), should be used if the prime objective is to record the action taking place or an event that occurs over a long period of time. When both identification and action are required still photography and CCTV should be used simultaneously. CCTV images and motion picture images cannot be substituted for conventional still photography since it is not possible to make high-quality, hard-copy enlargements from these processes. (See Part II, 9-1(5) of this manual concerning the use of photographic technicians for photographic surveillances.) The SPU will design and install unmanned automatic still-camera surveillance systems where the need arises. These utilize a variety of trip devices. [REDACTED] and other devices to activate the camera when subjects are present.

b2/b7E

EFFECTIVE: 02/12/92

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 62

13-7.5.1 Long Range Photography With Telephoto Equipment

The lens used depends upon the distance from the subject to the cover available.

(1) Telephoto lenses are available for still photography at distances up to 1500':

Distance Range	Rec. Lens Focal Length (2mm's per foot)
50' - 150'	up to 300mm.
150' - 300'	300mm to 600mm.
300' - 600'	600mm to 1200mm.
600' - 1500'	1200mm to 3000mm.

(2) Fast telephoto lenses are available for photography in situations in which the intensity of the light available is low. These are limited to up to 400mm.

(3) Deleted

EFFECTIVE: 02/12/92

13-7.5.2 Night Surveillance Equipment

(1) Night photographic surveillance problems may be solved with the utilization of light intensification equipment provided to each Special Operations Group (SOG) and maintained by the Special Photographic Unit, Laboratory Division. Night viewing devices are not designed for photography.

(2) Ultrahigh-speed films for surveillance photography in low-light-level situations, such as a dimly lighted street or entryway at night, are available. The use of such films with available fast lenses extends surveillance photography to many nighttime and other situations where the available light is extremely low. Film, equipment, and assistance for these applications can be obtained from the Laboratory.

(3) Infrared photography can be used to obtain photographs in total darkness. High-speed infrared film, infrared flashbulbs, light sources and infrared filters for light sources are available for such installations.

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 63

(4) Most offices are equipped with a [REDACTED]
[REDACTED] Personnel in those offices have been
appropriately trained. Only those personnel are to utilize the [REDACTED]
units.

b2/b7E

EFFECTIVE: 02/12/92

13-7.5.3 Photography With Concealed Cameras

(1) Concealed cameras are motor-driven still cameras (35
mm). Concealments available include: [REDACTED]

[REDACTED] Custom units can be made to solve specific problems.
Special equipment and concealments are available for FCI cases.
Contact the Special Photographic Unit on the secure phone system.

(2) The concealments can be activated by individuals at
the scene or by remote control for unmanned surveillances or camera
traps. Such equipment can be operated by direct wire connection,
timers, tripping devices or radio control.

(3) Camera equipment is available which is readily
adaptable for use from cover in mobile equipment-automobiles, panel
trucks, etc. Reflex (through the lens) focusing cameras are
particularly useful for this application.

EFFECTIVE: 07/25/97

13-7.5.4 Aerial Photography

Aerial photography can be used for planning, intelligence
gathering and court purposes. The Mamiya 645 provided to the field
is the recommended camera for aerial photography from fixed wing
aircraft or helicopters. [REDACTED]

[REDACTED] Contact the Special Photographic Unit, Extension [REDACTED]
for information and scheduling.

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 64

EFFECTIVE: 05/26/89

| 13-7.5.5 | Emergency Operational Support

A specialized photographic Emergency Response Team will provide immediate on-scene photographic intelligence during a crisis situation or any case requiring immediate results. Equipment, including a portable darkroom system, is prepackaged for immediate deployment to anywhere in the world. This whole-team concept and equipment is designed to provide photographic results without any outside source of personnel or other resources such as electricity. Contact the Special Photographic Unit, Extension [REDACTED] for information and scheduling. |

b2

EFFECTIVE: 05/26/89

| 13-7.5.6 Deleted

EFFECTIVE: 11/20/90

| 13-7.6 | Photographic Examinations | (See MIOG, Part II, 10-3, 13-7, and 13-7.6.1.) (Formerly 13-18) |

(1) Forensic examinations of photographic evidence are available from the Special Photographic Unit. Photographic evidence may include:

- (a) Film negatives
- (b) Slides
- (c) Instant prints/slides
- (d) Photographs
- (e) Cameras
- (f) Video tape

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 65

- (g) Unexposed film
- (h) Undeveloped film
- (i) Photographic accessories
- (j) Pornography
- (k) FCI Tradecraft
- (l) Motion Pictures
- (m) Image processing picture files
- (n) Digital camera image files

(2) Also, any other evidence may be submitted for studio photographic examinations using, for example, infrared, and ultraviolet techniques. This nonphotographic evidence includes, but is not limited to:

- (a) Documents
- (b) Clothing
- (c) Any obliterated writing or printing
- (d) Defaced or altered surfaces
- (e) Items with hollows or cavities

(3) The following are examinations of photographic evidence available from the Special Photographic Unit:

(a) Bank Robbery Film Examinations - Bank Robbery film (or video tape) is examined and compared to other submitted evidence (guns, clothing, mug shots, bags, hats, etc.). This examination may help establish a subject's presence at a crime scene by identifying clothing, weapons, or any other items linked to the subject. These examinations include surveillance video tapes that are increasingly popular for bank surveillance. Also subject height determinations may be made from these images (see Photogrammetry Examinations below at (3) (e)).

Note: It is important to remember that the negatives or the original video tape are the best evidence and should always be submitted when

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 66

an examination is requested. Before submitting, any prints needed for continuing the investigation should be made from the negatives, and at least one copy of the video tape should be retained in the field division.

In conjunction with the Firearms/Toolmarks Unit, bullet trajectories may be calculated through photogrammetric techniques.

(b) Photographic Comparisons - Photographic evidence is examined and compared to other evidence or photographs of evidence. Various photographs of a subject taken at different times and places may be compared to determine if the photographs are indeed of the same subject. The subject may be a suspect individual, vehicle, weapon, or virtually anything that may be photographed. Also, any items within a photograph may be compared, for example, a pendant around an individual's neck, rings, or tattoos.

(c) Time and Location Examinations - Photographic evidence may be examined to determine the location, time, and date that an image was taken.

(d) Authenticity Examinations - Photographic evidence may be examined to determine if the image is the result of a composite, a copy, or of some other alteration method to cause a misrepresentation. Evidence may also be examined to see if it is a copy of copyrighted or pornographic material.

(e) Photogrammetry - Actual dimensions may be derived from photographic images through the use of various geometric formulae. The most common is determining the height of bank robbery suspects. As an adjunct to this type of examination, plan drawings, or views may be generated. These are "overhead" representations of a scene depicted in a photographic image. These may be used for mapping a major crime scene from photographs taken of the scene. This may include onsite surveys by SPU personnel coupled with photographs taken by specially calibrated cameras.

(f) Infrared (IR), Ultraviolet (UV), and X-Ray Examinations - Obliterated writing or other marks may be made evident by examining evidence with IR, UV, and X-ray photography. These examinations are based on the principle that various substances may reflect, fluoresce, or luminesce at different rates. Examples include overwritten documents, documents with altered writing, objects with defaced serial numbers, or other identifying marks, or marks that may be invisible against a similarly colored background.

Sensitive

Manual of Investigative Operations and Guidelines
Part II.

PAGE 13 - 67

(g) FCI Tradecraft - The Special Photographic Unit examines and maintains a collection of foreign counterintelligence tradecraft. This is not necessarily limited to FCI cases. Any cases of items designed for concealed cameras, money, drugs, etc., may be examined for evidentiary purposes.

(h) Source and Age Examinations - In some cases photographic products (including film and prints) may be dated and source established by an examination of their manufactured characteristics. This may be helpful in establishing the time frame that a photograph may have been taken.

(i) Camera Examinations - Cameras may be examined to determine if they exposed a particular image. Also they may be examined to determine if they have been altered (including serial numbers), and for the purposes they may have been altered. These examinations include any photographic equipment or supplies that may have been seized as evidence.

(j) Image Processing - Photographic images that have been degraded as the result of being out-of-focus, blurred, under or overexposed, or any other problems contributing to a poor image may be corrected through the use of computer digital image processing.

(k) Scene Reconstruction - Photography may be used to "reconstruct" what may have been visible to a subject or witness under a given set of circumstances. This may also be used to establish the veracity of photographs introduced in court purporting to depict lighting conditions at a certain time and place.

(l) Analysis of Time and Motion - The speed of objects may be calculated in motion pictures, video tapes, or other images from sequential frame cameras.

(m) Photographic Consultation - The SPU is available to provide assistance on how to best preserve and transport photographic evidence. In cases where exposed or unknown film or other photographic materials are seized as evidence, the SPU may be able to determine whether or not the items have been exposed, and if so how they should be developed.

EFFECTIVE: 07/25/97

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 68

13-7.6.1 Video Tape Enhancement/Examination and Support
(See also MIOG, Part II, 13-7.1.1 and 13-7.6.1.)
(Formerly 13-29, 13-29.1, 13-29.2 and 13-29.3)

The Special Photographic Unit (SPU) of the Laboratory (Room 3449, Extension [REDACTED]) is responsible for the processing of video imagery where the image requires enhancement and the preparation of a photographic print. This video imagery may originate from time-lapse or full-motion video tapes of any format or from still video disks.

SPU can provide photographic prints and/or video tapes of these enhanced images. Requests for comparisons of video imagery to known photographic prints or to other submitted evidence (guns, articles of clothing, bags, hats, etc.) should be forwarded to the SPU.

SPU can also provide the following forensic video support services:

(1) Reconstruction of physically damaged video tapes. This includes tapes that have been damaged due to mechanical malfunction of a video tape machine or video tapes that have been deliberately damaged.

(2) Slow-motion or frame-by-frame playback of video tapes. This is often beneficial when actions or activities occur quickly and are not readily apparent to the viewer. This process is also valuable for recovering partially recorded video frames that also are not readily apparent to the viewer.

(3) Conversion of foreign video standards. There are three primary worldwide video standards (NTSC, PAL, and SECAM). These standards are not directly compatible. Tapes received from or destined to foreign countries may require standards conversion. In addition to providing this conversion process, the SPU can provide consultation and technical assistance in determining proper video standards.

(4) Production of demonstrative evidence video tapes for courtroom presentation. This is to include video tapes produced for crime scene documentation or reenactment and the preparation of video tapes containing English-translated subtitles of surveillance video tapes where the recorded conversation is in a foreign language.

(5) Where appropriate, SPU can edit and/or compile video segments for briefings or as investigative or demonstrative aids.

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 69

| (6) | Submission to the|SPU|should be by electronic communication under the case caption. Video frames or sequences that require enhancement or processing should be identified by using the time/date recorded on the video tapes when available. Should there be no time/date or an incorrect time/date recorded on the video tape, a complete description of the subject or activities in question should be provided and the tape stopped at the beginning of the pertinent segment. Also, if available, the manufacturer and model of the recording video tape machine should be included.

| (7) | It should be noted that video-based imagery does not contain the resolution of film and should not be used as a replacement for film, where image detail for identification purposes is required.

| (8) | Attempts should be made to minimize the number of times a video tape is played or reviewed. Continued or repeated use of video tapes, especially time-lapse video tapes, can cause physical degradation of the tape and can severely limit enhancement efforts. Original video tape should always be submitted.

EFFECTIVE: 07/25/97

13-8 SEROLOGY EXAMINATIONS

(1) Forensic serology consists of the identification and characterization of blood and other body fluids in the crime laboratory. Evidence is received mainly in connection with violent crimes, such as murder, rape, robbery, assault-and-battery. Evidence in burglary, hit-and-run cases and game violation cases is also frequently received.

(2) In cases where it has been determined that a person is infected with, or is suspected of being infected with either acquired immune deficiency syndrome (AIDS), tuberculosis or hepatitis| (A, B, or C), the Laboratory MUST be notified of the condition both in the incoming communication and the evidence labeled accordingly.

(3) If an investigator is not familiar with or is unsure about the submission of any particular evidence to the Laboratory, he/she should call to get advice.

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 70

EFFECTIVE: 11/20/90

13-8.1 Blood

EFFECTIVE: 11/20/90

13-8.1.1 Blood Examinations Aid Investigations

- (1) In location of the crime scene -- Identification of human blood can pinpoint the area for a crime search.
- (2) In determining the possible commission of a crime - Occasionally, the identification of human blood on a highway, sidewalk, porch, or in a car is the first indication of a crime's occurrence.
- (3) In identifying the weapon used - The DNA typing of human blood identified on a club, knife or hammer can be of considerable investigative and prosecutive value.
- (4) In proving or disproving a suspect's alibi - The identification of human blood on an item belonging to a suspect who claims an animal as the blood source. The identification of animal blood can substantiate the claim of an innocent person.
- (5) In eliminating suspects - The determination by DNA typing tests that human blood on suspect items is different from the victim's blood can facilitate the release of a suspect or help to substantiate a suspect's claim of injury.

EFFECTIVE: 05/31/94

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 71

13-8.1.2 Information Determinable by Blood Tests

(1) Identification of stains as blood - Chemical analyses are necessary to positively identify blood. The appearance of blood can vary greatly depending on the age of stains and on other factors.

(2) Determination whether blood is of human or animal origin - If animal, determination of specific animal family.

(3) DNA analysis of blood.

(a) Deleted

(b) Deleted

(c) Deleted

EFFECTIVE: 05/31/94

| 13-8.1.3 | Deleted |

EFFECTIVE: 11/21/97

13-8.1.4 Collection, Identification and Wrapping of Bloodstained Evidence (See MIOG, Part II, 13-6.7 (9), (10), (11), (12), (13).)

(1) Agents conducting crime scenes and handling any body fluids should wear latex gloves inasmuch as the status of infectious microorganisms (e.g., AIDS, Hepatitis B) that may be contained in body fluids will not be known. If aerosol droplets or airborne particles are produced during the crime scene search, surgical masks and eye protection are recommended. Particular care should also be taken when handling or searching for secreted sharp instruments such as knives and hypodermic needles. Agents should use mirrors and flashlights to look for secreted hypodermic needles and syringes prior to inserting the hand in areas they cannot clearly see. In any instance where an injury occurs and a body fluid comes in contact with a wound, however

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 72

minor, medical attention should be sought immediately. (See MIOG, Part II, 13-8.4 (5).)

(2) Deleted

(3) Garments and fabrics:

(a) Investigator's identifying marks should be put directly on the fabric in ink, away from stained areas if possible.

(b) Each item should be wrapped separately.

(c) Stains which are moist must be dried out thoroughly before wrapping or putrefaction of blood will occur.

(d) Drying should be done by exposure to the atmosphere in a secure, well-ventilated room and not be exposed to direct sunlight or heat.

(4) Blood on surfaces such as walls or floors - If possible, remove stained portion of wall or floor. If this is not possible, stains can be swabbed from surface using swabs slightly moistened with water. Air dry swabs and place in paper envelopes. DO NOT PLACE IN PLASTIC.

(5) Blood on automobiles involved in "hit and run" cases where a paint examination will also be requested should not be scraped off. It should be chipped off along with appropriate paint specimens with a sharp object such as a chisel or screwdriver and shipped to the Laboratory in one piece.

(6) Blood on pieces of glass:

(a) Pieces should be submitted if stains are too thin for removal of adequate amount by scraping.

(b) Specimens should be insulated in package to avoid breakage in transit.

(c) Mark item itself or on container holding pieces or scrapings.

(d) In circumstances where objects contain handprints or friction ridge detail present in blood, consideration should be given to removing sections of walls, floors, glass, etc., for submission to the Latent Fingerprint Section for examination and

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 73

chemical enhancement of these impressions for identification purposes.

(7) Blood in dirt or sand:

(a) If blood is encrusted on surface, the crusts should be removed and enclosed in separate pillboxes to avoid further contamination with dirt and sand during shipment. Remainder of specimen may be submitted in circular ice cream-type container.

(b) Mark containers appropriately.

(8) Blood on large metallic objects, such as car bumpers or pipes:

(a) If shipped in wooden box, the use of wooden cleats or wires inside box is suggested to hold specimen securely and avoid frictional removal of stains during shipment.

(b) Mark items themselves.

(9) Liquid blood samples: (See MIOG, Part II, 13-6.7 (9).)

(a) Samples from victim and suspect should always be submitted.

(b) No refrigerants and/or dry ice should be added to the sample.

(c) Blood samples (at least five cubic centimeters) from the victim and suspect should be collected in two vacutainer tubes, one containing EDTA (purple top) for DNA analysis and the other with no preservative (red top) for serological analysis. Package to protect from breakage and contain a spill. The internal packaging should include the "Biohazard" labels. (See also 13-8.4 (5).)

(d) No other anticoagulant or preservative is recommended. Package to protect from breakage, and submit at least 5 cubic centimeters of blood.

(e) Sample should be shipped refrigerated without delay to the Laboratory (air freight or similar rapid transit method).

(f) Stopper should be sealed with tape to avoid loosening due to air pressure differences in plane and possible loss of blood.

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 74

(g) While in storage, keep under refrigeration but
DO NOT FREEZE.

EFFECTIVE: 07/25/97

13-8.1.5 Blood Evidence Transmittal Letter

The letter of request should contain the following
information:

- | (1) | A brief statement of the facts surrounding the case.
- | (2) | Any claims made by the suspect as to the source of
blood on evidence items.
- (3) Deleted
- (4) Information concerning weather conditions to which
the evidence might have been exposed, contaminating substances, etc.
- (5) Information concerning disease state(s) of subject(s)
and/or victim(s) (examples: AIDS, Tuberculosis, Venereal Disease,
Hepatitis, etc.)

EFFECTIVE: 04/01/96

13-8.2 Other Significant Body Fluids

EFFECTIVE: 06/10/88

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 75

13-8.2.1 Body Fluid Examinations Aid Investigations

(1) Seminal Stains:

(a) Their identification by chemical and microscopic means on vaginal smears or swabs or on a rape victim's clothing may be of value in corroborating the claims of victim. Seminal fluid analysis will be performed by DNA analysis.

(b) Deleted

(c) Deleted

(2) Saliva Stains: In FBI cases, suspected saliva stains will be examined by DNA analysis. (See MIOG, Part II, 13-8.4 (3).)

(a) Deleted

(b) Deleted

(3) Urine Stains - May be qualitatively identified based on chemical testing; however, absolute identification may not be possible. DNA testing on urine stains may be attempted.

EFFECTIVE: 07/25/97

13-8.2.2 Deleted

EFFECTIVE: 09/24/93

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 76

13-8.2.3 Limitations on Seminal Stain and Saliva Stain|DNA Typing|

(1) Sometimes semen is mixed with urine or vaginal secretion of the victim and interpretation of DNA typing tests is more difficult.

(2) Saliva on cigarette stubs and on cigar butts may be DNA typable. Ash trays SHOULD NOT be simply emptied into a container. Individual butts should be separately packaged and care taken to avoid ash and debris contamination of any saliva present.

(3) Deleted

(4) ACCURATE EVALUATION OF|DNA TYPING|RESULTS ON QUESTIONED SEMEN AND SALIVA STAINS REQUIRES KNOWN LIQUID|OR DRIED|BLOOD SAMPLES FROM THE VICTIM AND SUSPECT.

EFFECTIVE: 04/01/96

13-8.2.4 Collection, Identification and Packaging of Evidence
Stained with Body Fluids | (See MIOG, Part II, 13-8.2.5.) |

(1) Semen Samples - Clothing or other material bearing suspected semen stains should be marked with dates and initials, DRIED IF MOIST, and each item packaged|separately in paper, NOT PLASTIC.|

(2) Saliva Samples: (See MIOG, Part II, 13-8.2.5.)

(a) Questioned samples should be handled as above for semen.

(b) For Dried Saliva Samples: (See MIOG, Part II, 13-6.7 (60).)

1. Saliva swabs (also called buccal swabs) can be collected using sterile cotton-tipped "Q tip" applicators. Generally these applicators can be purchased in individually wrapped sterile packets which contain a single sterile swab--generally a five-inch-long wooden stick with cotton tip.

2. The swab should be put in the mouth of the individual and placed firmly up against the inside of the cheek and

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 77

rotated. Generally two swabs, one from each cheek are collected. The swabs should be allowed to COMPLETELY AIR DRY, then packed and sealed in clean envelopes, paper packets, or in their original packet and conveyed to the Laboratory. After drying is complete, label appropriate envelope with type of sample, collector's initials, date and place of collection.

(c) NEVER submit liquid saliva samples.

(3) For Dried Blood Samples: From a fingerprick, or whole blood sample collected in a purple top (EDTA preservative) tube, a bloodstain is made on sterile, clean cotton cloth (usually washed cotton sheets). Two stains are usually prepared. The stains should be approximately one to two inches in diameter (about the size of a United States 50-cent piece). The stain should be allowed to COMPLETELY AIR DRY. The stain can be placed in a paper packet or envelope for shipping. The stains can then be stored in refrigerator/freezer conditions for a long period of time. (See MIOG, Part II, 13-6.7 (12).)

EFFECTIVE: 04/07/97

13-8.2.5 The Rape Case - Special Evidence Considerations (See MIOG, Part II, 10-3, 13-6.7 (67) & (68).)

(1) Because of the possibilities of serological evidence in rape being composed of possible mixtures of body fluids, evidence collection and preservation in a rape case warrant special consideration. The forensic serologist can often provide the investigator with valuable information beyond the statement that "semen is present" on an item if the necessary samples are obtained and properly preserved prior to submission to the Laboratory. The situation outlined below represents the ideal case; however, in many instances, much of the evidence listed may be obtained without excessive difficulty.

(2) It should be realized, however, that the majority of this evidence should be collected as soon as possible (within hours) of the crime.

(3) The following evidence should be obtained FROM THE VICTIM in a rape case:

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 78

(a) Two liquid blood samples at least 5 cc in volume. One red-topped tube for conventional serology analysis and one purple-topped tube for possible DNA analysis. These samples will enable the laboratory examiner to determine the victim's DNA characteristics for comparison with the evidence and the suspect's samples. (See MIOG, Part II, 13-6.7 (9) & 13-8.4 (5).)

(b) Four vaginal swabs (dry before packaging). These would be used for genetic grouping determination.

(c) Two (2) vaginal smear slides for use as a means of showing that spermatozoa (and semen) are, in fact, present. Slides to be sent to the FBI Laboratory should not be fixed or stained and all made from the vaginal swabs from step (b).

(d) Two clean swabs from the same package as the above vaginal swabs. These would be used as unstained control swabs to show that any result obtained from stained swabs is or is not due to the cotton of the swabs themselves.

(e) Deleted

(f) In addition to the above, items of clothing, bed clothes, etc., would logically be obtained from the scene and victim at this time or as soon after as possible.

(g) Appropriate hair samples should be collected from the victim (known head and pubic hairs, combed head and pubic hairs).

(4) Evidence collected from the SUSPECT(s) would logically include clothing, a liquid blood sample and a saliva sample, taken as described in 13-8.2.4 above, and hair samples.

EFFECTIVE: 07/25/97

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 79

13-8.3 DNA Analysis|Unit I|

The DNA Analysis|Units (DNA I and II) analyze|
deoxyribonucleic acid (DNA)|from biological tissues|recovered from
physical evidence in violent crimes. Evidence examined by the|units|
consists of known liquid and dried blood samples,|hairs, bones,
teeth,|portions of rape kit swabs and extracts, and body fluid stained
cuttings from homicide, sexual assault and serious aggravated assault
cases. These items of evidence are normally examined first to
determine the probative value of DNA analysis.

EFFECTIVE: 11/21/97

13-8.4 DNA Evidence Examination Policy

In general, this policy states that the FBI Laboratory
will accept evidence for DNA analysis from current, violent personal
crimes where appropriate standards for comparison are available. The
policy is specified as follows:

(1) BUREAU CASES

(a) Physical evidence submitted for DNA analysis in
connection with FBI investigations will be examined where appropriate.

(b) A known blood sample from the victim and suspect
for comparison purposes is required. No DNA analysis will be
conducted until known blood samples from both the suspect and the
victim have been received. Preliminary examinations, such as the
identification of blood or semen|or hair comparison,|may be conducted
without a known blood sample from the suspect, where appropriate.

(2) NON-BUREAU CASES

(a) DNA analysis on state and local cases will be
limited to homicide, sexual assault and serious aggravated assault
cases in which a suspect has been identified. In certain cases,
evidence will be accepted by the FBI Laboratory for DNA analysis even
though a suspect has not been identified. These exceptions include
serial homicide/rape cases and sexual assaults on young children.

(b) A known blood sample from the victim and suspect

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 80

for comparison purposes is required. No DNA analysis will be conducted until known blood samples from both the suspect and the victim have been received in the DNA Analysis Units.

(c) Requests for DNA analysis on previously adjudicated cases should not be submitted to the FBI Laboratory but should be referred by the investigative agency to one of the private DNA testing laboratories. Names and addresses of these laboratories can be provided on request.

(3) PCR TESTING (See MIOG, Part II, 13-8.2.1 (2).)

(a) The DNA Analysis Units now have on-line a technique called PCR (POLYMERASE CHAIN REACTION) testing. This technology allows the Laboratory to obtain a DNA type from other biological materials. Because of limited resources being devoted to this technology, strict case acceptance policy has been established by the Laboratory Division.

(b) Evidence for PCR analysis will be accepted only in FBI cases when a known blood sample from the suspect has been obtained and submitted along with the evidence. The Laboratory will not accept state or local cases or domestic police cooperation cases for PCR analysis unless previously authorized by the Assistant Director, Laboratory Division.

(4) REEXAMINATION POLICY

(a) It is the policy of the FBI Laboratory that no examination will be conducted on evidence which has been previously examined by another expert. However, the Laboratory will accept evidence samples for DNA analysis even though another crime laboratory may have conducted traditional tests on the evidence items if that crime laboratory does not have the capability to perform the DNA tests and if the submitted samples are determined to be of a quality and condition conducive to DNA analysis. The local forensic laboratory should be encouraged to contact the DNA Analysis Units of the FBI Laboratory prior to submission of this kind of evidence.

(b) Paternity or parentage testing involving a paternity index is not done by the DNA Analysis Units, even in criminal cases. The Laboratory does not currently perform these types of tests. Private paternity testing laboratories should be contacted for these services.

(c) In cases where conventional serology and no DNA

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 81

analysis is requested because of judicial rulings, trial delays, etc., it is the policy of the Laboratory that no analysis will be conducted.

(5) Evidence submitted for DNA analysis can be collected, preserved and transmitted to the Laboratory according to the guidelines set forth in Section 13-8.1.4 ("Collection, Identification and Wrapping of Bloodstained Evidence"): Bloodstained evidence should be completely air-dried before packaging and submitted promptly to the Laboratory. Two liquid blood samples, at least 5cc in volume, should be collected from both the suspect and victim; one red-top tube for conventional serology analysis (containing no preservatives) and one purple-top tube (containing EDTA) for DNA analysis. These blood samples should be submitted to the Laboratory without delay. In the event there will be a delay in submission of the dried stain evidence to the Laboratory, it should be kept frozen. (See MIOG, Part II, 13-6.7 (9), 13-8.1.4(9)(c) & 13-8.2.5 (3).)

EFFECTIVE: 11/21/97

13-9 MICROSCOPIC EXAMINATIONS

EFFECTIVE: 02/12/92

| 13-9.1 | Trace Evidence

| Trace evidence (hairs and fibers) examinations are
conducted by the Trace Evidence Unit. |

EFFECTIVE: 07/25/97

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 82

13-9.1.1 Trace Evidence Examinations Aid the Investigation

These examinations are valuable in that they assist in:

(1) Placing the suspect at the scene of the crime

(a) Transfer of hairs or fibers between the victim's and suspect's clothing in crimes of violence such as rape, assault and murder.

(b) Hairs or fibers from a suspect left at the scene of crimes such as burglaries, armed robberies and car thefts.

(2) Identifying the scene of the crime - Hairs or fibers left at the scene of crimes such as burglaries and armed robberies.

(3) Identifying the weapon or the instrument of a crime - Hairs or fibers on wrenches, knives or clubs.

(4) Identifying hit-and-run vehicles - Hairs or fibers adhering to suspect automobile.

EFFECTIVE: 07/25/97

13-9.1.2 Information Determined from an Examination of a Hair

Whether animal or human

(1) If animal, the species and/or family from which it originated (dog, cat, deer, beef, etc.)

(2) If human, the race, body area, method of removal from the body, damage, and alteration (bleaching or dyeing) and suitability for comparison with known hair samples may be determined.

(3) A comparison with known hair samples will result in a possible association, an elimination or a no conclusion.

(4) If a microscopic association is made between a questioned and known hair sample, DNA analysis may be performed on the questioned hair and compared to a known blood/saliva sample.

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 83

EFFECTIVE: 11/21/97

13-9.1.3 Information Determined From Fiber Examinations

(1) Identification of the type of fiber

- (a) Animal (wool)
- (b) Vegetable (cotton)
- (c) Synthetic (man-made)
- (d) Mineral (glass)

(2) Determination as to whether or not questioned fibers are the same type and/or color and match in microscopic characteristics as those fibers comprising a suspect garment.

EFFECTIVE: 02/12/92

13-9.1.4 Limitations of Hair Examinations

(1) Not absolute identification; however, is good circumstantial evidence.

(2) Age cannot be determined.

(3) Although racial characteristics, hair color and length may be of value for investigative lead purposes, microscopic characteristics exhibited by hairs are not. Furthermore, significant hair comparisons can only be conducted with known samples of hair, best obtained by collecting both pluckings and combings from an individual.

EFFECTIVE: 04/01/96

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 84

13-9.2 Fabric

A positive identification can be made if a questioned torn piece of fabric can be fitted to the known torn material.

EFFECTIVE: 02/12/92

13-9.3 Deleted

EFFECTIVE: 02/12/92

13-9.4 Cordage/Rope

A piece of rope left at the scene of the crime may be compared with similar suspect rope.

(1) Composition, construction, color and diameter can be determined.

(2) Manufacturer can sometimes be determined, if tracer present.

EFFECTIVE: 02/12/92

13-9.5 Botanical

Botanical examinations are conducted where plant material from a known source is compared with plant material from a questioned locale.

EFFECTIVE: 02/12/92

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 85

13-9.6 Anthropological

(1) Frequent identifications are made through comparisons of teeth with dental records and X-rays with corresponding bone structures.

(2) Examinations may be made to determine if skeletal remains are animal or human. If human, the race, sex, approximate height and stature and approximate age at death may be determined.

(3) DNA analysis may also be performed on the skeletal remains and compared to known blood/saliva samples in an attempt to assist in the identification process.

EFFECTIVE: 11/21/97

13-9.7 Wood

The presence of a suspect at the crime scene can often be established from a comparison of wood from his/her clothing, vehicle or possession with wood from the crime scene.

EFFECTIVE: 05/26/89

13-9.7.1 Types of Wood Examinations

- (1) Specific source
 - (a) Side or end matching.
 - (b) Fracture matching.
- (2) Species identification

EFFECTIVE: 05/26/89

13-9.8 | Deleted |

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 86

EFFECTIVE: 05/26/89

13-9.9 Deleted

EFFECTIVE: 05/26/89

13-9.10 Miscellaneous Examinations

These examinations include the following:

- (1) Fabric impressions
- (2) Glove prints
- (3) Feather Identification

EFFECTIVE: 05/26/89

13-10 CHEMICAL EXAMINATIONS

EFFECTIVE: 12/16/88

13-10.1 Toxicological Examinations

EFFECTIVE: 12/16/88

13-10.1.1 Purpose

Assists the medical examiner in determining the cause of death in suspected cases of poisoning.

EFFECTIVE: 12/16/88

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 87

13-10.1.2 Types of Poisons

- (1) Volatiles, such as carbon monoxide, alcohols, cyanide and solvents.
- (2) Heavy metals, such as arsenic, mercury, lead and antimony.
- (3) Nonvolatile organic poisons, such as drugs of abuse, pharmaceuticals and pesticides.
- (4) Miscellaneous, such as inorganic compounds, plant materials, caustic substances, and insects.

EFFECTIVE: 12/16/88

13-10.1.3 Background Information Useful to Toxicological Examiner

- (1) Copy of autopsy report.
- (2) Symptoms exhibited prior to death.
- (3) List of drugs administered to victim.
- (4) List of toxic chemicals normally encountered by victim in employment or at home.

EFFECTIVE: 12/16/88

13-10.1.4 Desirable Specimens for Complete Laboratory Examination

- (1) Brain (75 grams)
- (2) Liver (75 grams)
- (3) Kidney (75 grams)
- (4) Blood (20 cc) (add preservative and identify)
- (5) Urine (all)
- (6) Gastric contents (all)

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 88

- (7) Vitreous Humor
- (8) Any suspect food, drugs or chemicals

EFFECTIVE: 12/16/88

13-10.1.5 Preparation for Shipment to Laboratory

- (1) Place each organ and fluid in a separate sealed container.
- (2) Have pathologist label and initial each specimen.
- (3) Place container in insulated box with dry ice or freezer block (do not allow coolant to touch glass jars).
- (4) Mark package "Keep Cool" and transmit by overnight express.

EFFECTIVE: 12/16/88

13-10.2 Pharmaceutical and Drug Examinations

EFFECTIVE: 12/16/88

13-10.2.1 Information Helpful to Laboratory Examiner

- (1) Interview of suspect regarding source and use.
- (2) Prescription data.
- (3) If possible, submit sample in original container.

EFFECTIVE: 12/16/88

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 89

13-10.2.2 Collection and Preservation

- (1) Each item packaged separately and securely.
- (2) Each item and/or its container clearly identified by initials and item number.

EFFECTIVE: 12/16/88

13-10.2.3 Information Determined from the Examinations

- (1) Weight of pharmaceuticals.
- (2) Quantitation of active ingredients.
- (3) Whether a controlled substance or prescription item.

EFFECTIVE: 12/16/88

13-10.3 Arson Examinations

EFFECTIVE: 12/16/88

13-10.3.1 Reasons for Arson

- (1) Insurance | fraud. |
- (2) Revenge.
- (3) | Destruction of a crime scene. |
- (4) Pyromania.
- (5) Civil disobedience.

EFFECTIVE: 12/16/88

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 90

| 13-10.3.2 | Arson Evidence |

| (1) | Location

- | (a) Area of intense burning.
- | (b) Multiple areas of origin.
- | (c) "V" pattern areas. |

| (2) Arson | time delay | devices

-
- (a) Candle plants
 - (b) Cigarette in matchbook
 - (c) Molotov cocktail
 - (d) | Fused chemicals |
 - | (e) Electronic devices |

(3) Fire trails

- (a) Cloth ropes
- (b) Burn trails on carpeting
- (c) Deep charring trails in hardwood

(4) Removal of property - No typical remains of household
goods in debris

EFFECTIVE: 12/16/88

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 91

13-10.3.3 Types of Evidence

| Any sample from the point or area of origin, especially
specimens that are absorbent in nature or of a type that will retain a
flammable liquid, such as:

| (1) | Padded furniture

| (2) | Carpets

| (3) | Plasterboard

| (4) | Soil

| (5) | Clothing

| (6) | Molotov cocktails

EFFECTIVE: 12/16/88

13-10.3.4 Preservation of Evidence

Most readily flammable liquids are volatile and are easily
lost through evaporation.

(1) Use air tight containers

(a) Clean metal cans (preferable)

| (b) Kapak bags |

| (c) | Clean glass jars

(2) Properly identify specimen - Initial specimen or
container

EFFECTIVE: 12/16/88

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 92

13-10.3.5 Interpretation of Laboratory Results

(1) Gas Chromatography examination of distillates recovered from suspected arson debris usually aids in classifying the product with regard to distillation range such as gasoline, fuel oil and paint solvents.

(2) Limitations: Generally unable to identify specific brand of gasoline or fuel oil due to weathering, common intermixing of commercial brands and lack of distinguishing characteristics between brands.

EFFECTIVE: 12/16/88

13-10.4 General Chemical Analysis Examinations

EFFECTIVE: 12/16/88

13-10.4.1 Definition

Qualitative and quantitative analysis of miscellaneous chemical evidence.

EFFECTIVE: 12/16/88

13-10.4.2 Examples of Sources of Materials

(1) Deleted

(2) Fraud cases: Verification or disproving specifications in government purchases, product verification in "pyramiding" operations, con games, replacement of valuable product constituents with worthless constituents, etc.

(a) Desired information - Claims made for product by manufacturers or distributors, alleged constituents, complaints by users, etc.

(b) Limitations - Products cannot be tested mechanically or to determine pros or cons of use. Analysis is limited

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 93

to determination of constituents and literature search in reference thereto. Consideration of use of outside laboratories can be given to other necessary testing.

(3) Chemical destruction cases: Destruction of paint surfaces, lawns, and other valuables with harsh chemicals.

(4) Assault cases: Use of harsh chemicals on assault victims, lubricants used in rape and sodomy cases, miscellaneous unknown chemicals found at assault scene, etc.

(5) Sabotage: Harsh chemicals and other adulterants in fuel tanks and oil pans, gears, etc., of drive trains; sea water contamination aboard ships.

(6) Ink Analysis

(a) Scope - Comparison of the formulations of questioned and/or known ink specimens including typewriter ribbons and stamp pad inks.

(b) Limitations - When ink formulations are the same, it is not possible to determine whether or not they originated from the same source to the exclusion of other inks having similar formulations.

(c) Standard ink reference files necessary for possible association of a questioned ink with a manufacturer are available to the Laboratory.

(d) Determination of whether or not a document was written after the date shown thereon can only be made if a date taggant is in the ink. Only a limited number of companies utilize the taggant.

(7) Explosives and explosives residue analysis

(a) Post-explosion evidence

1. Scope - Examine evidence after an explosion for the presence of residues left behind from an explosive.

2. Types of Evidence - Metal, glass, plastics, rubber close to the seat of the explosion. Soil from the crater should be removed. Attempt to collect control samples from the surrounding area.

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 94

- contamination.
3. Take necessary precautions to avoid
 4. Containers for evidence
 - a. clean metal paint cans
 - b. plastic evidence bags placed and sealed
 - c. clean glass jars

in Kapak bags

(b) Preexplosion - raw explosive samples

1. Containers

- a. metal cans or glass jars
- b. be aware of shipping requirements for

explosives.

2. Limitations - In some cases the manufacturer of a material can be obtained. Comparison with samples for batch comparisons is possible.

(8) Paint and plastics analysis

(a) Paints

1. Scope - Comparison of paint samples from known source to a paint sample removed from a specimen.

2. Limitations - When paint samples match, it can only be said that the specimen may have come from the known source or one just like it. Only in rare cases can a positive match, to the exclusion of all others, be made.

3. National Automotive Paint File (NAPF) is housed in the Laboratory.

(b) Plastics

1. Scope - Analysis of plastic or polymeric materials. Plastic fragments from hit and run accidents can be reconstructed into its original shape.

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 95

(9) Tape Analysis

(a) Scope - Tapes come in a variety of forms such as masking, electrical, and duct tape. These materials have been used to bind homicide victims, cover drug packs, and components of improvised explosive devices. End matches are the most powerful results.

(10) Miscellaneous chemical examinations such as:

- (a) Chemical agents on bank robbery packets
- (b) Dyes encountered in bank dummy packets or security devices can be compared with known standards in the Laboratory
- (c) Constituent determination in patent cases
- (d) Flash and water soluble paper in gambling and espionage cases
- (e) Verification of stolen chemicals in ITSP and TFIS cases, and
- (f) Harsh chemicals or sugars in DAMV cases.
- (g) Adulterants in Tampering With Consumer Product cases.
- (h) Trace drugs in money, clothing, suitcases, and other containers
- (i) Smokeless powder comparisons
- (j) Food analyses
- (k) Cosmetic examinations
- (l) Button examinations
- (m) Lubricants - such as Vaseline in rape cases.

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 96

EFFECTIVE: 11/21/97

13-11 MINERALOGY EXAMINATIONS

(1) Mineralogy is part of the Trace Evidence Unit.

(2) Mineralogy examinations are conducted on those materials which are mostly inorganic, crystalline or mineral in character, and include glass, building materials, soil, debris, industrial dusts, safe insulations, minerals, abrasives, and gems.

Comparisons can, by inference, connect a suspect or object with a crime scene, prove or disprove an alibi, provide investigative leads or substantiate a theorized chain of events. (See MIOG, Part II, 13-15 (2).)

EFFECTIVE: 11/21/97

13-11.1 Glass

Glass, a noncrystalline, rigid material usually exhibits excellent physical, optical and compositional properties for comparison purposes. When a window breaks, glass particles can shower 10 feet or more toward the direction of the force. Particles, therefore, get onto hair and clothing of the perpetrator. Particles also become embedded in bullets and/or objects used to break windows. Particles of broken glass from a hit-and-run vehicle are often found on the victim's clothing.

(1) Deleted

(2) The Laboratory examiner cannot identify the source to the exclusion of ALL other sources; however, it can be stated and demonstrated that it is highly improbable that the particles came from a source other than the matching known source; if two or more different known sources can be matched, the conclusion is greatly enhanced.

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 97

EFFECTIVE: 11/21/97

13-11.1.1 Glass Fractures

Fracture patterns are unique. A physical match of two pieces of glass establishes that they came from a mutual source to the exclusion of all other sources; examinations also result in valuable information as to the direction of the breaking force.

(1) Penetration of glass panes by bullets or high speed projectiles produces a cone pattern from which the direction and the angle of penetration can be determined. If the cone is not present, stress line patterns as described below are used to determine the direction of the force.

(2) By a study of stress lines on radial cracks near the point of impact, the direction of the force which broke the glass can be determined.

(a) This determination depends on identification of the radial cracks and the point or points of impact. A sufficient amount of glass must be submitted to reconstruct a portion of the pane from the edge to the point of impact. All, or as much as possible, of the pane should be submitted.

(b) The pieces of glass remaining in the window after the breaking should each be labeled to indicate inside or outside, left, right, top or bottom prior to submission to the Laboratory. (See 13-11.1.3 below.)

(c) The direction of the breaking force usually cannot be determined from tempered glass (commonly found in side and rear auto windows) or very small panes of glass.

(d) Laminated glass, such as windshields, present special problems. Submit entire windshield if possible.

(e) Heat breaks can be identified, but the side on which the heat was applied cannot be determined from fracture edges.

(3) Pieces of glass may often be fitted together.

(a) By fitting pieces together with microscopic matching of stress lines, the Laboratory examiner can positively

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 98

identify the pieces as originally having been broken from a single pane, bottle or headlight. (See 13-11.1.3 below.)

(b) If pertinent portions of a bottle or headlight can be fitted together, the manufacturer, type, etc., may be determined for lead purposes.

EFFECTIVE: 11/21/97

13-11.1.2 Glass Fibers and Fiberglass Insulation Materials

Glass fibers from boats, auto fenders, filters and most often building or duct insulations may adhere to the clothing or belongings of suspects. By microscopic comparison, glass fibers are identified and compared with the known source.

EFFECTIVE: 09/24/93

13-11.1.3 Collection of Glass Specimens (See MIOG, Part II, 13-11.1.1(2)(b) & (3)(a).)

(1) In cases where the direction of breaking force is required, pieces left undisturbed in the window must be marked as to inside or outside, top, bottom, left, right and all available glass must be submitted so that enough pieces can be fitted together to identify the radial cracks near and at the point of impact.

(2) Where pieces are large enough to fit together, all available glass must be submitted to increase the probability of finding matching edges.

(3) Do not place glass samples in paper or plastic bags and envelopes. Wrap each piece securely and package tightly.

(4) Send all available items of clothing of the suspect, comb his/her hair and check for particles in sweat on skin and in wounds.

(5) Where fiberglass insulation is involved, be sure all sources from various areas are sampled. Look for added insulation

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 99

over older insulation. Send both.

EFFECTIVE: 09/24/93

13-11.2 Soils, Dusts, Debris

Soil is defined as any finely divided material on the surface of the earth and may contain such man-made materials as cinders, shingle stones, glass particles, paint, rust, etc. Soil, as a category, includes debris, industrial dusts, oily soil from under vehicles as well as natural soils.

EFFECTIVE: 06/15/81

13-11.2.1 Value of Soil as Evidence

(1) Soil varies widely from point to point on the surface of the earth and even more with depth. Many small samples are better than one large sample.

(2) Soil cannot be positively identified as coming from one source to the exclusion of all others; but the Laboratory expert can associate questioned soil with a most probable source, conclude that a source cannot be eliminated or that a point or area could not be the source of the questioned soil. Such conclusions have proven extremely valuable in the proof of criminal cases.

(3) Industrial dust specimens or soil near factories are often distinctive.

(4) Debris may contain particles characteristic of a specific area.

EFFECTIVE: 06/15/81

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 100

13-11.2.2 Collection of Soil Specimens | (See MIOG, Part II,
13-6.7 (62).) |

(1) The investigator should seek likely areas at the crime scene such as shoe prints, tire marks, burial sites or muddy areas where a transfer of soil to the suspect is logical. The investigator should attempt to get samples which visually appear to be the same as the soil on the suspect's shoes or belongings.

(2) Several samples should be taken from crime scene areas because of the above-mentioned variation in small areas; additional samples in at least four directions up to 300 feet from the scene should be sampled to show that a variation does exist and to allow the Laboratory to "judge" the probability that the questioned soil could have come from the area. Samples should be taken from the surface no deeper than shoes or tires would depress the soil. Many small samples are desirable, a mixture from a large area or a sample taken too deep may introduce unwanted variations.

(3) Alibi areas such as the suspect's yard or work area should be sampled.

(4) |Deleted|

(5) Where soil has fallen or been deposited inside buildings or cars send carpets or attempt to keep lumps intact by secure packing; lumps break up in a too large, unpacked container.

(6) Soil from under car fenders may be in layers. Such soil should be chipped or cut off and packaged so that layers can be kept intact for comparison with similar lumps that may be found at the crime scene.

(7) Shoes, tires and other items should be submitted to the Laboratory. Attempts to remove the soil in the field may destroy valuable soil characteristics.

EFFECTIVE: 07/25/97

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 101

13-11.2.3 Packaging of Soil Specimens | (See MIOG, Part II, 13-6.7
(62).)|

- | (1) | Air dry soil before packaging. |
- | (2) | Do not use envelopes or glass jars for soil.
- | (3) | Use leakproof containers such as film canisters or
plastic pill bottles.

EFFECTIVE: 11/21/97

13-11.3 Safe Insulations

Safe insulation is found between the walls of fire resistant safes in vaults and safe cabinets. It is readily transferred to tools and clothing.

EFFECTIVE: 01/11/85

13-11.3.1 Value as Evidence

- (1) Safe insulation can usually be identified as such.
- (2) The make of safe can often be determined by examination of the insulation.
- (3) Microscopic comparison of particles or deposits with insulation from the broken safe connects, by inference, clothing or tools with the safe.
- (4) Safe insulation on tools may "make" a case for possession of burglar's tools.

EFFECTIVE: 01/11/85

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 102

13-11.3.2 Collection and Packaging

- (1) Sample near broken edge of insulation.
- (2) Send tools or clothing to Laboratory; do not remove deposits in the field.
- (3) Pack to keep lumps intact; protect deposits on tools by wrapping.

EFFECTIVE: 05/11/87

13-11.4 Building Materials

EFFECTIVE: 05/11/87

13-11.4.1 Value as Evidence

(1) Where entry is through a roof or wall, particles adhere to clothing or tools and may be on the loot or in toolbags or vehicles.

(2) These materials are usually common materials.
Maximum value as evidence is gained through the presence of several types, such as brick, mortar, plaster, stucco, etc.

EFFECTIVE: 05/11/87

13-11.4.2 Collection and Packaging

(1) The hole should be examined and materials of each type should be obtained.

(2) Submit in leakproof containers.

EFFECTIVE: 05/11/87

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 103

13-11.5 Minerals, Rocks, Ceramics

These materials will be examined or compared as requested.

EFFECTIVE: 05/11/87

13-11.6 Abrasive Materials

In sabotage and malicious damage to engines, cars, trains, etc., abrasive materials may be put in oil or lubricants. These materials can be identified as sand or commercial abrasives and are of some value for comparison.

EFFECTIVE: 05/11/87

13-11.6.1 Collection of Specimens for Abrasives

(1) If oil, the oil from the engine sump and/or filters should be submitted; abrasives settle in oil or fuel.

(2) Send affected bearings or parts; the abrasive may be embedded; scratches or cuts may be typical of abrasive damage.

EFFECTIVE: 05/11/87

13-11.7 Gems, Precious Stones, Synthetic and Fake Gems

The Laboratory can determine whether gemstones are genuine, synthetic or fake. If expedient, a Laboratory examiner is available for on scene examinations. The Laboratory can, on a limited basis depending on inventory, provide identifiable or Bureau property gemstones for undercover operations whether or not recovery of the gemstones is anticipated.

EFFECTIVE: 09/24/93

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 104

13-12 FIREARMS IDENTIFICATION

Firearms identification deals with the comparison of bullets, cartridge cases and other ammunition components to a particular firearm to determine if they had been fired by that particular firearm to the exclusion of all other manufactured firearms.

EFFECTIVE: 04/07/97

13-12.1 Conclusions

Either one of the three conclusions listed below can be reached. If either (1) or (2) is reached, that conclusion is positive as in fingerprint identification.

(1) The bullet, cartridge case, or shotshell casing was fired by the weapon.

(2) The bullet, cartridge case, or shotshell casing was not fired by the weapon.

(3) There are not sufficient microscopic marks remaining on the bullet, cartridge case, or shotshell casing to determine if it was fired by the weapon or the condition of the weapon precludes the possibility of making an identification.

EFFECTIVE: 01/31/78

13-12.2 Terminology

EFFECTIVE: 01/31/78

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 105

13-12.2.1 Caliber

In general, caliber denotes the nominal bore diameter of a barrel measured in either hundredths of an inch (.01) or in millimeters (mm). This provides an initial grouping capability, such as referring to .22 caliber, .30 caliber or .38 caliber.

EFFECTIVE: 01/31/78

13-12.2.2 Cartridge Designations

These designations expand from the basic cartridge grouping in a variety of ways. Each one of these designations denotes a specific cartridge case size and configuration. While some cartridges will interchange, most are specific for a firearm of a particular cartridge designation. Among cartridge designations are the following:

- (1) Descriptive words: .38 Special, .41 Magnum, .380 Auto, 9mm Corto.
- (2) Original powder charge: .30-40 Krag.
- (3) Manufacturer's or designer's name: .30 Remington, 6mm Remington, .257 Roberts
- (4) Velocity: .250-3000
- (5) Year of adoption: .30-06 Springfield
- (6) Diameter in millimeters and length of case: 9 x 19, 8 x 57.

EFFECTIVE: 07/25/97

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 106

13-12.2.3 General Rifling Characteristics

These vary from manufacturer to manufacturer and consist of:

- (1) Number of lands and grooves.
- (2) The widths of the lands and grooves.
- (3) Direction of twist of rifling.
- (4) Caliber.

EFFECTIVE: 07/25/97

13-12.3 Types of Examinations

EFFECTIVE: 05/26/89

13-12.3.1 Bullets

Marks on bullets can be produced by rifling in the barrel of the firearm or possibly in loading.

(1) Recovered evidence bullet: Determine manufacturer, specific caliber, type and make of firearm from which fired and whether sufficient marks are present for identification. (Make of firearm involved based on general rifling characteristics.)

(2) Bullet versus firearm: Determine whether bullet fired from firearm.

(3) Shot pellets, buckshot and slugs from the victim or scene: Can identify size of the shot and gauge of the slug. Occasionally, shot can be identified to the barrel of a particular shotgun.

(4) When a bullet and/or fragments bearing no microscopic marks of value for identification purposes are encountered, it is often useful to perform a quantitative analysis of the bullet and/or fragment and compare them to the similarly analyzed bullets of any

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 107

recovered suspect ammunition (for example, cartridges remaining in suspect's firearm, cartridges in suspect's pockets, partial boxes of cartridges in suspect's residence). When two or more lead samples are determined to be compositionally indistinguishable from one another, a common manufacturer's source of lead is indicated. Lead composition information in conjunction with other circumstantial information is often useful in linking a suspect to a shooting. (Lead examinations are conducted by the Materials and Devices Unit. See MIOG, Part II, 13-14.)

Compositional analysis of shot pellets and rifled slugs can provide similar useful circumstantial information.

EFFECTIVE: 07/25/97

13-12.3.2 Fired Cartridge Case or Shotshell Casing

Marks on a fired cartridge case or shotshell casing can be produced by breech face, firing pin, chamber, extractor and ejector.

(1) Fired cartridge case found at scene: Determine specific caliber, type and possibly make of firearm in which fired, and whether sufficient marks are present for identification.

(2) Fired shotshell casing found at scene: Determine gauge, original factory loading and whether sufficient marks are present for identification.

(3) Wadding or shot from victim or scene: From wadding determine gauge and possibly manufacturer of wadding. From shot, determine size. Shot not identifiable with a suspect firearm.

(4) - Fired cartridge case/shotshell casing versus firearm: To determine whether loaded into and/or fired in firearm.

(a) Based on identifiable firing pin impression, breech face or chamber marks, can establish as fired in specific firearm.

(b) Based on extractor or ejector marks, can only identify as having been loaded into and extracted from specific firearm.

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 108

EFFECTIVE: 04/07/97

13-12.3.3 Unfired Cartridge or Shotshell

(Note: See 13-12.4.2 regarding "Shipping of Live Ammunition.") Sometimes it is important to determine whether the unfired cartridge or shotshell was loaded into and extracted from a firearm based on the presence of extractor and/or ejector marks. The following can be determined:

(1) Cartridge: Specific caliber, type of firearm involved and whether sufficient marks for identification.

(2) Shotshell: Gauge and whether sufficient marks are present for identification.

(3) Cartridge/shotshell versus firearm: Determine if loaded into and extracted from a suspect firearm. Does not apply to revolvers.

EFFECTIVE: 04/07/97

13-12.3.4 Gunshot Residues

Gunshot residues may be located, depending on the muzzle-to-garment distance, by

(1) Microscopic examination of the area surrounding the hole for gunpowder particles and gunpowder residues, smudging and singeing.

(2) Chemical processing of area surrounding hole to develop a graphic representation of powder residues and lead residues around hole. Test patterns obtained compared with those produced at various distances using suspect firearm and ammunition like that used in the case--from same source if possible.

(3) The Firearms/Toolmarks Unit (FTU) only examines victim's clothing for gunshot residues in order to determine distance

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 109

of the muzzle of the firearm to the clothing at the time of discharge. Therefore, only the clothing from the area where the victim was shot should be submitted for examination for gunshot residues. For example, if the victim was shot in the chest, requests for examination of the victim's pants, shoes, etc., for gunshot residues should not be made.

(4) In rare occasions the FTU will examine shooter's clothing for gunshot residues, primarily when there is evidence of a struggle between the victim and the subject. The FTU does not examine suspected shooter's clothing for the presence of gunshot residues in order to prove that they discharged a firearm. In the event an examination of a shooter's clothes for the presence of gunshot residues is needed, the request should be directed to the Chemistry Unit.

EFFECTIVE: 07/25/97

13-12.3.5 Shot Pattern

The distance at which a shotgun was fired can be determined. It is necessary to test fire THE SUSPECT|firearm|at various distances using the same type of ammunition as involved in the case being investigated. Fired shotshells from the suspect|firearm| can be submitted. See paragraph 13-12.4.2 regarding the shipment of live ammunition.

EFFECTIVE: 04/07/97

13-12.3.6 Trigger Pull

The amount of pressure necessary to fire a weapon can be determined.

EFFECTIVE: 05/26/89

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 110

13-12.3.7 Determination of Accidental Firing

"Accidental" is a determination of a state of mind; however, a firearm can be examined to determine if it can or cannot be fired without pulling the trigger.

EFFECTIVE: 04/07/97

13-12.3.8 Identification of Gun Parts

Gun parts found can be identified as to

(1) Type of firearm from which it originated

(2) In some cases, it might be possible to determine the part that came from a suspect firearm; however, in most instances, examination of the part will only determine if the part is consistent in observable physical characteristics with the type of parts utilized in the suspect firearm.

EFFECTIVE: 04/07/97

13-12.4 Submission of Evidence

EFFECTIVE: 05/26/89

13-12.4.1 Clothing for Gunshot Residue Examination

(1) Protect each article of clothing at the time of removal and wrap each separately. Each article of clothing that has blood on it must have a biohazard label placed on the outside of its individual package. A biohazard label must also be placed on the outside of the box containing the separate wrapped packages, as well as on the outer wrapping of the box. (See MIOG, Part II, 13-3.1 (4)(e).)

(2) Make certain all garments are AIR-DRIED in shade before submitting to the Laboratory.

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 111

(3) Provide autopsy reports and/or copies of autopsy photos if victim is deceased. Otherwise advise as to location of gunshot wounds.

EFFECTIVE: 04/01/96

13-12.4.2 Live Ammunition (See MIOG, Part II, 13-6.7 (5), (16), 13-6.7.1, 13-12.3.3, 13-12.3.5, 13-12.4.3; MAOP, Part II, 2-2.2.1, 6-2.3.9.)

Live ammunition cannot be sent through the U.S. Postal Service but can be shipped via Federal Express. The following guidelines must be strictly followed in order to comply with Department of Transportation regulations:

(1) Deleted

(2) Air Shipments (Federal Express) -

(a) Cardboard box with appropriate label and invoices marked "Federal Express."

(b) Shipper's certification for restricted articles.

(c) "Small Arms Ammunition" stamped on outside of box.

EFFECTIVE: 04/07/97

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 112

13-12.4.3 Bullets, Cartridge Cases and/or Firearms

(1) Ammunition components such as bullets, cartridge cases, wads and firearms can be sent to the Laboratory by registered mail, U.S. Postal Service. Complete cartridges, gunpowder and/or unfired primers must be shipped by Federal Express. (See MIOG, Part II, 13-6.7 (5), (15), (17), (29); MAOP, Part II, 6-2.3.9.)

(2) Firearms have been submitted to the Laboratory with foreign objects such as flex cuffs, pencils, etc., in the barrel/chamber area, or the actions have been left open which allowed packing material (styrofoam/shredded paper) to enter these areas. WHILE SAFETY IS CERTAINLY PARAMOUNT, AND EVERY EFFORT SHOULD BE MADE TO MAKE SURE A FIREARM IS UNLOADED WHEN IT IS SENT TO THE LABORATORY, it should be recognized that certain practices, while serving the purpose of rendering the firearm safe, can adversely affect some of the Laboratory examinations for which the firearm is being submitted.

(3) In firearms examinations, the most critical areas of a firearm are the bore, chamber and breech face. Placing a flex cuff through the barrel of a pistol, for example, could result in the cuff material rubbing against, and changing the microscopic marks in the bore and chamber areas of the barrel and the breech face area of the slide or dislodging trace evidence in these areas. Likewise, placing a pencil or rolled-up piece of paper in the action to keep it opened, could also adversely affect the marks on the breech face and also allow packing material to enter the firearm. In some instances, a firearm has been received which would not function due to shredded paper or styrofoam pellets having entered the action/chamber areas.

(4) As an examination of a firearm can involve additional Laboratory examinations for latent fingerprints, blood, etc., firearms evidence should be packaged to eliminate or reduce as much as possible the likelihood of damage to such evidence.

Firearms can be sent by registered mail, U.S. Postal Service.

EFFECTIVE: 04/07/97

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 113

13-12.5 Marking Specimens for Identification

(1) | Bullets, cartridge cases, shotshell casings, cartridges, shotshells and other firearms-related evidence should be marked with initials or other personal identifying data on the primary evidence container only. (Caution: Do not place markings on the item(s) itself. Any trace evidence on the item and the microscopic marks need protection from possible loss or destruction.) |

| (2) | Firearms: (See MIOG, Part II, 13-6.7 (29).)

| The primary container with the firearm should be marked with initials or other personal identifying data. (Caution: Do not place markings on the firearm itself. The firearm may need to undergo various examinations, such as DNA, Trace, or Latent Fingerprint; therefore, protection must be afforded to the firearm to avoid possible loss or destruction of evidence.) |

EFFECTIVE: 07/25/97

13-12.6 Obtaining Test Specimens

| Whenever possible, the firearm should be submitted to the Laboratory. If the firearm cannot be submitted, | call the Firearms/Toolmarks Unit for instructions. |

EFFECTIVE: 07/25/97

13-12.7 Standard Reference Files

EFFECTIVE: 06/26/91

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 114

13-12.7.1 Reference Firearms Collection

This collection contains over 3,000 handguns and 2,000 shoulder weapons and is used for such things as:

- (1) Locating serial numbers
- (2) Replacing inoperable firearms parts
- (3) Identifying gun parts

EFFECTIVE: 04/07/97

13-12.7.2 Standard Ammunition File

The Standard Ammunition File is maintained in the FBI Laboratory's Firearms-Toolmarks Unit (FTU). This file is continuously updated and contains over 15,000 commercial and military ammunition specimens of both domestic and foreign manufacture. These specimens serve as standards which assist in the determination of ammunition type and manufacture. A computerized database permits comprehensive searching of this file on the basis of the observable physical characteristics present on unknown ammunition components.

EFFECTIVE: 04/01/96

13-12.7.3 Reference Fired Specimen File

This file contains test bullets and cartridge cases obtained from firearms which have been fired in the Laboratory. (Note: An "Unidentified Ammunition File," "Open Case File" or "Unsolved Crime File" consisting of bullets and cartridge cases recovered from crime scenes is no longer maintained by the Laboratory.)

EFFECTIVE: 04/07/97

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 115

13-12.7.4 General Rifling Characteristics File (GRC)

This computerized data file contains information relating to the general rifling characteristics of a number of firearms. In those cases in which no firearm is provided, the GRC file is used by the Firearms-Toolmarks Unit to provide a list of firearms which could possibly have fired the submitted bullet or cartridge case.

EFFECTIVE: 04/01/96

13-12.8 Disposition of Firearms and Related Property

The following guidelines are to be used in Bureau cases.

(1) Any firearm to be disposed of should be done so by the Laboratory.

(2) The Laboratory can dispose of firearms and related property with a court order, Declaration of Forfeiture, and a Declaration of Abandonment Vesting Title to the United States. If such cannot be obtained, see United States Marshal's Manual, Section 709.01 (Prisoner's Property) or Section 322.01 (Abandoned Property). When obtaining a court order, the requesting attorney should be advised to seek an order directing the firearms into the custody of the FBI "for its use or for any other official purpose." The court order must be signed by a judge. (See MAOP, Part II, 2-4.4.6.)

(3) The Laboratory can dispose of firearms and related property purchased with Bureau funds when all investigations and court proceedings have been adjudicated.

EFFECTIVE: 04/07/97

13-12.9 Deleted

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 116

EFFECTIVE: 05/31/94

| 13-12.9.1 | Deleted |

EFFECTIVE: 05/31/94

| 13-12.9.2 | Deleted |

EFFECTIVE: 05/31/94

| 13-12.9.3 | Deleted |

EFFECTIVE: 05/31/94

13-13 TOOLMARK IDENTIFICATION

Toolmark examinations include, but are not limited to, microscopic studies to determine if a given toolmark was produced by a specific tool. In a broader sense, they also include the identification of objects which forcibly contacted each other; were joined together under pressure for a period of time and then removed from contact; and were originally a single item before being broken or cut apart. The inclusion of these latter areas results from the general consideration that when two objects come in contact, the harder (the "tool") will mark the softer. (Saws, files and grinding wheels are generally not identifiable with marks they produce.)

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 117

EFFECTIVE: 01/31/78

13-13.1 Conclusions

- (1) That the tool produced the toolmark
- (2) That the tool did not produce the toolmark, or
- (3) That there are not sufficient individual characteristics remaining within the toolmark to determine if the tool did or did not produce it.

EFFECTIVE: 01/31/78

13-13.2 Types of Toolmark Examinations

EFFECTIVE: 01/31/78

13-13.2.1 Toolmark with Tool

Several comparisons can be made between a tool and a toolmark such as the:

- (1) Examination of the tool for foreign deposits such as paint or metal for comparison with a marked object.
- (2) Establishment of the presence or nonpresence of consistent class characteristics.
- (3) Microscopic comparison of a marked object with several test marks or cuts made with the tool.

EFFECTIVE: 01/31/78

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 118

13-13.2.2 Toolmark Without Tool

Examination of the toolmark can determine:

- (1) Type of tool used (class characteristics)
- (2) Size of tool used (class characteristics)
- (3) Unusual features of tool (class or individual characteristics)
- (4) Action employed by the tool in its operation
- (5) Most importantly, if the toolmark is of value for identification purposes.

EFFECTIVE: 04/07/97

13-13.2.3 Metal Fracture

Fracture examinations are conducted to ascertain if a piece of metal from an item such as a bolt, automobile ornament, knife, screwdriver, etc., was or was not broken from a like damaged item available for comparison. This type of examination may be requested along with a metallurgical examination (see major topic 13-14 elsewhere in this section).

EFFECTIVE: 04/07/97

13-13.2.4 Marks in Wood

This examination is conducted to ascertain whether or not the marks left in a wood specimen can be associated with the tool used to cut them, such as pruning shears, auger bits, etc. This examination may be requested along with a wood examination (see secondary topic 13-9.7 elsewhere in this section).

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 119

EFFECTIVE: 01/31/78

13-13.2.5 Pressure/Contact

Pressure or Contact examinations are conducted to ascertain whether or not any two objects were or were not in contact with each other either momentarily or for a more extended time.

EFFECTIVE: 01/31/78

13-13.2.6 Theftgate Cast Material

Theftgate Cast Material impressions of stamped numbers in metal, such as altered vehicle identification numbers, can be examined and compared with other cast impressions, as well as with suspect die stamps. Instructions for use of this casting material can be obtained from the Firearms/Toolmarks Unit, FBI Laboratory. (See MIOG, Part II, 13-13.3.1.)

EFFECTIVE: 07/25/97

13-13.2.7 Lock and Key Examinations

(1) The purpose of a lock examination is to determine, if possible, if toolmarks are present that indicate attempts were made to pick the lock, or if some type of tool or instrument was used to force the lock. When such a request is made, only the lock or those parts of the lock which have visible toolmarks on them should be submitted. For example, if the outer doorknob was forced, then only that knob should be submitted for examination. Also, in the case of worn locks, marks that were already on the lock at the time of the crime should be noted in the request for examination.

(2) Examination of keys can determine their observable physical characteristics, such as number and depth of cuts, blade style, etc. A determination of whether key will operate a specific lock can only be made after the key is actually tested in the questioned lock and does not require an examination by an examiner from the Firearms/Toolmarks Unit.

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 120

(3) As the main thrust of the FTU examination is concerned with toolmarks, if there are questions about the operation of a particular style lock, consideration should be given to contacting a local locksmith with those questions.

EFFECTIVE: 07/25/97

13-13.3 Obtaining Evidence in Toolmark Cases | (See MIOG, Part II,
13-6.7 (64).)|

(1) It is most desirable, if possible, to submit the actual toolmarked area for direct comparison. (Note: In number restoration cases, the Laboratory will routinely make a cast of the toolmark for a possible future comparison with any suspect die stamps.)

(2) If it is impossible to submit the original, prepare and submit a cast, preferably using Theftgate Casting Material or a suitable silicone-based material. For instructions on how to prepare a plastic cast/impression see paragraph 13-13.3.1 below.

(3) Photographs, although helpful in presenting an overall location of the mark, are of no value for identification purposes.

(4) Do not forget to obtain samples of paint, safe insulation, and any other material likely to appear as foreign deposits on tools.

(5) - DO NOT place the tool against the toolmark for size evaluation.

EFFECTIVE: 07/25/97

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 121

13-13.3.1 Theftgate Cast Material Impressions (See MIOG, Part I,
26-2.8; Part II, 10-3, 13-13.2.6, 13-13.3.)

The following instructions are for making a plastic
cast/impression of stamped numbers in metal.

(1) All casts should be taken BEFORE ANY small number
restoration is attempted. (See "Items with Obliterated Identification
Markings" under secondary topic 13-14.2 elsewhere in this section for
further information on number restoration.)

(2) Casts should be taken using Theftgate Cast Material
(made by Advanced Ceramics Services, Denver, Colorado, Telephone
Number (303) 237-5456) which should be available in each office or can
be obtained by contacting the Firearms/Toolmarks Unit in the
Laboratory Division.

(3) The number one priority in taking a cast of stamped
numbers is cleaning the number area of any foreign matter as the cast
material will duplicate any foreign material left in the stamped
characters. Thus, paint and dirt should be removed from the stamped
area with a suitable solvent (acetone, gasoline or a commercial paint
remover). A toothbrush could be used to help clean down to the bottom
of the stamped area and IN NO INSTANCE should a wire brush be used to
clean the area as this will scratch the numbers and make subsequent
identification of the stamps impossible. If there is any rust in the
stamped numbers, use of "NAVAL JELLY" is helpful in removing the rust.

(4) Having cleaned the surface, a dam should be built
around it to retain the liquid casting material while hardening and
cooling. The liquid and the powder of the replica kit are mixed for
one minute in the plastic bottle that contained the powder. The dam
material should be a soft pliable clay-like material such as caulking
cord, "Play Dough" or modeling clay. Prior to forming the dam, nylon
filament tape should be placed at each end of the characters, partly
within the dam area to facilitate the cast removal. All voids around
the dam should be sealed to prevent leaking. Once the liquid has been
poured and hardened, lift up on the ends of the tape to lift out the
cast. If the cast has a lot of paint and rust, additional casts
should be taken until the best possible cast has been obtained and
this should be submitted to the Laboratory.

(5) The Theftgate Cast Material is available in three
formulations for use in three different temperature ranges: 40 to 69
degrees Fahrenheit, 70 to 80 degrees Fahrenheit, and over 80 degrees
Fahrenheit. At very low temperatures, setting time can be several

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 122

hours even when using the low temperature range formulation. In this instance, if possible, the vehicle or metal should be moved to a heated building. Further the area can be heated by several methods such as heat lamp, infrared light bulb, hair dryer directed on the number area and then upon the cast, etc. The use of a torch to heat the area is not recommended.

EFFECTIVE: 07/25/97

13-13.4 Submitting Toolmark Evidence to Laboratory (See MIOG, Part II, 13-6.7 (64).)

(1) Pack the evidence, possibly with cotton, to preserve the evidence and prevent contamination.

(2) Properly identify each item to facilitate court presentation. Consider the possible need in court of the object from which the specimen was cut.

(3) Submit the tool rather than making test cuts or impressions in field.

(4) Mark ends of evidence which are or are not to be examined.

EFFECTIVE: 07/25/97

13-13.5 Reference Files (See MIOG, Part I, 26-2.8.)

(1) National Automobile Altered Numbers File: The FBI Laboratory is maintaining in the National Automobile Altered Numbers File selected specimens, including surface replica plastic impressions of altered vehicle identification numbers found on stolen cars, trucks and heavy equipment. The purpose of this file is to have a central repository for such specimens of altered numbers so that comparisons can readily be made at any time in an attempt to identify recovered stolen cars and possibly link such vehicles with commercialized theft rings nationwide or other cases investigated by the Bureau.

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 123

(2) Deleted

EFFECTIVE: 04/07/97

13-13.6 Identification Manuals

Laboratory manuals concerning the identification of automobiles, foreign and domestic, tractor trucks, trailers and construction equipment are updated on a timely basis. These manuals contain both information and photographs which indicate [REDACTED] and provide investigative aids to the field Agent examining these kinds of equipment. Copies of these manuals can be obtained by contacting the Firearms-Toolmarks Unit of the Laboratory Division. b2/b7E

EFFECTIVE: 05/26/83

13-14 METALLURGY EXAMINATIONS (See MIOG, Part II, 13-12.3.1, 13-13.2.3.)

Metallurgy encompasses the science of metals and other materials. These materials may be metallurgically examined for comparison purposes and/or information purposes.

EFFECTIVE: 07/25/97

13-14.1 Examinations for Comparison Purposes

Determinations to ascertain if two metallic or nonmetallic objects came from the same source or from each other usually require evaluations based on surface characteristics, microstructural characteristics, mechanical properties and composition.

(1) Surface Characteristics - macroscopic and microscopic features exhibited by the metal or material surface including

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 124

fractured areas, accidental marks or accidentally damaged areas, manufacturing defects, material defects, fabrication marks and fabrication finish. The fabrication features reveal part of the mechanical history of how a metal was formed; e.g., if it was cast, forged, hot-rolled, cold-rolled, extruded, drawn, swaged, milled, spun, pressed, etc.

(2) Microstructural Characteristics - the internal structural features of a metal as revealed by optical and electron microscopy. Structural features include the size and shape of grains; the size, shape and distribution of secondary phases and nonmetallic inclusions; and segregation and other heterogeneous conditions. The microstructure is related to the composition of the metal and to the thermal and mechanical histories of the metal, including post-fabrication exposures and/or deformations.

(3) Mechanical Properties - describes the response of a material to an applied force or load, e.g., strength, ductility, hardness.

(4) Composition - the chemical element make-up of the material including major alloying elements and trace element constituents. Because most commercial metals and alloys are nonhomogeneous materials and may have substantial elemental variations, small metal samples or particles may not be compositionally representative of the bulk metal.

EFFECTIVE: 07/25/97

13-14.2 Examinations for Information Purposes

Some of the kinds of information that can result from metallurgical examinations of materials in various conditions are listed below:

(1) Damaged metallic or nonmetallic items

(a) Cause of the failure or damage.

(b) The magnitude of the force or load which caused the failure.

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 125

(c) The possible means by which the force or load was transmitted to the item and the direction in which it was transmitted.

(2) Burned, heated or melted metal

(a) Temperature to which the metal was exposed.

(b) Nature and/or direction of the heat source which damaged the metal.

(c) Whether the item was involved in an electrical short-circuit situation.

(3) Rusted or corroded metal - length of time the metal had been subjected to the environment which caused the rust or corrosion. Requires that the investigator submit information concerning the environmental conditions.

(4) Cut or severed material

(a) Method by which the material was severed - sawing, shearing, milling, turning, electrical arcing, flame cutting (oxyacetylene torch or "burning bar"), etc.

(b) Temperatures and/or type of equipment required.

(c) Deleted

(5) Fragments

(a) Method by which the fragments were formed.

(b) If fragments had been formed by high velocity forces, may determine if an explosive had been detonated and the relative magnitude of the detonation velocity.

(c) Possible identification of the item which was the source of the fragments. In bombings, timing mechanisms can often be identified as to type, manufacturer and model; determinations are often possible as to the time displayed by the mechanism when the explosive detonated and as to the relative length of time the mechanism was functioning prior to the explosion.

(6) Watches, clocks and timers

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 126

(a) Condition responsible for causing the timing mechanism to stop or malfunction.

(b) Whether the time displayed by the mechanism represents AM or PM (calendar-type timing mechanisms only).

(7) Deleted

(8) Lamp bulbs

(a) Whether a broken lamp bulb was incandescent at the time the glass portion broke.

(b) Whether an unbroken lamp bulb was incandescent at the time it was subjected to impact forces such as those developed in vehicular collisions.

(9) Objects with questioned internal components: X-ray radiography can reveal the interior construction and the presence or absence of cavities or foreign material.

(10) Items with obliterated identification markings - Obliterated identification markings are often restorable, including markings obliterated by melting of the metal (welding, "puddling"). Obliterated markings can also be restored on materials other than metal. Because different metals and alloys often require specific methods for restoration of obliterated markings, the Laboratory should be contacted before any field processing for number restoration is attempted. (See MIOG, Part I, 26-2.8 (1); Part II, 10-3, 13-13.3.1.)

(11) Speedometers: Speed indicated at impact.

EFFECTIVE: 07/25/97

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 127

13-15 MATERIALS ANALYSIS EXAMINATIONS

(1) These examinations are made by the Chemistry Unit.
(See MIOG, Part II, 13-10.) These examinations entail the use of microscopic, microchemical and instrumental techniques such as Fourier transform infrared spectroscopy, X-ray diffraction, pyrolysis gas chromatography - mass spectrometry, scanning electron microscopy, differential thermal analysis, capillary electrophoresis, liquid and ion chromatography, etc., for both organic and inorganic analyses, identification and/or comparison of the compositions of paints, plastics (polymers), tape (electrical, masking, and duct tapes), glues, caulker/sealants, cosmetics, explosives and explosive residues.

(2) Mineralogy is part of the Trace Evidence Unit
(see MIOG, Part II, 13-11 for mineralogy examinations).

EFFECTIVE: 07/25/97

13-15.1 Paints, Cosmetics, Plastic Products, and Tapes

EFFECTIVE: 09/03/93

13-15.1.1 Automobile Paints

It is possible to establish the color, year and make of an automobile from a paint chip by use of the National Automotive Paint File which contains paint panels representing the original paint finish systems used on all makes of American cars, light trucks, vans, and most foreign cars. A very careful search of the accident or crime scene should be made to locate small chips because:

(1) Paint fragments are often found in the clothing of a hit-and-run victim during Laboratory examinations.

(2) Paints may be transferred from one car to another, from car to object, or from object to car during an accident or the commission of a crime.

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 128

(3) The paint particles may not be big enough to recognize/detect with the unaided eye so suspected transfer items should be submitted to the Laboratory for complete analysis. Also, thinly deposited smears of paint may vary in color and should not be eliminated during a field examination.

EFFECTIVE: 05/31/94

13-15.1.2 Nonautomobile Paints and Other Coatings

(1) Coatings of all types can be analyzed and compared. Paint on safes, vaults, window sills, door frames, furniture, bicycles, etc., may be transferred when forcible contact is made with another object. For example, a comparison can be made between the paint on an object and the paint on a tool to determine if there was contact with a particular painted surface. However, the manufacturer cannot be determined (other than original automotive paint finishes).

(2) Fine art authentication through complete chemical analyses of the coatings/materials utilized in the painting can be performed.

EFFECTIVE: 05/31/94

13-15.1.3 Cosmetics and Related Items

Known and questioned samples of cosmetics, such as lipstick, face powder, body lotions and lubricants, and various other make-up materials can be compared with each other but they normally cannot be associated with a specific source, manufacturer or distributor.

EFFECTIVE: 05/31/94

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 129

13-15.1.4 Plastics/Polymers

It is usually not possible to specifically identify the particular source, use, or manufacturer of plastic items from composition alone but comparisons such as the following can be made:

(1) Trim from automobiles, depending upon the uniqueness of the composition, is compared with plastic remaining on the victim or property struck in a hit-and-run.

(2) Plastics comprising insulation on wire used in bombings or other crimes are compared with known or suspected sources of insulated wire.

(3) Miscellaneous plastic material (including buttons) from crime scenes is compared with possible sources.

EFFECTIVE: 05/31/94

13-15.1.5 Tape

A positive identification may be made with the torn or cut piece of tape left at the scene of the crime or on a victim and a roll of suspect tape (similar to fabric examination).

(1) Associations of tapes left at the scene and from suspected sources are determined from physical and compositional characteristics.

(2) Deleted

(3) Trace Evidence Unit maintains a duct tape reference file.

EFFECTIVE: 07/25/97

13-15.1.6 Explosive Residues

See Part II, Section 13-6.7.1.

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 130

EFFECTIVE: 05/26/89

13-15.2 Fluorescent Powders and Other Marking Materials

EFFECTIVE: 09/03/93

13-15.2.1 Purpose

Marking materials are used to prepare an object, be it a decoy package, cash box, money, etc., in order that a detectable trace will be left on a person or the property of a person who handled the object.

EFFECTIVE: 05/26/89

13-15.2.2 Selection Factors

(1) The choice of material depends on factors inherent with each situation. These materials can be obtained as kits from commercial vendors.

(2) The material used can be a dry powder, liquid, or grease and be available in many visible and fluorescent colors.

(3) Fluorescent materials require a source of ultraviolet light to examine the subject's hands or clothing.

(4) Deleted

(5) Deleted

EFFECTIVE: 09/24/93

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 131

| 13-15.2.3 | Deleted |

EFFECTIVE: 09/03/93

| 13-15.2.4 | Deleted |

EFFECTIVE: 09/03/93

| 13-15.2.5 | Deleted |

EFFECTIVE: 09/03/93

13-15.2.6 Fluorescent Materials

- subject.
- (1) Have the advantage of not being visible to the
 - (2) Have the capability of being subsequently identified as the same powder used, by analysis of deposits on clothing, etc.
 - (3) Have the disadvantage of requiring a source of ultraviolet light (see item (7) below).
 - (4) Phosphorescent materials are different from fluorescent powders and must not be used since these may be detected by the subject even without an ultraviolet source.
 - (5) Must be applied in a finely ground or powdered form.
 - (6) Choice of form depends on object to be marked, for

example:

Sensitive

Manual of Investigative Operations and Guidelines
Part II.

PAGE 13 - 132

(a) Contact areas of tools can be coated with a grease, such as vaseline, mixed with a fluorescent powder without creating suspicion. Richer deposits are transferred when grease film is used.

(b) Normally dry surfaces, such as gloves, money, doorknobs, steering wheels, etc., would arouse suspicion if coated with a grease. After coating an appropriate surface with grease, the remainder of object and/or container may be dusted with dry powder.

(c) Time, amount of light, and other factors may limit application to dusting since the dusting procedure is rapid and does not require meticulous attention.

(d) Liquid fluorescent materials normally used as a writing medium. Care must be taken to prevent liquid marks or discolorations on paper or surface treated.

(7) Availability of fluorescent materials: Questions on availability and appropriateness of chemicals to particular problems can be resolved by contacting the Trace Evidence Unit of the Laboratory, extension [REDACTED] or [REDACTED] b2

(8) Procedures for application:

(a) In applying grease, use bare fingers or an appropriate applicator and rub it over the surfaces of the items to be marked so as to leave a thin film. Avoid large "globs" of grease. The common fluorescent materials available from the Laboratory are not dangerous or toxic substances and will not be readily absorbed through the skin. However, normal precautions should be made to avoid direct inhalation or contact with the eyes and mouth.

(b) In applying powder form, numerous methods are commonly used, such as shaking powder over items, dusting with a powder puff or pad of cheesecloth, or brushing over the surfaces in a manner similar to that used to dust with fingerprint powder.

(c) Liquids can be applied with a clean pen, small paint brush, or spray-type dispenser.

CARE SHOULD BE TAKEN SO THAT THE FLUORESCENT SOURCE IS NOT DIRECTED AT THE EYES, SINCE THE ULTRAVIOLET RAYS FROM THE LIGHT CAN CAUSE DAMAGE TO THE EYES.

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 133

EFFECTIVE: 07/25/97

13-15.2.7 On-Site Laboratory Assistance to Field

Any requests for on-site assistance by Trace Evidence Unit personnel in a high-priority crime scene situation must be made by direct communication between the SAC and the Assistant Director, Laboratory Division. Such requests should only be made when the available services of the field crime scene search team will not fully meet the needs of the situation. This on-site support would include, but is not limited to, detection (i.e., explosives, drugs or drug by-products), recovery, preservation and delivery to the Laboratory of trace evidentiary materials considered to be of probative value in the investigation.

EFFECTIVE: 07/25/97

13-16 | SUPPORT SERVICES AND EXAMINATIONS IN BOMBING AND
EXPLOSIVE MATTERS |

EFFECTIVE: 09/24/93

| 13-16.1 | Deleted |

EFFECTIVE: 09/24/93

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 134

13-16.2 Handling, Transportation and Storage of Explosives|or
Suspected Explosives (See MAOP, Part II, 2-4.4.11.)|

(1) Explosives|or suspected explosives|should only be handled by trained Laboratory Division personnel or certified Special Agent bomb technicians. The handling, transportation and storage of explosives should always be carried out in a safe, reasonable and prudent manner consistent with applicable laws and regulations.

(2) Each field division, through liaison contacts with local law enforcement agencies and U.S. military commands, should establish suitable and proper storage for explosives seized in the course of Bureau investigations or for use in training matters dealing with explosives. In the event suitable and proper explosives storage arrangements cannot be achieved to meet a field division's requirements, the purchase of a portable magazine(s) may be required.

(3) Any problems or questions regarding the handling, transportation and storage of explosives should be immediately resolved through contact with the Laboratory|Division's Materials and Devices Unit.|

EFFECTIVE: 04/07/97

13-16.3 Render Safe Assistance to the FBI

All offices are to have established liaison with|public safety bomb squads and|United States Military Explosive Ordnance Disposal (EOD) Units|in order that assistance can be promptly obtained if explosives|and/or bombs are encountered in connection with official investigations. -|The public safety bomb squad response is an integral part of the FBI Counterterrorism and narcoterrorism programs, and as such, liaison with these squads is an extremely important responsibility which|should be handled by the Special Agent field bomb technician.

(1) The United States Army has EOD Units stationed throughout the continental United States plus Alaska and Hawaii. These Units have provided support to the Bureau in the past and have personnel qualified to handle explosives and bombs. Due to emergency conditions, requests for assistance from Army EOD Units will usually be oral. Such oral requests are to be confirmed by letter addressed

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 135

to the Commanding Officer of the EOD Unit involved.

(2) The Army does not have an EOD Unit in Puerto Rico. Therefore, the San Juan Office should have established liaison with an appropriate United States Navy facility.

EFFECTIVE: 02/12/92

13-16.4 On-Site Laboratory Assistance to Field

Any requests for on-site assistance by Laboratory personnel in an explosives-related situation must be made by direct communication between the SAC and the Assistant Director in Charge, Laboratory Division. Such requests should only be made when the available services of the field division bomb technician will not fully meet the needs of the situation. This on-site support includes, but is not limited to, forensic investigation at major bombing crime scenes, participating in raids or searches wherein explosives may be encountered and technical support for principal bomb squad.

EFFECTIVE: 02/12/92

13-16.5 [REDACTED] Technique

The Materials and Devices Unit, Laboratory Division, has the capability of [REDACTED] This technique, called the [REDACTED] is closely controlled by the Laboratory and may only be initiated by explosive specialists from the Materials and Devices Unit. ba/b7E

(1) The Laboratory maintains a collection of [REDACTED] from which to draw upon when this technique is deemed appropriate. Additionally, items not in stock may be obtained from manufacturers where appropriate lead time is allowed. Items in this collection include: [REDACTED]

(2) [REDACTED]

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 136

b2/b7E

[REDACTED]

(3) For this technique to be implemented, approval must be obtained from the applicable Criminal Investigative Division section supervising the parent case. Coordination will then be made with the Laboratory regarding the specifics of the [REDACTED] proposal. Under no circumstances should any FBI personnel attempt to conduct [REDACTED] without the appropriate approval and coordination with the Laboratory Materials and Devices Unit.

EFFECTIVE: 04/07/97

13-16.6 Shipping Explosives, Hoax Bombs, and Bomb Components to the Laboratory for Examination (See MIOG, Part II, 13-6.7 (44).)

(1) Explosives are currently classified as hazardous material. Therefore, special packaging is required and the amount which can be sent in each shipment is regulated.

(2) The Materials and Devices Unit is to be contacted for shipping and packaging instructions EACH AND EVERY TIME an explosive, hoax bomb, or bomb component is to be shipped to the Laboratory Division for examination. The shipping instructions furnished must be strictly adhered to because the improper packaging and shipment of an explosive is a serious matter affecting safety, and violations of shipping regulations will not be tolerated.

(3) Prior to mailing/shipping items between Bureau offices which, when x-rayed, might appear suspicious, an immediate teletype must be sent or a telephone call made to the recipient. The teletype or telephone call should identify the shipping method (United States Postal Service Registered, FedEx, etc.) identifying/tracking number, office of origin, description of contents, date it was mailed/shipped, and any other information which may be beneficial to the recipient.

(a) Upon receipt of the above-mentioned information, the recipient must complete an FD-861 and post it on or near the x-ray machine in a conspicuous manner. It is the responsibility of each office to designate an appropriate area for the posting of such

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 137

information and advise all employees responsible for x-raying incoming mail and related material of the designated area. Also, appropriate security must be afforded to the Mail/Package Alert Forms to prevent possible compromise. That is, the posting of such information in unsecured FBI space (i.e., loading dock, reception area, etc.) is strictly prohibited.

(b) The form must remain posted at all times until the item in question is received. Upon receipt of the questionable item, the FD-861 should be removed from the x-ray machine or designated area, and the bottom portion of the form completed (initials of the employee who identified the package and date received). The completed form should be retained for 90 days. Thereafter, the form should be disposed in official receptacles.

(c) The same procedures apply for mailing/shipping to the J. Edgar Hoover (JEH) FBI Building. An immediate teletype must be sent to FBIHQ. Attention: Mail Services Unit (MSU), Room 1B006, or call [REDACTED] (8 a.m. - 4:30 p.m., EST) or [REDACTED] (24 hours a day, seven days a week). The MSU will be responsible for ensuring appropriate JEH FBI personnel are advised of the questionable item. b2

(d) When mailing/shipping possible suspicious-looking items OUTSIDE the Bureau, offices should make a courtesy telephone call to the recipient, providing the same information as described above (i.e., shipping method, identifying/tracking number, date sent, description of contents, etc.). (See MIOG, Part I, 91-8 (11).)

EFFECTIVE: 06/04/97

13-16.6.1 Examination and Tests of Explosives and Explosive Devices

(1) The Laboratory|Materials and Devices Unit|will conduct all forensic explosive testing and examination of explosive devices at the Quantico explosives|ranges, or other ranges deemed appropriate,|in support of FBI investigations and prosecutions.

(2) Such examinations or tests which must be conducted in the field due to exigent circumstances must have the approval of the Laboratory Division. Special Agents of the|Materials and Devices Unit|will be assigned as appropriate to ensure that all forensic

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 138

considerations and safety requirements are in accordance with applicable laws and regulations.

(3) This requirement extends to the handling, shipping and storage of explosive materials and verification testing of live explosives or devices to be carried out in the field where investigative matters are involved.

EFFECTIVE: 04/07/97

13-16.7 Examinations of Bombs and Explosives

(1) Bombing evidence is examined to identify the components and fabrication techniques utilized in the bomb, to reconstruct the bomb, find clues that will assist in the identification of the bomb builder and to determine if the bomb is like previously examined bombs. The Materials and Devices Unit is primarily responsible for the examination of all explosive devices and hoax bomb devices. All bombing evidence should be shipped to the Laboratory to the attention of the Evidence Control Center and the Materials and Devices Unit. Forensic bombing examinations are subdivided into five categories: (1) the main charge explosive, (2) the fuzing system (initiation system), (3) function tests, (4) destructive capability evaluations and (5) intercomparison examinations.

(2) The Materials and Devices Unit must approve the proposed use of explosives by [REDACTED] in conjunction with the Criminal Investigative Division. The Materials and Devices Unit will provide guidance and instruction as necessary on the feasibility and safe handling of [REDACTED]. Under no circumstances should [REDACTED] without prior approval of the Materials and Devices Unit.

b2/b7E

(3) The Materials and Devices Unit must approve all [REDACTED]

in FBI investigations.

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 139

EFFECTIVE: 04/07/97

13-16.7.1 Explosive Examinations (See MIOG, Part II, 13-15.1.6.)

The Chemistry Unit conducts instrumental examinations of explosive materials from unexploded bombs and residue from exploded bombs. These examinations can yield the following information:

- (1) Explosive residue examinations often identify the type of explosive(s) used in the construction of the bomb, i.e., dynamite, slurry, military, gun powder or homemade.
- (2) Analysis of unexploded materials can very likely identify the manufacturer of the explosive, i.e., Dupont, Atlas, Hercules.
- (3) Analysis of unexploded materials from bombs can also provide detailed compositional information about the explosive that can permit comparisons with explosives seized from caches and suspects.
- (4) It is important to know that most residues of an explosive are water soluble, and, therefore, these residues must be protected from moisture. Also, other residues evaporate quickly necessitating the immediate sealing of collected debris in airtight metal cans. Also recognize that modern chemical analytical techniques are capable of detecting extremely minute amounts of explosives. These capabilities require that personnel handling bombing evidence be absolutely sure they are not contaminating evidence with residues on their hands or clothing that they have picked up elsewhere.
- (5) DO NOT USE A HEAT-SEAL CONTAINER, SCREW-ON LID OR OTHER HEAT-, FRICTION- OR STATIC ELECTRICITY- PRODUCING CONTAINER TO HANDLE, SHIP, TRANSPORT OR STORE LIVE EXPLOSIVES OR SUSPECT EXPLOSIVE MATERIALS. THIS DOES NOT INCLUDE SHIPPING OF EXPLOSIVE RESIDUE FOLLOWING THE COLLECTION OF DEBRIS FOLLOWING AN EXPLOSION.

EFFECTIVE: 07/25/97

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 140

13-16.7.2 Fuzing System Examinations

The fuzing system of a bomb is the mechanism that, when activated, makes the bomb explode. A fuzing system can be something as simple as a burning fuse, or as complicated as a radio control mechanism. Examinations of a fuzing system can provide valuable investigative information as well as forensic information.

(1)

b2/b7E

(2)

(3)

EFFECTIVE: 02/12/92

13-16.7.3 Function Tests of Bomb Fuzing Systems

Routine examinations of unexploded fuzing systems include evaluations to determine if the system could function the bomb if it were activated. Statements concerning these tests will be included in the Laboratory report. If requested, bomb fuzing system plans can also be evaluated to determine if they are workable.

EFFECTIVE: 02/12/92

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 141

13-16.7.4 Destructive Capability Evaluations

Routine examination of unexploded bombs includes an evaluation of the bomb's destructive capability. Statements concerning these evaluations are set forth in the Laboratory report. If important to the investigative effort, on-site evaluation of a bomb's blast effects can be made and expert testimony rendered about the size and type of explosive utilized.

EFFECTIVE: 02/12/92

13-16.7.5 Intercomparison Examinations

Intercomparison examinations of bombs, bomb debris and bombing related evidence are conducted to determine if the same person(s), plans and/or source of materials are involved in multiple incidents. The case Agent should request these types of examinations when investigation indicates a common link between bombing incidents. It should be noted that in certain situations the suspect and bombing incident can be positively linked through intercomparison examinations

ba/67E

EFFECTIVE: 02/12/92

13-16.8 Explosive Reference Files

The Materials and Devices Unit maintains extensive reference files on commercial and military explosives and improvised explosive devices or homemade bombs. These files contain technical data plus known standards of explosive items and bomb components. Information in these files is routinely compared with bombing evidence under examination and any associations will be reported.

EFFECTIVE: 04/07/97

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 142

13-16.9 Bomb Data Center Program

The additional mission of the FBI Bomb Data Center is to provide state of the art training to and develop technology for public safety bomb disposal technicians, provide operational support to law enforcement agencies during special events and/or crisis management situations and to gather and disseminate information pertaining to bombing matters.

EFFECTIVE: 04/07/97

13-16.9.1 Technical Publications

The FBI Bomb Data Center is responsible for the collection, collation and dissemination of up-to-date statistical and technical information concerning improvised explosive devices, render safe procedures, explosive research and technical equipment used by public safety bomb technicians.

The principal publications of the Bomb Data Center are disseminated through three distinct mailing lists:

(1) PUBLICATIONS CONTAINING UNRESTRICTED INFORMATION - These publications provide information of a general nature. They set forth the results of tests conducted on bomb handling and detection equipment and other data of general interest. The dissemination of these publications is not restricted to law enforcement agencies. Public utilities such as electric power, natural gas, water or similar companies which carry out functions relating to welfare and security of a community, and corporate security offices may be placed on the mailing list to receive unrestricted information. These publications are mailed to the heads of participating organizations, or they may be addressed to the head of any subordinate unit designated by the department head, e.g., commander, bomb squad; lieutenant, burglary squad, and require no special security precautions. The publication is known as the GENERAL INFORMATION BULLETIN (GIB).

(2) PUBLICATIONS CONTAINING RESTRICTED INFORMATION - These publications, available only to public safety agencies and certain military units, provide information of sensitive nature and are labeled RESTRICTED INFORMATION. The present information about the design and functioning of specific bombs which have actually been

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 143

constructed, current and vital information concerning new or potential bomb-type hazards, methods of coping with certain bombs, and other information of specific interest to the bomb incident investigator. Because the information is considered restricted, the distribution of these bulletins is limited to those participants who have a need to know. They are mailed to the heads of participating organizations or they may also be addressed to the head of any subordinate unit designated by the department head, e.g., commander, bomb squad; lieutenant, burglary squad, for dissemination only to those persons who have a need for the information contained therein. They must not be made available to unauthorized persons. All participants who receive these publications also receive those containing unrestricted information. Recipients of restricted material must agree to safeguard the information. This publication is known as the INVESTIGATORS' BULLETIN (IB).

(3) SPECIAL TECHNICIAN'S BULLETIN (STB) - These publications, containing technical information intended only for the trained bomb technician, are also labeled RESTRICTED INFORMATION. They detail information regarding disarming procedures which have been employed against specific bombs, new or novel commercial items which may ultimately be encountered in improvised explosive devices, and other technical data which will be of specific interest to bomb technicians. Any attempt by an untrained person to apply the techniques or procedures contained in the STB could result in injury or death. Because of this, the STB is not mailed to the agency head but to the bomb squad commander for dissemination to qualified active members of the bomb squad. After receipt, it is the specific responsibility of the individual bomb technician to assure that these publications are not made available to unauthorized individuals. To obtain the STB, each bomb technician must be certified by his/her chief or supervisor in accordance with the following instructions:

(a) For Hazardous Devices School Graduates - The name and rank or title of the technician, the name and mailing address of the department or agency to which he/she belongs, and the date that he/she is presently employed as a bomb technician.

(b) Others - Active duty military EOD personnel will receive STB's through their parent commands.

(4) In addition to the established mailing list program, the Bomb Data Center can supply FBI offices, public safety agencies and corporate security personnel with bomb threat cards, physical security manuals and handout material on the bomb threat challenge.

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 144

(5) The Bomb Data Center compiles and publishes quarterly statistical summaries on bombing incidents throughout the United States. Data utilized in these summaries is reported to the Bureau by Form FD-436. Use of this form is not restricted to incidents bearing the 174 classification (Explosives and Incendiary Devices; Bomb Threats). The statistical integrity of the bomb incident summaries requires that all explosive incidents in the following categories be reported: (See Correspondence Guide-Field, 3-5.2.)

(a) ACTUAL use of an explosive or incendiary device

(b) ATTEMPTED use of an explosive or incendiary device

(c) RECOVERY of an actual or hoax device

EFFECTIVE: 04/07/97

13-16.9.2 [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 145

67E
EFFECTIVE: 04/07/97

13-16.9.3 Technical Research

The FBI Bomb Data Center manages research programs involving remote-render safe technology, explosive breaching, incendiary devices and firing systems of explosive and incendiary devices. Much of this research is conducted in conjunction with other federal agencies. Completed research reports are distributed to tactical units within the FBI as well as other interested public safety agencies.

EFFECTIVE: 04/07/97

13-16.9.4 FBI Hazardous Devices School (FBI HDS)

(1) Basic training of public safety bomb technicians in the United States is provided at the FBI Hazardous Devices School (FBI HDS), Redstone Arsenal, Huntsville, Alabama. The FBI has funded and administered FBI HDS through the Bomb Data Center since 1981 when Congress mandated that the FBI would assume responsibility for the training of public safety bomb technicians. An annual Interagency Support Agreement with the U.S. Army provides military support at Redstone Arsenal. The U.S. Army provides a staff comprised of full time military and civilian personnel.

(2) The basic course is designed to train state and local public safety officials as bomb technicians. The basic course combines classroom and range instruction in explosives technology, electronic circuitry and components of explosive devices, nonelectric components and priming, use of special equipment for the detection and handling of explosive devices, and render safe equipment and techniques. The basic course is given eight times per year with 18 students enrolled in each course.

(3) HDS basic course applicants must be committed to five years of continuous service on an active bomb squad. Travel, lodging,

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 146

and other expenses at the basic course are the responsibility of the trainee's agency.

(4) The one-week refresher course reviews basic principles and explores current developments in bomb disposal. The bomb technicians are placed in a variety of simulations which challenge their technical ability. HDS conducts twelve refresher courses each year with sixteen bomb technicians enrolled in each. The HDS refresher course is open to all basic course graduates. Reimbursement for travel, lodging, and subsistence is available from the FBI.

(5) ATTENDANCE PROCEDURE:

Any full-time, sworn employee of a local, state or federal public safety agency with a render safe responsibility may be selected for the HDS attendance. Priority selection status is given to local and state personnel with full-time render safe responsibilities. Departments which sponsor students for the basic course must certify that the required safety equipment (full-coverage bomb suit, portable X-ray system, disrupter, demolition kit, and quality hand tools) is in the agency's inventory. Applications must be reviewed by the field office Special Agent bomb technician working with the Police Training Coordinator.

(a) All applicants must: (See MIOG, Part II, 13-16.9.7.)

1. Be volunteers;
2. Be full-time, sworn, salaried officers assigned to bona fide public safety agencies;
3. Not be color blind;
4. Have vision in each eye which is not worse than 20/200 uncorrected and correctable to 20/20;
5. Not have a hearing loss in either ear which is greater than 60 decibels; and
6. Be in good health with no permanent or limiting disabilities.
7. Must fall within the Bureau weight chart (National Academy Standards) or have no more than 22 percent body fat.

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 147

(b) All applicants should:

1. Be committed to bomb technician work for a minimum of five years after graduation from HDS;
2. Have a minimum of five years' experience with their respective agencies prior to the date of the application;
3. Upon graduation, be assigned to duties normally associated with those of a bomb technician; and
4. Upon graduation, attend the one-week refresher course every 36 months.

(c) Requests for attendance must be directed to the local FBI field division, Attention: Police Training Coordinator. The requesting agency will receive:

Form FD-731 Information Form
Form FD-732 Waiver Form
SF-88 Medical Examination Form
Form 2-205 Attachment to Medical Form
FD-406 Authority to Release Information
| Performance Standard Test Certification
| (Refresher candidates) |

(d) The FBI field division submitting the application is responsible for the following investigative steps:

1. Office indices check
2. Birth date verification
3. Credit and arrest check for five-year period preceding date of application. Authority to Release Information (FD-406) must be obtained from the nominee at onset of the investigation. Credit checks will be conducted by contractor personnel at FBIHQ.

Any information developed which reflects unfavorably upon character or reputation of nominee must be completely resolved. SAC should make his/her recommendation based on results of investigation. Selection will be based on availability of space, number of technicians already trained in that area, and specific need of department.

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 148

EFFECTIVE: 04/07/97

13-16.9.5 Bomb Technician's Seminar

Regional seminars are conducted by Bomb Data Center staff and field Special Agent bomb technicians on the construction and utilization of improvised explosive devices, techniques for remote neutralization, discussions of research and development and a review of new technical equipment. This seminar is only available to trained bomb technicians who are graduates of the FBI Hazardous Devices School.

EFFECTIVE: 04/07/97

13-16.9.6 Post-Blast Investigator Seminar

Regional seminars are conducted by Bomb Data Center staff on explosives recognition, investigative techniques and bomb crime scene procedures. This seminar is available to law enforcement personnel with investigative responsibilities in bombing cases.

EFFECTIVE: 04/07/97

13-16.9.7 Special Agent Bomb Technician Program

The Special Agent bomb technician program is voluntary and requires attendance at a four-week explosives course at the Hazardous Devices School, Redstone Arsenal. The purpose of this training, initiated more than fifteen years ago, is to provide specialized explosive training to Special Agents to improve the technical proficiency in bomb investigations and to establish a liaison link with public safety bomb squads. When the FBI assumed administration of the Hazardous Devices School in 1981, the cadre of Special Agent bomb technicians became an integral part of the Bureau's program of bomb technician and bomb investigator training.

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 149

(1) Special Agents nominated for this training shall meet the following criteria:

(a) Be an experienced investigator with a minimum of two years in the field.

(b) Have an overall Performance Appraisal Report rating of "Superior."

(c) Be in good physical condition, meeting the minimum standards detailed in section 13-16.9.4 (5) (a).

(d) Have a minimum of five years of service remaining prior to retirement.

(e) Successfully complete the recommended elements of the "Performance Standard Test."

(f) Be a volunteer, recognizing the inherent dangers of working with live explosives.

(g) Be recommended for the program by the SAC, to include observations regarding the candidate with the respect to:

1. oral/written communication skills.

2. ability to function well under stressful conditions.

3. availability for travel, both overseas and domestic, to assist in Bureau special assignments; major incidents, and regional police training.

4. demonstrated ability to work in a team environment. (See (i).)

(h) It is recommended that candidates for the program serve as members of the field division's Evidence Response Team; become certified police instructors; and have no other significant collateral duties.

(i) Following successful completion of the HDS Basic Course, Special Agent bomb technicians will serve an 18-month probationary period. Probationary Special Agent bomb technicians will be evaluated by Materials and Devices Unit personnel in the areas outlined in 13-16.9.7 (1) (g) 1. through 4. and performance of

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 150

the duties outlined in 13-16.9.7 (2) (a) ADMINISTRATIVE, (b) LIAISON, (c) TACTICAL, and (d) TRAINING. Additional evaluation will take place during the annual recertification seminar and through participation at a Regional Bomb Technician Seminar.

(2) Special Agent bomb technician, in addition to other duties as a field investigator, has the following responsibilities:

(a) ADMINISTRATIVE

1. Provides information and advice to the SAC in all matters involving the use, possession or transportation of explosives.

2. Coordinates the recovery of explosive evidence in FBI investigative matters as well as its safe shipment to the FBI Laboratory.

3. Compiles and reports to the Bomb Data Center information involving explosive devices encountered by public safety bomb squads and military EOD units.

4. Expeditiously reports to the Laboratory Division by telephone extraordinary bomb related events.

5. Assists the field office management in the development of emergency planning for a bombing occurrence.

6. Assists the office crime scene coordinator as necessary regarding bombing crime scene examinations and evidence collection.

7. Obtains and controls proper bunker space for the storage of explosive evidence, training devices, and tactical items.

8. Advises the Bomb Data Center of upcoming special events where specialized equipment may be required.

(b) LIAISON

1. Establishes and maintains communication with local military and civilian bomb disposal units.

2. Establishes and maintains communication with professional organizations (i.e., International Association of Bomb

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 151

Technicians and Investigators - IABTI) in their area, to include membership in and attendance at organizational functions.

3. Establishes and maintains communication with other federal agencies to ensure information is obtained regarding their encounters with explosives.

4. Stimulates participation in the Bomb Data Center publication program by encouraging innovative research or recording of unusual incidents by local bomb squads.

(c) TACTICAL

1. Acts as an information link between field office management and its tactical units in situations involving explosives.

2. Assists in assessments of potential explosive and/or booby trap devices encountered during investigative, arrest and search operations.

3. Is available to tactical units for "on scene" technical assistance and direct liaison with supporting bomb squad personnel.

(d) TRAINING

1. Plans and conducts periodic training for FBI personnel as office needs dictate. Such training may include bomb threat assessment, search techniques, explosives recognition or other similar courses.

2. Assists the Materials and Devices Unit in its national training program conducted regionally throughout the year by participating in at least one regional school.

3. Assists the field office police training coordinator with local requests for bomb-related instruction.

4. In addition to regional schools MUST participate in the Materials and Device Unit sponsored annual recertification program to assess technical abilities and safe explosive handling practices.

EXPLOSIVE BREACHING TECHNIQUE IS NOT AUTHORIZED FOR ANY
FBI OR POLICE TRAINING PROGRAM

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 152

The Laboratory Division has trained personnel to provide additional support to the SAC in situations in which explosives may be anticipated. BOMBING TECHNICIANS OF THE MATERIALS AND DEVICES UNIT are available to provide advice on safety perimeters at a bomb location, remote handling procedures for the render safe of an improvised explosive device, effect liaison with the faculty of HDS, direct access to the worldwide system of bomb data centers and provide direct liaison with public safety bomb squads. EXPLOSIVES SPECIALISTS OF THE MATERIALS AND DEVICES UNIT will provide assistance in the processing of bombing crime scenes, searches of bomb factories, [REDACTED] support and necessary forensic assistance. b2/b7E

EFFECTIVE: 04/07/97

13-16.9.8 Render Safe Equipment

(1) The primary goal of the bomb technician training at the Hazardous Devices School (HDS) is to save lives. Bomb technicians are taught remote render safe techniques so as to minimize the dangers inherent in bomb disposal activity. NO "HANDS ON" RENDER SAFE PROCEDURE IS RECOMMENDED UNLESS A LIFE IS IN IMMINENT DANGER AND THERE IS NO ALTERNATIVE. In order to support this philosophy, the FBI has included a wide range of high technology equipment in its training program. This equipment is utilized to illustrate the variety of remote techniques, to stimulate the acquisition of similar equipment by bomb squads and to provide an assessment of the capabilities of the equipment.

(2) The Laboratory Division possesses two self-contained bomb disposal vehicles. The vehicles contain a state-of-the-art bomb containment sphere which is designed to absorb the deadly pressure and fragmentation of an explosive device. Each truck also contains a bomb disposal robot and a bomb protection suit. When combined with other render safe equipment on the truck, the response package provides a variety of low-risk alternatives for a render safe operation. All of the equipment is designed for use during the critical time between detection of the bomb and detonation. The technology applies to initial assessment of the improvised explosive device, remote removal or on-site disruption. This equipment is available to augment public safety bomb squad or military EOD equipment at special events.

(3) All SA bomb technicians are trained in the use of

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 153

general bomb disposal equipment, such as x-ray machines and
| disrupters. | Bomb Data Center | and HDS personnel also train on the use
of more technical bomb disposal equipment.

EFFECTIVE: 04/07/97

| 13-16.9.9 | Deleted |

EFFECTIVE: 04/07/97

13-16.9.10 Requests for Assistance

(1) All direct operational support performed by the
| Materials and Devices Unit | must be in response to requests made by the
SAC and coordinated with the Criminal Investigative Division.

(2) Laboratory Division personnel and equipment as well
as field SA bomb technicians can provide assistance in the following
situations wherein the use of explosives might be anticipated:

(a) Major Case - When situation involves FBI or Task
Force jurisdiction, raid or arrest planning should include the
availability of the local public safety bomb squad or military EOD
units (Note Posse Comitatus restrictions on military seizure or
processing of evidence). If other agency support is not feasible, SAC
may request FBIHQ assistance.

(b) Special Event/Major Case - Local or state law
enforcement is usually the lead agency in physical security matters
with FBI jurisdiction aligned with terrorism possibilities. Public
safety bomb squad may request priority training assistance at HDS or
in a regional seminar. Technical support for the principal bomb squad
may be requested through the local SAC and FBIHQ.

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 154

EFFECTIVE: 04/07/97

13-17 DOCUMENT EXAMINATION (See MIOG, Part I, 7-14.9 (1) and NFIPM, Part 1, 7-6.1.)

Document examination consists for the most part of a side-by-side comparison of handwriting, typewriting, and other written and printed items to establish origin or authenticity. In addition to submitting documents for document examinations, consideration should always be given to submitting them for latent fingerprint examinations (see Part II, Section 15 of this manual). Latent fingerprint examinations are conducted, if requested, after the original document has been photographed and the requested document examinations have been conducted.

EFFECTIVE: 07/25/97

13-17.1 Conclusions

Conclusions are positive and reliable when the examinations are conducted by competent experts. (Note: Age, sex, character, etc., cannot be determined in handwriting. Pseudoexperts in this field, "graphologists" or "graphoanalysts," purport to have this ability, but have no scientific validity.)

EFFECTIVE: 07/25/97

13-17.1.1 Identification

This conclusion is a definitive conclusion stating to the exclusion of all other sources.

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 155

EFFECTIVE: 07/25/97

||13-17.1.2| "No Conclusion" Examinations

In some document examinations, a "no conclusion" is reached as opposed to an "identification" or examination conclusion. Some of the reasons for a "no conclusion" are:

(1) Limited questioned material

(2) Inadequate known material

(3) Lack of contemporaneous standards (long interval of time exists between the preparation of the questioned and known material)

(4) |Distortion/disguise| (definite conclusions often impossible)

(5) Lack of sufficiently identifying characteristics (although ample quantities of both questioned and known samples are available) |and/or|

| (6) Elimination of a suspect source. |

EFFECTIVE: 07/25/97

13-17.2 Documentary Evidence

All efforts must be made to maintain and preserve documentary evidence in the same condition as it was received. This evidence must not be folded, torn, tampered with, marked or touched unnecessarily, stamped, soiled, subjected to indented writing, mutilated, etc. Each item of evidence should be placed in a separate envelope/container. Photocopies should be placed in paper rather than plastic envelopes as photocopies often stick to plastic mutilating the document.

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 156

EFFECTIVE: 07/25/97

13-17.2.1 Marking for Identification

| Evidence will be marked according to FBI Laboratory
policy. |

EFFECTIVE: 07/25/97

13-17.2.2 Original vs. Photocopy

| The original evidence itself rather than a photocopy
(copy made with a photocopier machine) should be submitted because
many examinations can be conducted only on the original. Also, the
original is utilized by the examiner to prepare court exhibits.
| Limited examinations, however, can be made using good quality
photographs of the original evidence. A photocopy is normally
satisfactory for file searches. In no case should the inability to
forward the original evidence constitute a valid reason for not
requesting an examination.

EFFECTIVE: 07/25/97

| 13-17.2.3 Obtaining Known Handwriting Samples (See MIOG, Part I,
87-5.2, 91-17.1.5; Part II, 13-6.7 (44).)

The following guidelines are to be used to obtain known
handwriting and/or hand printing samples from a person (writer).

| (1) Reproduce the original conditions as nearly as
possible, the same text, size of paper, size of writing, space
available for the writing, type of writing instrument, etc.
| Should always try to duplicate. Obtain the full text of the
questioned writing in word-for-word order at least once, if possible.
Signatures and less extensive writing should be prepared several
times, each time on a different piece of paper. In hand printing
cases, both upper case (capital) and lower case (small) samples

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 157

| should be obtained. |

(2) Obtain samples from dictation until it is believed normal writing has been produced (the number of samples necessary cannot be determined in advance).

(3) Do not allow the writer to see either the original document in question or a photograph thereof prior to or during the taking of the samples.

(4) Remove each sample from the sight of the writer as soon as it is completed.

(5) Do not give instructions in spelling, punctuation or arrangement.

(6) | Deleted |

| (7) | In forgery cases the Laboratory should also be furnished with genuine signatures of the person whose name is | allegedly | forged.

| (8) | Obtain samples with both the right and left hands.

| (9) | Obtain samples written rapidly, slowly, and at varied slants.

| (10) | Obtain samples of supplementary writings such as sketches, drawings, manner of addressing an envelope, etc.

| (11) | Writer should initial and date each page.

| (12) | Witness each sample with date and initials | (and | name).

| (13) | Deleted

| (14) | If readily available, samples of undictated writing should be obtained, such as application for employment, social or business correspondence, school papers, | canceled checks, | etc.

EFFECTIVE: 07/25/97

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 158

13-17.2.4 Obtaining Known Typewriting Samples (See MIOG, Part II,
13-6.7(64))

The following guidelines are to be used to obtain known typewriting samples.

(1) | If the typewriter is equipped with a carbon film ("one-time") ribbon, remove the ribbon prior to taking exemplars and submit it to the Laboratory whenever available. |

(2) | Obtain a full word-for-word text of the message in question using as nearly as possible the same degree of touch as used in the questioned text.

(3) | Obtain | at least two | samples of the complete keyboard (all letters, numerals and | symbols both upper and lower case). |

(4) | Obtain pertinent identifying data regarding the typewriter (make, model, serial number, etc.) and type this data as well as information such as the date sample was obtained, name of person taking the sample, where the typewriter was located, etc., on the sample.

(5) | Obtain data, if available, regarding when the machine was last serviced or repaired.

(6) | Properly witness each sample (initial and date on reverse side).

(7) | If the typewriter uses a cloth ribbon also obtain a stencil sample as follows:

(a) Physically remove the cloth ribbon from the typewriter or mechanically move it by placing the ribbon mechanism in the stencil position

(b) Place a piece of carbon paper over a piece of ordinary paper and insert them both in the typewriter

(c) Begin typing and allow the faces of the type to strike the carbon paper directly, and

(d) Submit the stencil sample, which is the typed text on the ordinary paper, to the Laboratory. (A stencil sample gives very clear impressions of the typefaces.)

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 159

(8) If the typewriter contains no ribbon and one is not readily available, obtain a stencil sample by following steps (b) through (d) above.

EFFECTIVE: 07/25/97

13-17.2.5 Obtaining Known Photocopy Samples

The following guidelines are to be used when obtaining known samples from photocopy machines.

(1) Obtain at least 10 samples with no document on the glass plate and the cover down.

(2) Obtain at least 10 samples with no document on the glass plate and the cover up.

(3) Obtain at least 10 samples with a document on the glass plate and the cover down.

(4) Identify each sample as to make, model, and conditions under which sample was made.

(5) On the transmitting communication to the Laboratory, if possible, list any of the following information that can be obtained from the known photocopy machine:

(a) Toner - Locate toner supplies and record toner components, manufacturer, and descriptive information

(b) Paper - Sheet or Roll fed

(c) Options

1. Color - Determine if the machine has optional color capabilities and what colors are available

2. Editor - mask and trim, or editor board

3. Reduction, enlargement, and zoom

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 160

EFFECTIVE: 05/11/87

13-17.3 Requesting Examinations

When a document examination is desired, follow the instructions in paragraph 13-3.1 (Requests for Examination of Evidence) elsewhere in this section, and include in the requesting communication the following:

- (1) Which of the submitted items are the questioned and the known specimens
- (2) Which questioned items are to be forwarded for latent fingerprint processing, and
- (3) Personal characteristics of the writer, such as any nervousness, disability, illness, injury, etc.

EFFECTIVE: 07/25/97

13-17.4 Types of Document Examinations

- (1) Handwriting (script)
 - (2) Hand printing
 - (3) Signature
 - (a) If a traced signature, try to locate the document containing the pattern or master signature from which traced.
 - (b) If a simulated or copied signature, include samples of genuine signatures to determine the extent of simulation.
 - (c) If a freehand signature, the forger has no knowledge of how the genuine signature looks.
 - (4) Typewriting

(a)

b2/b7E

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 161

ba/b7E

(b) An examination of questioned typewriting can assist in determining a possible make and model of typewriter and/or typewriting element used to prepare the material.

(c) Questioned and known typewriting specimens of the same size and style of type cannot be identified unless individual defects or wear characteristics are exhibited in the samples.

(5) Paper

(a) Definite identification is seldom possible.

(b) Consideration should be given to indented writing, watermarks, tool or knife marks along the edges, whether the paper was torn in a manner to leave stubs in a tablet, and whether torn edges are suitable for comparison with torn edges on a source item.

(c) Some paper examinations are partially destructive and will not be conducted unless specifically advised.

(6) Paper-fiber transfer

An examination of the original document must be conducted with the suspect carbon film typewriter ribbon to determine whether or not the typewriter ribbon was utilized in the preparation of the questioned document.

(7) Writing instruments (pencils, pens, crayons, ball-point pens)

(8) Checkwriters

(a) Examination of checkwriter impressions assists in determining the manufacturer of the machine used to produce the impressions.

(b) Positive identification of questioned with known samples is infrequent because the construction of checkwriting machines inhibits the development of unique identifying defects and wear characteristics.

(9) Printing, photocopying, and other duplication

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 162

processes

(a) Printed documents may be associated as originating from a common source or may be identified with known printing paraphernalia.

(b) Photocopies may be associated as originating from the same source or may be identified with a particular machine.

| (10) | Indented writing

(a) Photographic, electrostatic, and lighting techniques are used to determine the context of indented notations.

(b) The document should not be folded or creased.

(c) Care should be taken to ensure accidental indented writings are not made in a document after its collection as evidence.

| (11) | Obliterated or eradicated writing

(a) Nondestructive methods include photography, using ultraviolet and infrared techniques, and microscopic examination.

(b) Staining methods may produce minor stains. The Laboratory should be advised whether minor staining may be applied.

| (12) | Used carbon paper

(a) Carbon paper should not be folded or creased.

(b) Examination may disclose the context of handwritten or typewritten material pertinent to an investigation.

| (13) | Burned or charred paper (See MIOG, Part II, 13-6.7.)

(a) Questioned entries on charred or burned paper may be observed with appropriate examination.

(b) Charred paper should be protected by a polyester film encapsulation method or shipped to the Laboratory in the original container in which it was burned at the crime scene. Contact the Laboratory for more specific instructions.

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 163

(c) If above options are not feasible, ship the charred paper between layers of cotton in a rigid container.

(14) Dating of a document

(a) May be based on watermarks, letterhead or other printing, and typewriting.

(b) Determination of exact dating is highly unlikely; however, it is possible to determine when items became commercially available.

(15) Wet documents

(a) Material should be frozen before shipping items to the Investigative Operations and Support Section.

(b) Freeze-dry methods of preservation will permit items to dry and reduce risk of decomposition.

(16) Deleted

EFFECTIVE: 07/25/97

13-17.5 Standards Files (Containing Known Standards Supplied by Manufacturers and/or Gathered by FBI Employees)

(1) Office Equipment File

(a) Consists of original samples of typewriting, photocopy machines, printers, and facsimile machines, from both foreign and domestic countries.

(b) Portions of this file permit classification of questioned printed material on the basis of make and model.

(2) Watermark Standards

(a) An index of watermarks and brands used by paper manufacturers.

(b) Aids in tracing source or origin of paper.

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 164

(3) Deleted

(4) Checkwriter Standards

(a) Collection of original checkwriter impressions.

(b) Permits classification of questioned checkwriter impressions as to make and model.

(5) Shoe Print and Tire Tread Standards (See MIOG, Part II, 13-19.1.5.)

(6) National Motor Vehicle Certificate of Title File

See 13-17.6(4) of this section for further information.

(7) Deleted

EFFECTIVE: 07/25/97

13-17.6 Reference Files - Material Collected Through Casework

(1) NATIONAL FRAUDULENT CHECK FILE

(a) Contains computerized and copies of samples of checks, writings, and other documentary material used by persons involved in fraudulent check schemes.

(b) Assists in identifying individuals involved in fraudulent check schemes and associates questioned material in various cases as having originated from a common source.

(c) A search through the file will be made even though the questioned material was previously searched through a check file maintained by a state or local agency, or technically examined by another agency.

(2) ANONYMOUS LETTER FILE (See MIOG, Part I, 91-17.2.)

(a) Consists of a computerized reference collection,

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 165

including digitized copies of notes and extortion and threatening letters. The criteria for an Anonymous Letter File search is as follows:

1. Kidnapping
2. Bomb threats
3. Case of the times (Abortion Clinics, Church Burnings, etc.)
4. Threats to Federal Officials
5. Contamination Issues.

(b) Assists in identifying the source of such questioned material and associates questioned material in various cases as having originated from a common source.

(c) Letters of domestic abusive or "crank" nature are neither searched nor added to the file, unless mitigating circumstances so warrant.

(d) Letters determined to be of no prosecutive value are not to be submitted to the Laboratory, unless mitigating circumstances so warrant.

(3) BANK ROBBERY NOTE FILE (See MIOG, Part I, 91-17.1.)

(a) Consists of computerized and digitized copies of writings of known bank robbers, of holdup notes found in the possession of known suspects and of notes used in actual holdups, or attempted holdups, of banks and other establishments.

(b) Assists in identifying questioned notes with known writers and associates questioned notes in various robbery cases as having originated from a common source.

(c) Notes and miscellaneous questioned writings found on counters and wastebaskets in banks which are obviously the work of mischief or prank will NOT be searched, and will NOT be added unless mitigating circumstances so warrant.

(4) NATIONAL MOTOR VEHICLE CERTIFICATE OF TITLE FILE (See MIOG, Part II, 13-17.5 (6).)

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 166

(a) Consists of a questioned section comprised of
copies of counterfeit and/or altered motor vehicle titles, by state,
utilized in the transfer or sale of a stolen motor vehicle.

(b) Consists of a known section comprised of
authentic motor vehicle titles from each state.

(c) Assists in identifying counterfeit titles as
having originated from a common source.

(d) Will provide a known standard for a
determination to be made as to the authenticity of a questioned title.

(5) Deleted

(6) Deleted

EFFECTIVE: 07/25/97

| 13-18 PHOTOGRAPHIC EXAMINATIONS | (MOVED TO 13-7.6) |

EFFECTIVE: 07/25/97

13-18.1 Deleted

EFFECTIVE: 07/25/97

| 13-18.2 | Deleted |

EFFECTIVE: 02/12/92

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 167

13-18.3 Deleted

EFFECTIVE: 02/12/92

| 13-18.4 | Deleted |

EFFECTIVE: 02/12/92

| 13-18.5 | Deleted |

EFFECTIVE: 02/12/92

13-19 SHOE PRINT AND TIRE TREAD EXAMINATIONS

EFFECTIVE: 02/12/92

| 13-19.1 How to Collect | the | Physical Evidence | (See MIOG, Part II,
10-3, 13-6.4.6.) |

| Shoe | and tire tread impression | evidence found at the scene of a crime provides important evidence for investigation and eventual prosecution of the case. All impressions should first be photographed. The | evidence or item bearing the | original impression should then be transmitted to the Laboratory, if | possible. This is easily possible in cases when the impression is on broken glass, paper, or on another surface which can be removed from the crime scene; however, it should also be seriously considered and extended to bulkier items such as doors, pieces of flooring, etc., particularly in violent crimes. If the original item cannot be removed from the scene and transmitted to the Laboratory, examination quality photographs, followed by casting or lifting techniques should be made to complete the recovery of that evidence. These techniques are described below. |

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 168

EFFECTIVE: 04/07/97

13-19.1.1 Photographing and Documenting the Evidence (See MIOG,
Part II, 13-6.4.6.)

(1) GENERAL CRIME SCENE PHOTOGRAPHS AND NOTES

General crime scene photographs are those which are taken from various distances and angles to capture the general appearance of the scene and to document certain facts about the scene. When taking general crime scene photographs of a shoe or tire impression, they should include both long-range, mid-range and close-range color photographs of the evidence. ISO 200 or 400 color film should be used. These photographs should be taken to create a zoom-in effect to show the relationship of the impressions to the surrounding area. THESE PHOTOGRAPHS ARE NOT SUITABLE FOR DETAILED FOOTWEAR OR TIRE EXAMINATIONS.

(2) EXAMINATION QUALITY PHOTOGRAPHS

Examination quality photographs are those which are taken from directly over the impressions utilizing a tripod, a scale and special lighting. The purpose of these photographs is to take a photograph which can be enlarged to the natural size via the scale and which reflects a high degree of detail. THESE PHOTOGRAPHS ARE USED FOR FORENSIC EXAMINATIONS.

The following is a procedure list for taking examination quality photographs:

(a) USE A SCALE IN EVERY EXPOSURE. Position a finely divided and accurate scale, such as a flat metric ruler, next to and on the same plane as the impression. A label may be placed in the picture to identify which impression you are photographing, in order to associate the photograph to the general crime scene photographs, crime scene sketches, etc.

(b) USE A QUALITY CAMERA. The camera should ideally be a larger format camera; however, suitable photographs can be taken with a MANUAL FOCUS 35 mm camera if proper procedures are followed. The camera should be equipped with a normal macro lens or a zoom lens in the 35-80 mm range. Load the camera with fine-grained color or black and white ISO 125 film. Check the ISO setting on the camera if the camera does not adjust to it automatically. Attach a

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 169

cable shutter release if needed.

(c) Adjust the height and position of the camera on a tripod and position it directly over the impression so that the shoe impression and ruler nearly fills the frame. Make sure the film is parallel to the impression's surface, i.e., the lens is perpendicular to the impression.

(d) Determine what special lighting will be used.
In most cases, oblique lighting should be used.

(e) For oblique lighting, a 6-foot flash extension cord must be used so that the flash can be held about 4-5 feet from the impression. This distance will allow for an even exposure across the impression. For a two-dimensional impression, such as a dust impression on a bank countertop, the flash should be positioned about 4 feet away from the impression but only about 1 inch above the surface the impression is on so that the light will graze the impressed area. For a three-dimensional impression, first decide what the height of the flash should be for the impression. The deeper the impression the higher the flash. The more shallow the impression, the lower the flash. The purpose of the oblique light is to lighten the higher areas of the impression while shadowing the lower depressed areas of the impression, thus providing increased contrast between the two. Block out any bright ambient light, particularly if the impression is outside in daylight. This can be achieved by draping a black cloth around part of the tripod or simply having someone hold the black cloth or a piece of cardboard or position their body next to the impression to block out the light and darken the area being photographed. This is very important and will maximize the benefit of the oblique light and result in much greater contrast and detail in the photograph. Several photographs with the oblique flash should be taken from at least three different sides of the impression. Always use a scale!

(f) For three-dimensional impressions, close down the f-stop to f-22 for greater "depth of field." Always make sure the camera is set on flash synchronization.

(g) ALWAYS FOCUS THE CAMERA! FOCUS THE CAMERA ON THE IMPRESSION, NOT THE SCALE, PRIOR TO EACH EXPOSURE. Use a cable shutter release or the camera timer to prevent movement of the camera during exposure.

(h) Take several exposures at each position, varying the light position, particularly if you feel this impression

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 170

is a difficult one to photograph.

(i) TAKE SEVERAL PHOTOGRAPHS OF EACH IMPRESSION.

(3) PHOTOGRAPHIC EQUIPMENT KIT CHECKLIST

Having a photographic kit prepared in advance, will help result in the proper photographic treatment of the evidence. Below is a list of items which should be included in a crime scene kit to cover both the needs of general crime scene photography and "examination quality" photography:

Camera(s) with manual focus and interchangeable lenses. Macro or zoom lens or wide angle lens for general crime scene photos. Cable shutter release. Electronic flash. Long "Flash Extension Cord" (6 feet). Light meter (for incident light as well as flash). Device for checking focus (focus loop or macro focus aid). Tripod (preferably the inverted type). Fine-grained black/white and color films (ISO 125 or less). Color film for general crime scene (200-400 ISO). Scale (rigid and flat ruler, at least 6 inches long). Labels and writing instruments. Numbered cones or markers for general crime scene. White chart board for backfill lighting. Black cloth or screen for ambient light shield. Lens filters.

EFFECTIVE: 07/25/97

13-19.1.2 Casting Three-Dimensional Shoe and Tire Impressions
(See MIOG, Part II, 13-6.4.6 and 13-6.7 (56).)

Casting is the filling of a three-dimensional impression, usually in soil, sand or snow, to capture the maximum amount of detail in that impression for examination purposes. DENTAL STONE with a PSI rating of 8,000 or more should be used for casting footwear and tire impressions. Dental Stone (or Die Stone), available through local dental supply houses, having a minimum PSI of 8,000 or above, preferably colored, is the desired casting medium. The PSI is a compression strength measurement which should be listed on the container along with the proper ratio of powder to water which should be used for mixing. There is no need to buy premixed or modified dental stone from forensic suppliers, some of which have not been satisfactory.

NOTE: Plasters, plaster of paris or dental plasters are NOT

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 171

SUFFICIENTLY HARD, do not resist abrasion when they are cleaned and, therefore, should NOT be used.

(1) ZIP-LOCK BAG METHOD FOR DENTAL STONE CASTING

(a) "Zip-lock" bags are highly recommended as a means of conveniently storing premeasured amounts of dental stone powder. A zip-lock bag measuring approximately 8 by 12 inches can easily store 2 pounds of dental stone material. Each footwear impression normally can be cast with 2 pounds. With several premeasured zip-lock bags stored and on hand, the casting of impressions at the crime scene will only involve the addition of a few ounces of water to each bag as needed. The bag can be used to both mix and pour the dental stone mixture. Those who have tried this method have found that it is a quick, clean, and convenient method of casting.

(b) Dental stone, like other gypsum materials is usually sold in quantities of 25, 50, or 100 pounds. By obtaining a source of zip-lock bags, approximately 8 by 12 inches in size, these larger containers of dental stone can be quickly divided into 2 pound portions in each bag. The bags can be laid on their side and flattened out to remove the excess air and zipped closed. The bags will keep the casting material dry and will be convenient to use when needed.

(c) When the time comes to prepare a cast, the preprepared zip-lock bags of dental stone are ready and conveniently available. To reach the necessary viscosity, dental stone requires approximately 5 to 6 ounces of water per pound. The stone will require even less water. For a 2 pound bag of dental stone, approximately 9 to 10 ounces of water will need to be added. This can be conveniently done by utilizing a 12 ounce soda can or other measure. Since the exact amount of casting material will vary slightly from bag to bag, and the powder-to-water ratio will vary slightly from one brand of dental stone or die stone to another, the following procedure is recommended. Pour about two thirds of the estimated water needed into the bag. Allow the water to soak into the dental stone for two minutes. Zip the bag closed and mix the casting material by massaging and gently squeezing the bag. If more water is needed, add an ounce of water and continue to mix the material. Make sure that all of the material in the corners of the bag is mixed. If too much water is accidentally added, simply add a small amount of dental stone from another bag. The proper viscosity should be that of pancake batter or thick cream. The mixture should not be watery nor should it be so thick that it won't flow into an impression. When the

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 172

water and dental stone are completely mixed and the proper viscosity is reached, the casting material is ready to be poured. This is easily accomplished by unzipping the bag and, holding it at ground level next to the edge of the impression, and carefully pouring the material into the impression.

(d) The zip-lock bag method has proven to be a very popular one and provides a convenient, clean and rapid way of preparing a quality cast. If more than one cast is being prepared, the person conducting the casting can solicit the help of other individuals to assist in the mixing portion of this process.

(2) MIXING DENTAL STONE IN A BUCKET

Although the zip-lock bag method is distinctly favorable for footwear impressions, the normal size of most tire tread impressions would necessitate the mixing of larger amounts. If a large quantity of dental stone is to be mixed at one time in a bucket, such as for a tire impression, the quantity of powder to water should first be determined. For instance, if 10 pounds of dental stone identical to the aforementioned example is used, where every 2 pounds of dental stone required 9.6 ounces water, 10 pounds would require 48 ounces of water. The water should first be added to the bucket and then the dental stone should be sifted into the water. The mixture should be stirred thoroughly when adding the powder and continuously for at least three minutes. Once the material is thoroughly mixed, the material can be poured into the impressioned area.

(3) POURING THE CASTING MATERIAL

(a) Whether a form is used or not and whether the casting material is mixed in zip-lock bags or in buckets, the procedure and precautions for pouring the casting material into the impressioned area are the same. Casting material has sufficient weight and volume to easily erode and destroy valuable detail if it is carelessly poured directly onto the impression. This is especially true in the case of fragile soil and sand impressions. When pouring the casting material from the zip-lock bags, the bag should be placed next to the impression so that the casting material does not cascade onto the impression, but instead, falls on the adjacent ground after which it will flow into the impression. When pouring the material from a bucket into the impression, a flat stick or a spoon should be held over an area to the side of the impression. The casting material can be poured from the bucket onto the stick or spoon in a way so that the spoon or stick will absorb the impact of the dental stone which will then flow harmlessly into the impression. With impressions which

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 173

are on a slope or with impressions which have forms around them, the casting material could be poured from the bucket onto the higher ground next to the impression in a way so that the casting material would then naturally flow into the impression. Again, it should be emphasized that the entire impression must be filled with casting material until it has OVERFLOWED.

(b) Sometimes when mixing large amounts of dental stone in a bucket the viscosity of the dental stone may be ideal at the beginning of the pour but too viscous by the end of the pour. This is due to the settling of the mixture. Making sure the dental stone and water are thoroughly mixed immediately before pouring each impression can help offset this.

(c) Occasionally, whether the dental stone mixture is in a bucket or a bag, it is not apparent that the mixture is too viscous until it has been actually poured. Of course, then it is too late to change the mixture. The viscous mixture can be encouraged to flow into the impression simply by taking your finger or a small stick and vibrating it back and forth on the surface of the mixture. This will help the dental stone to relax and flow into the impression. Be careful not to put the stick or finger more than about 1/4 inch below the surface of the casting material as it might damage the impression.

(d) Before the cast completely hardens, it is possible to scratch the date, your initials and other needed information onto the back side of it. An alternate way of identifying the cast is to set a paper clip into the back of the cast before it sets. When the cast sets, an identifying tag can be attached to the paper clip.

(e) The cast should then be left undisturbed for at least 20 to 30 minutes in warm weather. If the temperature is cold, the cast should be allowed to sit considerably longer. Many casts have been destroyed or damaged because they were lifted too soon. When the time has come to lift the cast, care should be taken so as not to damage it. If the cast has been poured in sand or loose soil, it should lift very easily. Casts which are poured in heavier soils such as mud or clay, may require more careful treatment when being lifted.

(f) Allow the cast to air dry for AT LEAST 48 HOURS before cleaning it. It does not reach its total hardness for 24 to 48 hours.

(4) CLEANING A DENTAL STONE CAST

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 174

Cleaning a dental stone cast should be left to the examiner after drying for 48 hours and thoroughly attaining maximum hardness. Dental stone casts made in sand or light soil can be cleaned simply by using water and a soft brush. Those casts poured in heavy clay soils which adhere to the cast surface can be cleaned by submerging the cast in a saturated solution of potassium sulfate for about 30 - 60 minutes. This will assist in the removal of soil from its surface. A soft brush can be carefully used to help free stubborn soil. Afterwards, rinse the cast thoroughly in water and then allow the cast to thoroughly air dry.

EFFECTIVE: 07/25/97

13-19.1.3 Lifting Two-Dimensional Impressions from Surfaces
(See MIOG, Part II, 13-6.7 (61).)

Lifting an impression allows for the transfer of a two-dimensional residue or dust impression to a lifting film giving it greater contrast. It also allows for it to be transported to the laboratory and photographed.

Lifting can be accomplished with an electrostatic lifting device (useful for dry impressions of dry origin), with gelatin lifting materials (useful for both dry and wet origin impressions) and adhesive lifting materials (used only for lifting impressions which have been developed with fingerprint powder and which are on nonporous surfaces).

(1) ELECTROSTATIC LIFTING DEVICE FOR LIFTING DRY RESIDUE IMPRESSIONS

(a) With the electrostatic lifting device, footwear impressions can be lifted from virtually any surface, both porous and nonporous. The device works best on DRY DUST OR DRY RESIDUE FOOTWEAR IMPRESSIONS WHICH ARE ON SURFACES THAT ARE RELATIVELY CLEAN. For impressions which fall into that category, the lifting device is excellent at lifting footwear impressions. If the impressions were wet when they were made or if they become wet or damp prior to lifting, the electrostatic lifting device WILL WORK POORLY OR NOT AT ALL. It is important to understand that THE ELECTROSTATIC LIFTING DEVICE IS USEFUL FOR DRY IMPRESSIONS AND NOT IMPRESSIONS OF WET ORIGINS. It is also important to remember that impressions which do

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 175

not lift are NOT destroyed. Therefore, in cases where it is unknown whether an impression is of wet or dry origin, the use of the electrostatic lifting device will not risk the loss of or damage to the impression.

(b) It has always been a difficult, if not impossible, to successfully photograph and retrieve certain types of dust and residue footwear impressions, particularly if the impressions were on a surface where contrast was poor, on textured surfaces or in instances where the impressions were either latent or were barely visible. The electrostatic lifting device now makes it possible to both locate and retrieve footwear impressions of this type which have been previously overlooked, ignored, or lost in unsuccessful attempts to retrieve them. In fact, it may also be used to lift totally latent impressions from surfaces where it is suspected footwear impressions may be present even though they cannot be seen. It is therefore an excellent crime scene device which can be used to make a "blind search" of areas where it is likely that the suspect walked and therefore could potentially contain latent but retrievable dry residue impressions.

(c) The best way to familiarize oneself with the usage, applications and limitations of the electrostatic lifting device is to try a variety of lifting procedures on a variety of both dry and wet origin impressions and on a variety of surfaces. Equipped with this knowledge and experience, the use of the electrostatic lifting device at crime scenes and in laboratory casework becomes an easy routine.

(d) Not all dry impressions can be "successfully" lifted. Attempts to lift residue footwear impressions on a dirty surface which itself contains loose residue will result in both the impression and the background residue being lifted together. The lifting film will be covered with residue and the footwear impression will be lost in it. However, if the shoes of the suspect are damp or sticky and walk through a dirty surface, it may be possible to detect "negative" impressions where the residue on the surface was removed and adhered to the shoe and the negative image of the shoe sole remained.

(2) PROCEDURE FOR USING ELECTROSTATIC LIFTING DEVICES

Most electrostatic lifting kits will be accompanied by instructions; however, some basic instructions are supplied here. To lift an impression with the electrostatic lifting device, the following procedures should be used:

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 176

(a) POSITION THE GROUNDING DEVICE

The ground wire of the electrostatic lifting device must be attached to the ground plate or other grounding material. The ground plate should be positioned as follows:

1. If at all possible, position the ground plate beneath the impressed item. This would be the best choice in the case of impressions on paper, loose carpeting, and other movable items. Since the lifting film may be larger than the impressed item, a piece of clear chart board or similar nonconductive material must be used as a separator and should be placed between the impressed item and the ground plate to keep the lifting film separated from the ground plate. If the metal laminated layer of the lifting film is in contact with the ground plate, arcing will occur and the device will not work.

2. Very often the impression will be on a surface, such as a tile floor, where the ground plate cannot be placed beneath the impression. In those instances, position the ground plate at least 2 inches away from the lifting film and with the metal side of the ground plate facing the ground or surface.

3. If the impressed item is on surfaces such as a door, chair seat, etc., place the ground plate in the best position to be most effective. In the case of a door, the ground plate can be taped to the rear side of the door with the metal side facing the impression. In the case of the chair, it can be taped alongside the impression on the chair or beneath the seat. To be most effective, the metal side of the ground plate should be in maximum contact with the adjacent surface whenever possible.

4. Occasionally, the footwear impression will be on a metal object such as a car hood, metal cabinet or other metal object. In those cases, the ground plate can be used or the ground lead can be attached directly to the car frame or metal object. ON METAL SURFACES AN ALTERNATE PROCEDURE SHOULD BE USED FOR THE PLACEMENT OF THE LIFTING FILM. (SEE STEP #2 IN (b) BELOW.)

After positioning the ground plate, attach one end of the ground wire to it or in the case of a metal object, connect the ground lead to that object. Plug the other end of the ground lead into the voltage source.

(b) PREPARE AND POSITION THE LIFTING FILM OVER THE

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 177

IMPRESSION

1. Position a piece of lifting film over the impression with the black side facing against the impression. The black side will face down and the metal laminated side will face up. The placement of the lifting film should be handled carefully so as not to disturb or smear the impression. NEVER slide the lifting material over the surface. The lifting film should not touch any part of the ground plate. It may be necessary to place a piece of clean chart board between the impressed item and the ground plate or to make other adjustments so that the film and ground plate are not in contact with one another.

2. In cases where the impressed surface is metal, carefully place a piece of clear, very thin (1 or 2 mil) mylar or polyester over the impression. Then place a slightly smaller piece of lifting film, black side down, over the mylar. The mylar should be bigger than the lifting film to assure that none of the black lifting film is touching the metal surface. Continue with the lifting procedure as outlined; however, remember that the lifted impression will now be on the mylar. The mylar and the black lifting film can be lifted and kept together to provide the necessary contrast.

3. The electrostatic lifting of some impressions, particularly those which are latent or which may not be detectable until after lifting, can leave the crime scene technician with a lifted impression which can no longer be oriented as to its direction in the crime scene. It has been suggested that marking the lifting film and the impressed surface will later facilitate the orientation of the lifted impression. The need for this step should be considered prior to making any lifts.

(c) PLACE THE PROBE ON THE LIFTING FILM

1. The tip of the hand-held probe should be held in contact against an edge of the metal laminated backing of the lifting film. There is no need to move the probe around during the charging of the film. It should remain in contact with the film during the entire procedure. THE VOLTAGE CAN NOW BE TURNED ON. It is usually only necessary to turn the voltage on a low setting although in cases where the current must travel through thicker materials, a higher setting will be required. The application of sufficient voltage will cause the lifting film to be pulled down tightly against the impression. In some instances air bubbles will be trapped beneath the film. These will often disappear in a few seconds. If any air bubbles remain trapped beneath the film they may be rolled out with a

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 178

clean fingerprint roller or brayer. This should be done very gently by lightly passing the roller over the film. The weight of the roller is all the pressure that should be used. Excessive pressure while rolling the film may damage the impression. If arcing occurs between the film and the ground, either the power is set too high or part of the lifting film is touching or too close to the ground plate.

2. After the power is turned off, allow the probe to remain in contact with the film for approximately five seconds for the purpose of discharging the film. When this is done, the film can be seen to relax as the charge leaves it.

(d) REMOVE THE LIFTING FILM

1. The film can now be removed from the impressioned area by carefully peeling it off from one end to the other. Once the film is removed, lay it on a clean flat surface with the black side facing up. In a totally dark room examine the film carefully with oblique light to see if an impression has been transferred to it. If this is not possible at the crime scene, then all lifts should be saved until they can be examined in TOTAL DARKNESS. Film should never be discarded without first CAREFULLY EXAMINING THE FILM IN A DARKENED ROOM WITH THE AID OF A STRONG OBLIQUE LIGHT. Many times, film which is viewed in ambient lighting or without a strong oblique light source will initially appear to contain no impressions. Further examination of that film in total darkness with a strong oblique light often reveals the presence of valuable impressions.

2. Often many residue impressions are so heavy that the first lifting process actually results in a lifted impression with too much residue. In those cases, a second lift of the same impression should be made as it sometimes results in an impression which appears clearer and much better for examination.

(3) STORAGE OF THE LIFTING FILM AFTER LIFTING

(a) Lifted impressions are fragile and can easily be damaged if the film is not secured. The film often contains a residual charge which can attract other dust and debris or cause the film to cling to another surface. For that reason, the lifting film should be protected immediately after being removed from the impression.

(b) To properly preserve and store the impressioned item or lifting film containing an impression, it should be stored

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 179

securely in a folder or in a shallow photographic paper box. Do not use pizza boxes or similar low-grade cardboard or cardboard boxes as the residual charge on the lifting film will pull dust from the cardboard and interfere with the lifted impression. If a folder is used for the film, place the film on one side of the folder and secure it with a piece of tape. If the film should slide around in the folder or is pulled out of the folder while it is closed, the delicate lift will be damaged. Whenever the lift must be removed, the folder should be opened first, followed by removal of the lift. When a shallow box is used, the impressed item or lift can be taped securely into the bottom of the box.

(c) Items which contain a dry residue footwear impression SHOULD NEVER BE WRAPPED IN PLASTIC OR STORED IN A PLASTIC BAG. If they are, a partial transfer of the impression to the plastic will take place.

EFFECTIVE: 07/25/97

13-19.1.4 | Other Enhancement/Recovery Considerations

Specialized photographic, physical and chemical enhancement techniques may be utilized in the Laboratory for all types of impressions, providing the original impressed item can be removed from the scene and submitted to the Laboratory.

EFFECTIVE: 04/07/97

13-19.1.5 Laboratory Examinations | (See MIOG, Part II, 13-17.5.) |

(1) Footwear Computer Database Collection

Extensive footwear design and reference materials are maintained in the Laboratory to assist in determining the manufacturer of a particular shoe or tire design.

(2) If known shoes or tires of suspects are obtained and transmitted to the Laboratory along with the questioned impression

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 180

evidence, the Laboratory can make forensic comparisons and can determine:

- (a) If the suspect's shoes or tires correspond in design and size with the questioned impressions.
- (b) If the suspect's shoes or tires correspond in wear and other identifying characteristics allowing for A POSITIVE IDENTIFICATION.
- (c) That the shoe or tire designs can be eliminated.

EFFECTIVE: 07/25/97

| 13-20 | RACKETEERING | RECORDS ANALYSIS

EFFECTIVE: 05/25/90

13-20.1 Types of Specialized Assistance and Examinations Available

EFFECTIVE: 05/25/90

13-20.1.1 Bookmaking/Numbers Operations

Analysis and interpretation are made of handwritten and printed systems of recording wagering on sports events; policy and numbers betting based on horse and dog racing, stock market data, drawn numbers, etc. Testimony is given concerning interpretation of records and/or manner of conducting such gambling operations and terminology.

EFFECTIVE: 05/25/90

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 181

13-20.1.2 Loan Sharking (Shylocking) Records

Analysis of accounting-type notations to determine amount of outstanding loans, amounts paid in accrued interest and principal, total number of loans, and true annual rate of interest computed by the actuarial method.

EFFECTIVE: 05/25/90

13-20.1.3 Prostitution

Prostitution records are analyzed to determine the scope of the business, including the number of employees, their roles, gross and net revenues, and other financial information.

EFFECTIVE: 05/25/90

13-20.1.4 Drug Records

Analysis and interpretation of records relating to illicit drug operations. Records are examined to identify the type of drugs being distributed, their gross and/or net weights or quantities, income generated, money flow, number of persons involved and other like information. Emphasis is placed on supporting drug cases resulting in judicial proceedings such as grand juries, criminal trials, sentencing hearings and forfeiture hearings.

EFFECTIVE: 05/25/90

13-20.1.5 Lotteries, etc.

Evidence of this nature would include lottery tickets, sports parlay cards, sweepstakes, tip tickets and boards, punchboards, and machine tickets. If the printing plates or numbering dies are located, it may be possible to prove that evidence collected was printed by the particular plate or die.

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 182

EFFECTIVE: 05/25/90

13-20.1.6 Deleted

EFFECTIVE: 05/25/90

13-20.1.7 Money Laundering

Analysis and interpretation of records relating to money laundering business. Cryptic and actual business records are examined to determine the financial flow of the operations.

EFFECTIVE: 05/25/90

13-20.2 Types of Gambling Evidence

(1) Sports wagering slips.

(2) Numbers wagering slips.

(3) Summaries of wagering slips or tallies including adding machine tapes used to calculate wagering or to summarize writer's accounts. Charting of wagers, systematically done to determine volume of wagering on various events.

(4) Accounting and financial records or "bottom sheets" showing numerous accounts (sometimes code-designated), amounts and/or commissions paid to writers.

(5) Related paraphernalia - sports schedules or line sheets, sports records materials, dream books, cut cards, parlay manuals, conversion charts, scratch sheets, racing forms, etc.

(6) Semidestroyed material such as charred, shredded, torn or wet water-soluble paper.

(7) Transcripts of pertinent legally obtained telephone conversations.

(8) Mechanical, electro-mechanical and electronic video

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 183

gambling devices, including coin-operated slot machines as well as devices which electronically simulate or depict the playing of card games, casino games, bingo, keno, lotteries, and horse races.

EFFECTIVE: 06/26/96

13-21 CRYPTANALYSIS

Because of the unique nature and wide scope of these examinations and of the material which may be available for examination, it may be appropriate to telephonically contact the Investigative Operations and Support Section of the FBI Laboratory to resolve any questions that might arise.

EFFECTIVE: 03/21/95

13-21.1 Types of Examinations

EFFECTIVE: 11/21/89

13-21.1.1 Cryptanalytic

- (1) Cryptograms or codes.
- (2) Notes or notebooks containing cryptic notations.
- (3)- Material containing symbols or unusual literal or numerical notations.
- (4) Correspondence or documents which might contain hidden intelligence, such as
 - (a) Marked letters or numbers.
 - (b) Double meaning, wherein certain words and/or phrases are given arbitrary meanings by the writer.

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 184

(c) Concealment ciphers, where letters or words are significant according to their positions in the document.

EFFECTIVE: 06/26/96

| 13-21.1.2 | Deleted |

EFFECTIVE: 11/21/89

13-21.2 Material to be Furnished to the Laboratory

EFFECTIVE: 11/21/89

| 13-21.2.1 | Cryptanalytic |

- (1) Any work papers available.
- (2) Identity of foreign languages that might be involved.
- (3) Information as to what the intent or subject area of the document might be.
- (4) Complete background information on the case.
- (5) Special training subject may have received.
- (6) Books, code books, cipher machines, pads, tables, etc., in the subject's possession.

EFFECTIVE: 06/26/96

13-21.2.2 Deleted

Sensitive
PRINTED: 02/18/98

Manual of Investigative Operations and Guidelines

Part II

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 185

EFFECTIVE: 11/21/89

13-21.2.3 Deleted

EFFECTIVE: 11/23/87

13-22 POLYGRAPH EXAMINATIONS

EFFECTIVE: 11/23/87

13-22.1 General Information

The following general information applies to the polygraph technique and its use in the FBI:

(1) The theory of detection of deception is predicated upon the principle that individuals usually manifest certain physiological reactions when practicing deception, particularly if the truth might produce an undesirable effect on their personal welfare. The reactions are primarily involuntary in character and normally cannot be controlled. During a polygraph examination, changes in the examinee's respiratory cycle, galvanic skin response and mean blood pressure and heart rate are recorded simultaneously and continuously on chart paper during a series of questions. The polygraph chart thus produced is evaluated to determine if the recorded reactions are of the type normally associated with truth or deception. A polygraph test, however, only determines the examinee's perceptions of the truth, not actual truth.

(2)- Based upon the examiner's study of the degree and nature of changes and variations in the recorded parameters, one of the following opinions can be reached:

- (a) That the recorded responses were not indicative of deception;
- (b) That the recorded responses were indicative of deception;
- (c) That the recorded responses are inconclusive; or

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 186

(d) That the examiner expresses no opinion as to the truthfulness of the examinee due to the incomplete nature of the examination.

(3) Findings and conclusions resulting from interpretations of polygraph charts are generally not admissible in court. There appears to be a trend, however, toward admissibility of the polygraph test results.

(4) Statements, admissions and confessions obtained during a polygraph examination are admissible in court.

(5) The polygraph may be used for the following purposes:

(a) To aid in determining whether a person has pertinent knowledge of a particular matter under investigation or inquiry.

(b) To aid in determining the truthfulness of statements made or information furnished by a subject, victim, witness, informant, and/or an individual making allegations.

(c) To obtain information leading to the location of evidence, individuals or sites of offenses.

(d) To assist in verifying the accuracy and thoroughness of information furnished by applicants and employees in certain situations as specified in section 13-22.12 (Applicants) and section 13-22.13 (Employees).

(6) To enable the Bureau to realize the maximum benefit from their specialized training and skills and in order that they may retain their proficiency in the technique, polygraph examiners are to be utilized primarily as polygraph examiners/interrogation specialists. For this reason, and in order to ensure that each field office has equal access to an examiner, "territorial assignments" have been made for polygraph examiners. Examiners assigned to particular offices are responsible for a territory which includes their own office of assignment and designated neighboring field office. Requests for examinations are to be handled on a priority basis without regard to the examiner's office of assignment. In the event that the examiner responsible for covering a particular office is unavailable to conduct an examination that is needed on an expedite basis, SACs are authorized to coordinate directly with another neighboring office to obtain the services of an examiner.

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 187

EFFECTIVE: 11/23/87

13-22.2 General Policy

The following general policies apply to the use of the polygraph by the FBI:

(1) The polygraph technique is highly reliable and valuable as an investigative tool when used by a competent and ethical examiner.

(2) The polygraph is to be used selectively as an investigative aid and results considered within the context of a complete investigation. Polygraph results are not to be relied upon to the exclusion of other evidence or knowledge obtained during the course of a complete investigation. Use of the polygraph for dragnet-type screening of large numbers of suspects or as a substitute for logical investigation by conventional means is prohibited.

(3) Polygraph examinations will be administered only to individuals who agree or volunteer to take an examination. In criminal cases, information concerning a person's refusal to take a polygraph examination shall appear only in the unproductive investigation section of the prosecutive report or in the administrative section of other reports.

(4) The following areas are not to be probed unless directly relevant to the investigation or inquiry.

- (a) Religious beliefs or affiliations
- (b) Beliefs and opinions regarding social matters
- (c) Information concerning sexual opinions or practices
- (d) Political beliefs and organizational affiliations of a nonsubversive nature.

(5) Polygraph examinations may only be conducted when the examiner, in his/her professional judgment, believes the results will be accurate. All reasonable efforts must be made to ensure accuracy of the results.

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 188

EFFECTIVE: 11/23/87

13-22.3 Authorization/Approval for Conducting Examinations

The following guidelines govern authorization for the conduct of polygraph examinations:

(1) The SAC or person acting for that official may authorize polygraph examinations in connection with an ongoing Bureau case, except as follows:

(a) For authorization regarding polygraph examinations of Bureau employees and persons who make allegations against Bureau employees, see 13-22.14.

(b) Examinations conducted as a cooperative service to other federal agencies must receive prior authorization of the Assistant Director, Laboratory Division, or person acting for that official. SACs should forward such requests to Laboratory Division, Polygraph Unit, with recommendations concerning the propriety of the polygraph examination by a Bureau examiner, consistent with the factors of 13-22.4, and other pertinent interests of the Bureau. All such requests will be considered on a case-by-case basis.

(c) No polygraph examination will be conducted by a Bureau examiner for a state, county or municipal law enforcement agency as a police cooperation matter.

(d) Regarding polygraph examinations of defendants in post-conviction and presentencing situations, the SAC may authorize examinations in those postconviction situations where the polygraph is used in furtherance of continuing investigative interests, such as determining if the defendant perjured himself/herself during trial, verifying that defendants have fully complied with plea bargaining arrangements and conditions, determining the accuracy of information provided by convicted cooperating witnesses and testing the validity of extenuating and mitigating circumstances bearing on sentencing considerations. FBIHQ authority is necessary to conduct a polygraph examination in those situations where the purpose of a proposed polygraph examination would be to determine the veracity or guilt of a defendant with respect to an issue previously determined by trial. Such situations would include a presentence request or order for a polygraph examination by a presiding judge to determine in essence

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 189

whether the defendant was really guilty of the offense for which he/she was convicted.

(2) In cases where FBIHQ approval is required, the authorizing FBIHQ official shall be identified on the Polygraph Examination Report (FD-498) which is forwarded to FBIHQ.

(3) Only Bureau polygraph examiners are to be used in FBI cases.

(4) Prior to SAC authority for a polygraph examination in a Financial Institution Fraud case, the USA should be contacted to ensure the USA will consider prosecution should a subject be identified. The result of contact with the USA should be confirmed in writing by appropriate communication to the USA and reported in all subsequent communications relating to the polygraph examination. (See MIOG, Part I, 29-5.)

(5) The decision as to whether or not to employ a polygraph examination must be made with the awareness that it might impact on other prosecutive actions. Therefore, consultation with the office of the USA should take place where deemed appropriate.

(6) Bureau polygraph examiners are trained to evaluate the suitability of the polygraph technique and they should be directly consulted, when possible, as to its applicability and limitations in particular situations. Unresolved issues will be referred to the FBIHQ Polygraph Unit.

EFFECTIVE: 10/13/95

13-22.4 Factors to be Considered in Approving Examinations

When evaluating the advisability of utilizing the polygraph the following factors should be considered:

(1) Determine if investigation by other means has been as thorough as circumstances reasonably permit, the proposed examinee has been interviewed and, consistent with the circumstances of the case, the development of additional information by means of a polygraph examination is believed essential and timely for further conduct of the investigation or inquiry.

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 190

(2) Ensure that there is reasonable cause to believe that the person to be examined has knowledge of or was involved in the matter under inquiry or investigation or if the person is withholding information relevant to the inquiry or investigation.

(3) Determine if age is a factor. If a minor is to be examined, ensure a waiver is obtained from a parent or guardian.

(4) Are there any known physical or mental abnormalities?

(5) If the examinee is in custody, can full security and control be assured?

(6) Will the use of the polygraph jeopardize any local or Federal prosecution?

(7) What were the results of any prior polygraph examinations afforded the examinee?

EFFECTIVE: 09/15/80

13-22.5 Verification of Information

When information is supplied to the FBI and that information is not reasonably subject to verification by other investigative methods, use of the polygraph could be of value. Utilization of polygraph should be considered prior to making significant commitments of the Bureau's manpower or financial resources solely on the basis of unverified information. Use of polygraph will in no way absolve Agents of their responsibility to conduct all logical investigation possible by conventional means in order to verify the truthfulness and accuracy of information furnished.

EFFECTIVE: 09/15/80

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 191

13-22.6 Responsibilities of the Case Agent

The case Agent is normally the first person to realize that a polygraph examination may be helpful to the investigation. In this regard it is important for the case Agent to understand certain aspects of polygraph procedure and to be fully aware of the existing policies concerning the use of the polygraph. A case Agent has the following responsibilities in connection with polygraph examinations:

- (1) Before a case Agent attempts to determine whether a proposed examinee will consent to an examination, it must first be ascertained that the SAC concurs in the need for and authorizes the use of the polygraph. Indiscriminate solicitation of individuals to submit to a polygraph examination is not an efficient or effective investigative procedure.
- (2) When a polygraph examination has been authorized, the case Agent should promptly reinterview the proposed examinee and ascertain if he/she will agree to submit to the examination. If the examinee is agreeable to the test, the case Agent will notify an examiner from his/her office or, in the event no examiner is assigned, the examiner of another office assigned to provide such support. The case Agent will then schedule a time and place for the examination to be conducted which is mutually agreeable with the examiner and the proposed examinee.
- (3) The case Agent should bring to the attention of the examiner any previously determined illness or psychiatric condition which would preclude the conduct of a meaningful polygraph examination.
- (4) If the examinee is suffering from any current illness or physical condition, consideration should be given to rescheduling the examination.
- (5) The person to be examined should not be subjected to lengthy interrogation immediately prior to the examination.

(6)



ba/b7E

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 192

b2/b7E

(7) An investigator who is thoroughly familiar with the investigation, preferably the case Agent, should be available to assist the polygraph examiner as required during the test. This investigator should also be available to take any statement or confession which the examinee may elect to give after the examination is concluded.

EFFECTIVE: 10/13/95

13-22.7 Mental and Physical Fitness of the Examinee

Due to the nature of the polygraph examination the following guidelines apply:

(1) Persons who are not in sufficiently sound physical or mental condition will not be afforded a polygraph examination.

(2) A person to be examined should have had adequate food and rest before the examination. Examinee should not, at the time of the examination, be under the effects of alcohol, narcotics, drugs, stimulants, or sedatives. During the pretest interview, the examiner will specifically inquire of the person to be examined whether or not he/she is presently receiving or has in the past received medical or psychiatric treatment or consultation.

(3) Polygraph examinations will not be conducted if, in the opinion of the examiner, any of the following inhibit the individual's ability to respond or otherwise cause the individual to be an unfit candidate for examination:

(a) It is apparent that the examinee is mentally or physically fatigued.

(b) The examinee is unduly emotionally upset, intoxicated, or adversely under the influence of a sedative, stimulant, or tranquilizer.

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 193

(c) The examinee is known to be addicted to narcotics.

(d) The examinee is known to have a mental disorder which causes the examinee to lose contact with reality or which could reasonably result in the examinee becoming violent during a test.

(e) The examinee is experiencing physical discomfort of significant magnitude or appears to possess disabilities or defects which, in themselves, might cause abnormal physiological reactions.

(4) Should the examiner or examinee have any doubt concerning the above conditions, the matter should be referred to the FBIHQ Polygraph Unit for determination and appropriate action. An examiner will not attempt to make a psychiatric or physical diagnosis of an examinee.

(5) If an examiner has any doubt concerning the ability of an examinee to safely undergo an examination, a statement from the examinee's physician must be obtained before proceeding with the test.

EFFECTIVE: 01/11/85

13-22.8 Polygraph Examination Room

EFFECTIVE: 01/11/85

13-22.8.1 Considerations in Selecting Polygraph Room

The polygraph examination room is of the utmost importance to professional and successful examinations. The room should be relatively free from outside noise and distraction which could break the mood carefully created by the examiner or which could cause distortion in the chart tracings and make them difficult or impossible to interpret. The polygraph room should also have a neat, professional appearance as such will contribute to the confidence the examinee has in the examiner--an essential prerequisite for a successful examination. Each should include an observation device and sound reproducer to allow authorized witnesses to see and hear the activities of the examination.

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 194

EFFECTIVE: 01/11/85

13-22.8.2 Specifications for Polygraph Room

Offices undergoing remodeling or occupying new space should contact the FBIHQ Polygraph Unit for detailed recommendations and construction specifications for polygraph rooms and furnishings.

EFFECTIVE: 10/13/95

13-22.9 Legal Representation of the Examinee

In criminal matters if so requested, the examiner should provide examinee's attorney a briefing on polygraph procedures. Consistent with other case interests, the attorney may monitor the examination if the facility has that capability. The attorney should not be in the same room where the examination is being conducted.

EFFECTIVE: 01/11/85

13-22.10 Pretest Interview

During the pretest interview the following items will be covered with the examinee by the examiner.

(1) The examinee will be advised:

(a) Of his/her rights, if appropriate, in accordance with the "self incrimination clause" of the Fifth Amendment to the Constitution and that an attorney may be obtained and consulted.

(b) That the examination will be conducted only with the examinee's prior consent.

(c) Of the characteristics and nature of the polygraph instrument, the procedures to be followed during the examination, and all the questions to be asked during the testing phase of the examination.

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 195

(d) Whether the area in which the examination is to be conducted contains a two-way mirror or other observation device, and whether the conversation during the examination will be monitored in whole or in part by any means.

(2) An appropriate consent or agreement form will be executed. Should the examinee agree to be examined, but refuse to sign the consent or agreement form, this should be noted on the form by the examiner and witnessed by one other person. The following forms will be used for this purpose:

(a) FD-328, Consent to Interview With Polygraph. This form is to be executed immediately prior to each examination, except those of applicants and employees who are examined under the provisions of 13-22.13.1 of this manual.

(b) FD-328a, Employee Agreement To Interview with Polygraph In Connection With An Administrative Interview. This form is to be executed prior to each examination under the provisions of 13-22.13.1.

(c) FD-328b, Applicant Agreement To Interview With Polygraph. This form will be executed prior to each examination of an applicant.

(3) The examiner will discuss the examinee's background with the examinee and obtain information to complete the necessary forms and to properly formulate questions.

(4) The matter under investigation, inquiry, or at issue, will be discussed in detail with the examinee.

(5) The test questions will be formulated by the examiner based on the case facts and the pretest phase of the examination. Each question to be used will be thoroughly discussed with the examinee. Words and terminology in questions must be completely understood by the examinee and wording will be in the vernacular of the examinee insofar as is possible. The examinee must understand the full meaning of each question. The questions should be simple, direct, and designed to elicit a "yes" or "no" answer only. They should not imply guilt on the part of the examinee.

EFFECTIVE: 12/16/88

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 196

13-22.11 Reporting Procedures

The following procedures shall apply in reporting the results of the polygraph examination:

(1) Normally within ten working days following the completion of each examination, the examiner will forward, by special preprinted envelope, the following items which will reflect his/her preliminary opinion of test results for quality control review by a second certified Bureau examiner.

(a) Polygraph Examination Worksheet (FD-497) - submit original and one copy to FBIHQ.

(b) Polygraph Examination Report (FD-498) - submit original and one copy to FBIHQ.

(c) Consent or Agreement form (FD-328, FD-328a, or FD-328b)

(d) Copy of Interrogation, Advice of Rights (FD-395) (if used)

(e) All polygraph charts

(2) As polygraph examination results are not considered final until completion of the quality control review, preliminary opinions of truth or deception should not appear in any other document prior to concurrence in that opinion by polygraph review personnel of FBIHQ. This includes airtels, teletypes, etc. Examiners should advise case Agents of the danger involved in transmitting unofficial or preliminary findings. The Polygraph Examination Report (FD-498) is to be considered as a draft report until approved by supervisory personnel at FBIHQ.

(3) In criminal cases, upon completion of review at FBIHQ all polygraph documents will be returned to the field. In inquiry type examinations and those otherwise involving Bureau employees or applicants, the polygraph documents will be retained at FBIHQ.

(4) In the event it is determined that further testing or reevaluation is necessary, all documents and charts will again be forwarded to the Laboratory for additional quality control review following such reevaluation or retesting.

(5) Upon completion of the polygraph examination, an FD-

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 197

302 should be prepared to reflect all relevant admissions made by the examinee. However, the opinion of the polygraph examiner regarding indications of truth or deception will be recorded only on the Polygraph Examination Report (FD-498), which will be submitted to the case file in the same manner as other laboratory reports after review by FBIHQ quality control personnel. If no admissions are made, an FD-302 is not necessary as all relevant information will be on the FD-498.

(6) A copy of all correspondence pertaining to polygraph matters should be designated for Bufile 80-5, the Polygraph Matters control file.

(7) Data regarding polygraph examinations and results (FD-498) is to be reported in the body of investigative reports in the same manner as other investigative matters.

EFFECTIVE: 10/13/95

13-22.12 Polygraph Examinations of FBI Applicants (See MIOG, Part I, 67-7.10, Part II, 13-22.1(5)(d).)

(1) All FBI applicants for support and Special Agent (SA) positions (including on-board support employees who apply for SA positions) must undergo a polygraph examination focusing on national security issues, use or sale of illegal drugs and completeness of the FD-140 (Application for Employment). Standardized testing formats have been provided to each field polygraph examiner for their use. These examinations are to receive priority attention and should be handled in a manner that will expedite the applicant process.

(a) Deleted

(b) Deleted

(c) Deleted

(2) The Special Agent Applicant Unit (SAAU) and the Bureau Support Applicant Unit (BSAU), Personnel Division will ensure that all applicants are advised that they will be required to submit to a polygraph examination during the processing of their application and prior to their employment to assist in the resolution of issues directly related to national security, the FBI guidelines regarding

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 198

the sale and use of illegal drugs and the accuracy/completeness of the FD-140 (Application for Employment-FBI).

(3) Any pertinent information developed during the polygraph examination should be provided in writing by the applicant on a supplemental information form.

(4) A preemployment polygraph examination is one element of the overall applicant screening process. It is not to be considered as a substitute for a thorough and complete background investigation. The preemployment polygraph test is NOT designed to assess trustworthiness and suitability in areas NOT covered by the examination.

(5) Failure to submit to a polygraph examination, or failure to satisfactorily cooperate during the examination will be considered in determining whether the applicant shall be hired. Prior to the examination, the examiner will obtain the applicant's agreement in writing to take the polygraph examination (FD-328b).

(6) Deleted

EFFECTIVE: 04/29/97

13-22.12.1 Polygraph Examinations of FBI Applicants - Drug Issues (See MIOG, Part I, 67-7.10.1.)

(1) All applicants for permanent employment with the FBI are required to submit to a polygraph examination on specific issues, i.e., those which relate to their trustworthiness and eligibility for a "Top Secret" security clearance (security issues) and those which relate to their use of illegal drugs (drug use) as well as veracity of information furnished on their application. To address questions and concerns regarding use of the polygraph for drug issues, an applicant will be placed in one of three specific categories:

- (a) Passed - No Indication of Deception
 - (b) Failed - Deception Indicated
 - (c) Inconclusive - Unable to Determine Results
- (2) Concerns raised regarding use of the polygraph to

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 199

address drug use and/or results of drug use examinations predominantly are associated only with the second category--those cases in which an applicant failed the examination. Cases involving a failed polygraph examination on drug use will be readily categorized as follows:

(a) Failed - Subsequently Admitted Deception - Drug Use EXCEEDS FBI Suitability Standards

(b) Failed - Subsequently Admitted Deception - Drug Use DOES NOT EXCEED FBI Suitability Standards

(c) Failed - Denies Deception

(3) Applicants whose polygraph results fall into the first category above merit NO further consideration for employment. These applicants do not meet FBI suitability standards regarding drug use.

(4) Applicants who fall into the second category above are NOT eligible for further applicant processing. A lack of candor displayed by an applicant during the polygraph phase warrants their disqualification. Each applicant should be advised of the significance of candor during the applicant process and advised to tell the truth prior to their polygraph examination.

(5) Applicants whose drug use polygraph examination results fall into the last category, "Failed - Denies Deception," warrant particular review. In those instances in which an applicant fails the polygraph on drug use issues and maintains that he/she has told the truth and can offer no explanation for the deceptive outcome of his/her polygraph, the FBI will take the following action:

(a) On-Board Support Personnel Applying for the Special Agent (SA) Position: When an on-board support employee fails a polygraph examination regarding drug use issues, that fact must be reported to the Office of Professional Responsibility (OPR) so that an appropriate inquiry may be conducted. In such cases, the employee will be required to submit to an interview conducted under the auspices of an OPR investigation regarding his/her use of, or other association with illegal drugs, and a signed sworn statement will be taken from the employee regarding his/her involvement in the illegal use of drugs. In addition, OPR will conduct appropriate investigation to determine if the employee has used illegal drugs post-employment with the FBI and/or used illegal drugs preemployment and failed to disclose the exact nature or extent of that use to the FBI. During the course of the OPR inquiry, the employee will be required to again

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 200

submit to a polygraph examination regarding drug use. The second polygraph examination will be conducted by a polygrapher other than the individual who administered the first examination. If the employee fails the second examination, the administrative inquiry will continue, as may be appropriate, in accordance with current FBI policy in such matters and no further processing for the SA appointment will be conducted. If the employee passes the second polygraph examination regarding drug use and has not admitted deception on the prior examination or involvement with or use of illegal drugs previously unknown to the FBI, OPR will complete its inquiries and forward its findings to the Adjudication Unit. Upon adjudication, SAAU will once again consider the employee for the SA position.

(b) Outside Applicants Who Fail the Polygraph Examination regarding Drug Use and Deny Deception: Individuals who seek FBI employment and fail their polygraph examination regarding drug use will be disqualified from further consideration except in limited circumstances. Each applicant will be advised by the Personnel Division of the results of his/her examination and whether he/she has been determined eligible for further processing.

(6) If an applicant from outside the FBI fails the polygraph, and maintains that he/she has not been deceptive, he/she may request to be considered for further applicant processing. This request should be sent by the applicant directly to the FBIHQ division head or SAC that previously has been sponsoring the applicant's employment application. If deemed appropriate by the FBIHQ division head or SAC, the applicant should be thoroughly interviewed regarding his/her use/involvement with illegal drugs. This interview should be conducted by an experienced Special Agent other than the polygrapher or SA previously involved in processing the applicant for employment. The result of that interview must be documented in detail in an FD-302. It will be the responsibility of an FBIHQ division head or SAC to personally review the applicant's file to determine if further consideration is warranted on the merits of the case. An FBIHQ division head or SAC may submit a written recommendation to the Personnel Division to request that an applicant be given a second polygraph on the basis of the information developed subsequent to the polygraph examination. Such information should, of course, provide a basis justifying the applicant's reexamination. To ensure consistency and equity in decisions to afford such applicants further consideration, the Deputy Assistant Director - Personnel Officer, Personnel Division, will be responsible for approval of the decision to afford an outside applicant a second polygraph examination.

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 201

EFFECTIVE: 04/29/97

13-22.13 Polygraph Examinations of FBI Employees

In addition to other pertinent requirements, the following policy applies to all polygraph examinations of Bureau employees.

EFFECTIVE: 01/11/85

13-22.13.1 Polygraph Examinations of FBI Employees Who Are Required to Submit to an Employee Interview (See MIOG, Part I, 263-6(3); II, 13-22.10(2), 13-22.13.2(1), (3), 13-22.13.4(1), (3), 13-22.14(2)(c); MAOP, Part I, 1-20(2)(e), 13-4.1.)

(1) When approved in accordance with 13-22.14, an employee who is required to submit to an employee interview may be requested to submit to a polygraph examination. The Bureau may draw an adverse inference from an employee's refusal to submit to such a polygraph examination, provided that such refusal alone shall not be the sole basis for disciplinary action against the employee.

(2) In the case of a security clearance adjudication, an employee's refusal to submit to a polygraph examination has the effect of denying the Security Programs Manager (SPM) the ability to complete a favorable security adjudication on the trustworthiness of the employee. The inability of the SPM to make an affirmative finding of trustworthiness will result in the revocation of an employee's Top Secret (TS) security clearance. Since a TS security clearance is a condition of employment, the FBI Personnel Officer is simultaneously advised of the revocation decision and thereafter the employee is dismissed from the rolls of the FBI.

(3) The following requirements must be satisfied if an employee is requested to submit to a polygraph examination pursuant to (1) and (2) above:

(a) The polygraph examination must be conducted in accordance with Bureau regulations for employee interviews;

(b) The employee must be advised of the consequences of a refusal to submit to a polygraph examination, and that failure to

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 202

satisfactorily cooperate during a requested polygraph examination will be considered a refusal to submit to an examination;

(c) Prior to the examination, the examiner will obtain the examinee's agreement to be examined or polygraph (FD-328a, Employee Agreement To Interview With Polygraph In Connection With An Administrative Interview); and

(d) The investigation must concern a serious violation of law or policy involving one or more of the following situations:

1. The intentional and unauthorized release of sensitive protected information (including, for example, classified information, investigatory material and information, the disclosure of which is prohibited by law or regulation) with the reasonable expectation that it would ultimately be disclosed to those from whom the information is protected and would seriously and adversely affect an FBI function;

2. Serious questions concerning an employee's relationship with or allegiance to a foreign power;

3. The illegal or improper exercise of influence, coercive or otherwise, by an individual or group on an employee which could reasonably be expected to seriously affect or inhibit the employee in the impartial and effective performance of the employee's duties; or

4. The intentional and unauthorized destruction, mutilation, alteration, misplacement, taking, falsification, or other impairment of previously existing Bureau documents or evidence in the Bureau's possession or control.

5. Use of or unauthorized dealing in controlled substances, as defined under the Comprehensive Drug Abuse and Controlled Substances Act of 1970, Title 21, United States Code, by Bureau employees during the course of their employment.

6. The furnishing of false statements or the failure to candidly disclose information concerning prior criminal activities requested during the course of his/her employment processing. (See MIOG, Part II, 13-22.13.4.)

7. Allegations, evidence or indications of theft, fraud and/or misuse involving money, credit cards, securities

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 203

and/or property belonging to, or in the possession of or under the control of the United States Government.

EFFECTIVE: 10/13/95

13-22.13.2 Polygraph Examinations of Bureau Employees Who Are Subjects of Criminal Investigations

A polygraph examination may be given to an employee who is the subject of a criminal investigation if the following requirements are satisfied:

(1) If the employee is required to submit to the interview then the polygraph examination given in conjunction with the interview shall be governed by the policies set forth in 13-22.13.1 above.

(2) If the allegations involve violations of Federal statutes within the Bureau's investigative jurisdiction, and the employee is not being required to submit to the interview but is doing so voluntarily, a polygraph examination may also be given if each of the following conditions are satisfied:

(a) Current Bureau regulations and procedures for employee interviews are observed;

(b) Current Bureau regulations and procedures applicable to polygraph examinations in criminal investigations are observed;

(c) The employee is requested to submit to a polygraph examination only in circumstances in which a nonemployee would be requested to submit to a polygraph examination; and

(d) The employee agrees to take the examination (FD-328, Consent to Interview With Polygraph).

(3) If the allegations involve violations not within the Bureau's investigative jurisdiction, polygraph examinations may only be given pursuant to 13-22.13.1 or 13-22.13.3.

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 204

EFFECTIVE: 08/17/84

13-22.13.3 Voluntary Polygraph Examination of Employees

An employee may be asked or an employee may ask to undergo a polygraph examination in the following circumstances:

(1) If the employee is the subject of an FBI criminal investigation, the use of the polygraph shall be governed by the policies set forth in 13-22.13.2.

(2) If the employee is not the subject of an FBI criminal investigation, and the employee is not being required to submit to an employee interview, but is doing so voluntarily, then the employee may also be asked to submit to the interview in the form of a polygraph examination, or the employee may ask for the examination if the following requirements are satisfied:

(a) The employee must be advised that the examination is totally voluntary; that the employee may change the decision at any time without any disciplinary action being taken or adverse inference being drawn;

(b) The employee must signify in writing that he or she is voluntarily submitting to the polygraph examination by executing FD-328, (Consent To Interview With Polygraph); and

(c) FBI regulations and procedures for employee interviews must be observed.

EFFECTIVE: 08/17/84

13-22.13.4 Routine and Periodic Use of Polygraph Examinations for Bureau Employees

(1) Except as provided in 13-22.13.4, routine polygraph examinations of employees not suspected of being involved in any of the situations listed in 13-22.13.1 (2)(d) are prohibited.

(2) Employees who are subjected, or whose circumstances suggest that they could be subjected, to extremely coercive influences by an individual or group may be requested to submit to a polygraph

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 205

examination on a periodic basis to determine if the coercive influences are significantly affecting the performances of their duties. Coercive influences include, but are not limited to, relative-hostage situations, extortion, blackmail, and similar circumstances where it is reasonable to believe that the individual or group could significantly influence the employee's work performance.

(3) Polygraph examinations authorized by 13-22.13.4 shall be conducted consistent with the procedures and policies set forth in 13-22.13.1.

EFFECTIVE: 08/17/84

13-22.14 Approval and Conduct of Employee Polygraph Examinations
(See MIOG, Part I, 263-6(3); II, 13-22.3, 13-22.13.1;
MAOP, Part I, 13-4.1.)

(1) All polygraph examinations of FBI employees and those who have made allegations against FBI employees must be approved by the Assistant Director, Inspection Division, or another person designated by the Director. In the case of polygraph examinations requested pursuant to a security clearance adjudication, the Director has delegated approval authority to the Assistant Director, National Security Division.

(2) The following standards apply for approval of polygraph examinations:

(a) No employee may be requested or asked to submit to a polygraph examination without an adequate demonstration of facts or circumstances indicating the need for a polygraph examination of that individual.

(b) All reasonable efforts must be made to resolve allegations or questions before requesting an employee to submit to a polygraph examination.

(c) Before any employee is requested to submit to a polygraph examination, the refusal of which may be used as a factor in determining whether the employee will be subjected to disciplinary action (13-22.13.1), there must be a substantial objective basis to suspect that the individual may be involved in one of the situations

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 206

| listed in 13-22.13.1.

| (d) |Employees| who are requested or asked to submit to polygraph examinations will be fully advised of their options and the potential consequences of the exercise of those options.

(3) Use of the results of polygraph examinations.

(a) Disciplinary action will not be predicated solely upon the results of a polygraph examination, or upon the refusal to submit to a polygraph examination. (See (d).)

(b) The results of a polygraph examination may be considered with other evidence.

(c) Employees will be furnished the results of a polygraph examination prior to being subjected to any disciplinary action based in part on the results of the examination.

(d) An employee's refusal to submit to a polygraph examination in the case of a security clearance adjudication has the effect of denying the Security Programs Manager (SPM) the ability to complete a favorable security adjudication on the trustworthiness of the employee. The inability of the SPM to make an affirmative finding of trustworthiness will result in the revocation of an employee's Top Secret (TS) security clearance. Since a TS security clearance is a condition of employment, the FBI Personnel Officer is simultaneously advised of the revocation decision and thereafter the employee is dismissed from the rolls of the FBI.

(e) The results of a polygraph examination may be maintained with the records resulting from the investigations. Dissemination of such information shall be strictly limited to persons who have a legitimate right or requirement for access to the information.

(f) Deliberate or negligent misuse of the results of polygraph examinations shall be grounds for administrative action.

(4) Polygraph examination of employees will be administered away from their own office of assignment. This procedure will help protect the confidentiality of the inquiry/investigation and lessen the outside pressure on the employee which could be associated with employee's friends' and associates' knowledge of employee's participation in examination. (See MIOG, Part I, 263-6(2); MAOP, Part I, 13-4.1.)

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 207

(5) Polygraph examinations of Bureau employees are to be administered by an FBIHQ examiner. In the event an FBIHQ examiner is not available, the examination will be conducted by an examiner selected by FBIHQ.

EFFECTIVE: 10/13/95

13-22.15 Selection, Training, and Certification of Polygraph
Examiners

Requirements have been established to ensure that Bureau examiners meet the highest standards of integrity, competence, and professional excellence.

EFFECTIVE: 11/23/87

13-22.15.1 Selection and Training of FBI Polygraph Examiners

(1) To meet future needs for polygraph examiner trainees, a pool of candidates will be maintained by FBIHQ from which trainees will be selected. Any Agent interested in being trained in this investigative specialty should submit a memorandum to the SAC who will forward the requesting memorandum, with personal recommendations, to FBIHQ, Attention: Laboratory Division. Interested Agents should indicate if they are willing to accept transfer or if they desire consideration only for their current division.

(2) When vacancies occur, trainees will be selected by an FBIHQ selection board, in coordination with affected SACs.

(3) No Agent will be transferred to fill a polygraph examiner vacancy without his/her prior concurrence.

(4) Prior to selection, Agents will be interviewed by the selection board at FBIHQ and undergo a nonspecific polygraph examination.

(5) The following factors will be evaluated in selection of Agents to receive polygraph examiner training.

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 208

- (a) At least five years' investigative experience
- (b) Experience and demonstrated success as interviewer/interrogator and as case Agent in complex investigations
- (c) Ability to perform well under stress and in confrontational situations
- (d) Availability for travel to conduct examinations in other divisions and throughout own field office territory as required (should NOT be in a hardship assignment or have medical mandates (restrictions) that would prohibit the employee from required travel.)
- (e) Good judgment, maturity, dependability, self-motivation, and ability to work well alone should be clear attributes of Agent
- (f) Willingness to be assigned to a headquarters city office, devote full time to polygraph examiner duties, and forego involvement in other collateral/coordinator-type activities.

(6) Agents selected for the program will complete the Polygraph Examiners Training Course at the Department of Defense Polygraph Institute, Fort McClellan, Alabama. The course, which is approximately 14 weeks in length, includes instruction in polygraph theory and procedures, psychology, physiology, semantics, question formulation, instrumentation, and legal matters related to polygraph. During the course students also conduct 50 polygraph examinations of persons who participate in mock crime situations.

EFFECTIVE: 12/27/93

13-22.15.2 Certification of Examiners

To be certified as an FBI polygraph examiner the following must be satisfied:

- (1) The examiner must be a graduate of a Bureau-approved polygraph school.
- (2) The examiner must successfully complete an internship consisting of conducting a minimum of 12 examinations with supervision

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 209

of a certified Bureau examiner.

(3) The continued demonstration of proficiency in the polygraph techniques.

(4) The examiner should, if possible, conduct a minimum of 48 examinations per year. Examiners assigned duties in direct support of the FBI's quality control program at FBIHQ are exempt.

(5) The examiner should attend at least one FBI polygraph in-service training course or Bureau-approved polygraph refresher course or seminar at least every two years.

(6) Any examiner who has lost the requirements for certification can be recertified by successful completion of a Bureau-approved refresher course. In addition, the examiner being recertified will be required to conduct a minimum of 12 examinations under the supervision of an FBI certified examiner. Upon the completion of the above, the FBI certified examiner supervising the examiner for recertification will, in writing, forward his/her recommendations as to recertification to FBIHQ.

EFFECTIVE: 11/23/87

13-22.15.3 Refresher Training and Polygraph Seminars

Requests to attend refresher training courses, polygraph seminars, and/or meetings of professional polygraph associations should be handled in the following manner:

(1) Submit requests (Optional Form 170) along with appropriate details to FBIHQ, Attention: Polygraph Unit.

(2) Expenses incurred in conjunction with approved attendance at such functions are to be claimed on an expense voucher.

(3) Pertinent information gleaned at meetings, especially results of polygraph research, should be furnished to FBIHQ for possible distribution to all Bureau examiners.

EFFECTIVE: 12/19/86

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 210

13-22.15.4 Performance Appraisal

(1) Field polygraphers have been assigned two critical elements by which their performance as polygraph examiners is evaluated. Because of the uniqueness of their responsibilities, i.e., frequently serving more than one field division and the review of each examination both technically and procedurally through a mandated quality-control process, these particular elements are rated and reviewed by Supervisory Special Agent Polygraph Examiners assigned to FBIHQ. This procedure does not preclude, at the SAC's discretion, the addition of critical elements generated by field offices reflecting other duties and responsibilities handled by their assigned polygraphers.

(2) Only the critical elements relating to polygraph performance will be rated and reviewed by FBIHQ. If additional elements are established by the field office, they are to be rated and reviewed by appropriate field supervisors. All critical elements (the two prepared for the Polygraph Program and any prepared by the field) will be combined to determine the overall rating of the employee prior to forwarding the performance appraisal to the Performance, Recognition and Awards Unit, Personnel Division.

EFFECTIVE: 04/21/94

13-22.15.5 Voice-Stress Devices Prohibited

Use of voice-stress devices to determine the truthful or deceptive nature of a person's oral statements is prohibited. Only Bureau-approved polygraph examiners using true polygraph instruments designed to record at least three physiological parameters including respiration, heart rate/blood pressure, and galvanic skin response (GSR), are authorized to conduct detection of deception examinations.

EFFECTIVE: 12/19/86

13-23 TRANSLATION POLICY (See MAOP, Part I, 22-6.)

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 211

EFFECTIVE: 09/08/93

| 13-23.1 | Deleted |

EFFECTIVE: 09/08/93

| 13-23.2 | Deleted |

EFFECTIVE: 09/08/93

| 13-23.3 | Deleted |

EFFECTIVE: 09/08/93

| 13-23.4 | Deleted |

EFFECTIVE: 09/08/93

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 212

13-24 ARTIST CONCEPTIONS

Consideration should be given to the preparation of artist conception portrait drawings of unknown subjects in selected Bureau cases. These sketches are prepared by Visual Information Specialists (VIS) at Headquarters from "look-alike" reference photos selected from the FBI Facial Identification Catalog and other descriptive data furnished by witnesses or victims.

EFFECTIVE: 12/10/91

13-24.1 Policy

EFFECTIVE: 12/10/91

13-24.1.1 General | (See MIOG, Part II, 13-25.1.1(1).)

(1) Because of a limited staff of VIS, requests for artist conceptions other than those where the FBI has investigative jurisdiction must be approved on the merits of each individual request by Assistant Director of the Laboratory Division.

(2) In most instances, VIS prepare drawings from descriptive data transmitted to Special Projects Section via facsimile machine. If special handling is requested, a composite drawing can be completed in 2-4 hours. On cases of national import, consideration will be given to sending the VIS to the field location. A composite drawing prepared during a hypnosis session would be one such instance. VIS will participate in accordance with Bureau policy governing use of hypnosis as an investigative aid.

(3) Offices utilizing Identi-Kits or other automated systems can have these composites modified or redrawn according to specifications submitted by field office. Although the Identi-Kit cannot duplicate the skill and versatility provided by the VIS in the illustration of a facial likeness, it can serve a useful purpose as one of the methods Bureau offices can employ to prepare composites if the VIS cannot respond within time limits the field investigation in progress requires.

(4) As the investigation progresses, the Laboratory,

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 213

Attention: Special Projects Section, should be advised of the use and effectiveness of the drawing as an investigative aid.

EFFECTIVE: 06/26/96

13-24.1.2 Dissemination

(1) The SAC may approve releasing Bureau prepared artist conceptions for publication by the news media in unknown subject cases in which the witnesses have stated the drawing is an excellent likeness to the unknown subject. After approval is received, file numbers and issue date information must be removed from the prints prior to releasing them. This is done by cutting off the bottom portion of each print.

(2) FBIHQ approval is required before an artist conception can be used in a circular letter.

EFFECTIVE: 08/16/82

13-24.1.3 Administrative Identification

All artist conceptions should, whenever possible, carry a Bureau file number, field office file number, and the date that the drawing was issued. This data will appear at the very bottom of the photographic prints of these drawings and may, if desired, remain on these prints while they are used for investigative purposes. The data must remain on the prints when they are produced as evidence at trial.

EFFECTIVE: 08/16/82

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 214

13-24.2 Requesting an Artist Conception

(1) The "look-alike" references from the FBI Facial Identification Catalog are recorded on an FD-383 (Facial Identification Fact Sheet) which, along with other detailed descriptive or illustrative material, is forwarded to the Laboratory, Attention: Special Projects Section. Requests should be limited to those cases in which the witnesses can provide detailed descriptions, have selected a sufficient number of characteristics from the Facial Identification Catalog, and be reasonably confident they can recognize a likeness of the unknown subject if a sketch is produced.

(2) All offices and resident agencies having a facsimile device should consider using this device for transmitting the FD-383 and related reference material directly to the Laboratory, Attention: Special Projects Section, between 8:00 a.m. and 5:30 p.m., Washington, D.C., time. The telephone number of this facsimile in the Special Projects Section is [REDACTED] Contact FBIHQ during other hours. ba

(a) Use of the facsimile device will ensure expeditious handling of the request.

(b) Also, use of FTS line can provide a direct communication between the artist and the interviewing Agent or witness when necessary.

EFFECTIVE: 08/16/82

13-24.3 Results of Request

(1) The drawing will be prepared in the Special Projects Section in the shortest possible time existing priorities permit, and transmitted to the requesting office by facsimile device for evaluation by the witnesses. Revisions may be requested by the field as needed until a good likeness is developed.

(2) Three polaroid copies of the drawing will be sent to the requesting office by routing slip on the same date as the facsimile transmission. If more than three Polaroid copies are deemed necessary, they may be made using field office facilities or from suitable local sources after approval of the likeness by the witnesses. If the extra copies cannot be obtained in the field, they may be ordered from the Laboratory, Attention: Special Projects Section.

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 215

EFFECTIVE: 03/23/92

13-25 FACIAL AGING

Consideration should be given to the preparation of facially aged photographs of children and adults, using a computerized aging system located at FBI Headquarters. These aged photographs are prepared by Visual Information Specialists (VIS) of the Laboratory Division.

EFFECTIVE: 03/23/92

13-25.1 Policy

EFFECTIVE: 03/23/92

13-25.1.1 General

(1) As set forth in the policy statement for Artist Conceptions, (13-24.1.1) requests for facial aging must be restricted to those cases where the Bureau has jurisdiction. Any exceptions must be approved by the Assistant Director of the Laboratory Division.

(2) In situations requiring a child's photograph to be aged/updated, photographs of a parent, brother, or sister are requested as they may be scanned into the system and incorporated with the victim's photograph to produce the aged or projected image of how the child is likely to appear.

(3) A similar methodology is used in aging adult subjects; however, family photographs are generally not incorporated with the subject to achieve the aged image. The addition of facial lines and hair, increase or decrease in body weight, and a change of hairstyle are the most common factors used in this process, and these are borrowed from other facial images available to the artist.

(4) The value of this technique lies in the fact that when the computer system is used by an experienced artist, the rendering is more technically accurate than those produced entirely by

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 216

hand, and it can be produced much faster.

(5) In some instances, it may be advisable or necessary for the Bureau artist to accompany the case Agent in interviews with the victim's family.

EFFECTIVE: 06/26/96

13-25.2 Administrative Identification

All aged photographs should, whenever possible, carry a Bureau file number, and the date that the photograph was issued. This data will appear at the very bottom of the photographic prints and may, if desired, remain on these prints while they are used for investigative purposes. The data must remain on the prints when they are produced for, or used as, evidence at trial.

EFFECTIVE: 03/23/92

13-25.3 Requesting a Facially Aged Photograph

In order to ensure the accuracy with which a photograph may be aged, the requesting office should submit several of the highest quality photographs available of the victim/subject, as well as all pertinent descriptive data regarding the victim/subject, i.e., date of birth, facial characteristics, etc. This information should be forwarded to the Laboratory Division, Attention: Special Projects Section by an FD-790 (Special Projects Section Work Order).|

EFFECTIVE: 03/23/92

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 217

13-25.3.1 Results of Request

(1) The aged photograph will be prepared in the Special Projects Section in the shortest possible time existing priorities will permit. Revisions may be requested by the field as needed until a projected likeness is developed.

(2) One black and white, 4" x 5" photographic print of the aged rendering will be shipped to the requesting office. If more than one print is deemed necessary, they may be made using field office facilities or from a suitable local source. If the extra copies cannot be obtained in the field, they may be ordered from the Laboratory Division, Attention: Special Projects Section.

EFFECTIVE: 03/23/92

13-26 VISUAL AIDS

The Special Projects Section, Laboratory, has the ability to design and prepare visual aids for investigative and prosecutive assistance, law enforcement training, as well as for administrative and informational purposes. (For information concerning artist conception portrait sketches, see paragraph 13-24 above.)

EFFECTIVE: 03/23/92

13-26.1 Requests

EFFECTIVE: 03/23/92

13-26.1.1 From FBIHQ

All requests from FBIHQ must be directed to the Special Projects Section by an FD-790 (Special Projects Section Work Order).

EFFECTIVE: 03/23/92

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 218

13-26.1.2 From the Field

All requests from the field must be directed to the FBIHQ Laboratory Division by an FD-790 to the attention of the Special Projects Section and must contain the the following:

- (1) A general description of the work requested
- (2) The purpose and its use
- (3) All available reference and explanatory data, and
- (4) A sketch, if applicable, which does not have to be drawn to scale but must contain detailed measurements.
 - (a) If the request is for an investigative or prosecutive aid, it is to be submitted to the appropriate substantive investigative desk at FBIHQ for approval.
 - (b) Deleted
- (5) The case caption and file number if applicable.

EFFECTIVE: 09/03/93

13-26.2 Drawings

- (1) Two-dimensional visual aids include prosecutive and investigative aids such as:
 - (a) Street map for locating evidence, buildings, witnesses or routes.
 - (b) Plat map for locating evidence, buildings, subjects or witnesses.
 - (c) Terrain map showing wooded areas or other physical features.
 - (d) Combination map and photographic display to illustrate appearance of specific areas.
 - (e) Floor plan for locating evidence or movement of

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 219

subjects.

(f) Diagram to explain check-kiting, telephone contacts or organizational structures.

(g) Statistical charts, graphs and bar charts.

(h) Enlargement of accounting papers or bank forms.

(2) Drawings will be prepared from information furnished or if the situation warrants, from on-the-scene data collected by FBIHQ personnel. Source material that can be used by the Special Projects Section as reference for preparing the drawings can often be found at municipal and other government offices.

(a) Floor plans at building inspector.

(b) Plat plans at tax assessor.

(c) Street and curb plans at highway department.

(d) Maps at U.S. Geological Survey.

(3) All source material must be verified for accuracy before submission.

EFFECTIVE: 03/23/92

||13-26.3| Models (Three-Dimensional)

(1) When deemed essential and approved by FBIHQ, a three-dimensional model can be prepared in major cases. The model will be constructed from measurements, photographs, and on-the-spot observations made by FBIHQ personnel to ensure authentication for the admittance of the model as evidence.

(2) The construction of three-dimensional models for use in aiding the United States Attorney to present his/her case are limited to instances when a clear illustration of the facts cannot be achieved with a two-dimensional chart. In most instances they are prepared to scale and are necessarily constructed from data collected on the scene by the VIS from Special Projects Section.

(3) The cost of preparing the three-dimensional trial

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 220

model limits its use to major cases or those where alternate means of illustration cannot be used to supply a vital point to the prosecution of the case. Circumstances often falling within these guidelines include:

(a) Sections covering two or more physical levels such as between floors of a building or decks of a ship.

(b) A replica of a mechanical device which cannot be transported to the courtroom.

(c) A reproduction of terrain showing altitudes and distances.

(4) Requests for models should be made reasonably soon after occurrence of the crime to enable the VIS to construct the model to represent the scene accurately at time crime was committed.

EFFECTIVE: 05/26/89

||13-26.4| Special Investigative Equipment

Special equipment or enclosures can be constructed with approval of FBIHQ.

EFFECTIVE: 05/26/89

||13-26.5| Special Surveillance Graphics

With approval of appropriate FBIHQ substantive desk, a variety of graphic items can be designed and prepared as a comprehensive package to assist in the staging and operation of special surveillance activities.

EFFECTIVE: 05/26/89

||13-27| RADIATION HAZARDS

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 221

EFFECTIVE: 05/26/89

||13-27.1| Introduction

Radioactive materials are in use in the nuclear power industry, nuclear weapons industry, academic and industrial research environments and in medicine. Accidents, death and injuries resulting from the handling and transportation of radioactive materials have been few; however, the role of radioactive materials in a terrorist incident, an extortion or a theft presents a special hazard to the investigator. Radiation is invisible and insensible; therefore, special knowledge about it will enable the investigator to intelligently evaluate its hazard.

EFFECTIVE: 05/26/89

||13-27.2| Terminology

EFFECTIVE: 05/26/89

||13-27.2.1| Atoms

Atoms are small particles of matter which have the characteristics of an element. For example, gold and silver are both elements and the smallest particle of gold or silver which can be identified as gold or silver is an atom of gold or an atom of silver.

EFFECTIVE: 05/26/89

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 222

||13-27.2.2| Isotopes

Isotopes are varieties of the same element which have the same chemical properties but have a different nuclear structure and therefore different physical properties. For example, we have three isotopes of hydrogen; namely, Hydrogen One, Hydrogen Two and Hydrogen Three.

(1) Stable isotopes are ones which are incapable of spontaneous change and thus are not radioactive.

(2) Unstable isotopes undergo spontaneous changes and emit nuclear radiations.

EFFECTIVE: 05/26/89

||13-27.3| Nuclear Radiations

Nuclear radiations involve the emission of energy or particles from a nucleus.

EFFECTIVE: 05/26/89

||13-27.3.1| Alpha Particle

Alpha particle is a positively charged particle emitted from a nucleus and similar to a helium nucleus. It has a relatively large mass with low penetrating power and a short range. Alpha particles will usually not penetrate the skin but danger occurs when alpha emitters are introduced into the lungs or intestines.

EFFECTIVE: 05/26/89

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 223

||13-27.3.2| Beta Particle

Beta particle is a high speed negatively charged electron emitted from a nucleus. It has little mass, low penetrating power and a short range. The more energetic particles will penetrate the skin. Danger is due to skin burns and internal damage if the emitter enters the body and lodges in a body organ.

EFFECTIVE: 05/26/89

13-27.3.3 Gamma Ray

Gamma ray is a unit of radiation energy similar to, but more energetic than, X-rays. Gamma rays can do body damage even when the source is located outside of the body due to their penetrating power.

EFFECTIVE: 07/25/97

13-27.3.4 Neutron

Neutron is a subatomic particle which has no electrical charge and it is one of two principal particles in the nucleus.

EFFECTIVE: 07/25/97

||13-27.4| Radiation Effects

Nuclear radiations avoid detection by all our senses. Excessive dosages are normally hazardous. Police activity in or around radiation areas requires special vigilance. Radiation hazards are usually considered as either external or internal hazards.

EFFECTIVE: 05/26/89

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 224

||13-27.4.1| External Hazards

Bodily damage can result from overexposure to gamma rays even though the radioactive material is outside the body. Gamma rays are external hazards.

EFFECTIVE: 05/26/89

||13-27.4.2| Internal Hazards

Bodily damage can result if radioactive material emitting alpha and beta particles contaminates our food or the air we breathe and in this manner is taken into our bodies in excessive amounts. Alpha and beta particles are considered internal hazards.

EFFECTIVE: 05/26/89

||13-27.5| Detection Equipment

EFFECTIVE: 05/26/89

||13-27.5.1| Survey Meters

Survey meters are portable instruments designed to enable one to evaluate a particular radiation. They may be designed to detect and measure alpha, beta and gamma radiation and are used for the evaluation of contaminated foods and water. Survey meters read either in roentgens/hour or milliroentgens/hour (1,000 milliroentgens = 1 roentgen).

EFFECTIVE: 05/26/89

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 225

||13-27.5.2| Dosimeters

Dosimeters are pocket-size instruments used to measure the total beta-gamma dosage accumulated by the person wearing the dosimeter. Some dosimeters can be read at any time by the wearer (self-reading dosimeters). Other dosimeters, such as film badges are not self-reading. These latter-type dosimeters are processed in a laboratory. Dosimeter readings are normally in roentgens or milliroentgens.

EFFECTIVE: 05/26/89

||13-27.6| Significance of Detection Equipment Readings

EFFECTIVE: 05/26/89

||13-27.6.1| Roentgen

Roentgen is a standard unit of measure of the energy of X-ray or gamma radiation which is absorbed. Often the term milliroentgen, which is one thousandth part of a roentgen, is used. The following table is a listing of radiation doses and their effects.

Acute Dose (roentgens)	Probable Effect of Total Body Dose
0 to 50	No obvious effect, except possibly minor blood changes.
80 to 120	Vomiting and nausea for about 1 day in 5 to 10 percent of exposed personnel. Fatigue but no serious disability.
130 to 170	Vomiting and nausea of about 1 day, followed by other symptoms of radiation sickness in about 25 percent of personnel. No deaths anticipated.
180 to 220	Vomiting and nausea for about 1 day, followed by other symptoms of radiation sickness in about 50 percent of personnel. No deaths anticipated.

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 226

270 to 330	Vomiting and nausea in nearly all personnel on first day, followed by other symptoms of radiation sickness. About 20 percent deaths within 2 to 6 weeks after exposure; survivors convalescent about 6 months.
400 to 500	Vomiting and nausea in all personnel on first day, followed by other symptoms of radiation sickness. About 50 percent deaths within 1 month; survivors convalescent for about 6 months.
550 to 750	Vomiting and nausea in all personnel within 4 hours from exposure, followed by other symptoms of radiation sickness. Up to 100 percent deaths; survivors convalescent for about 6 months.
750 to 1000	Vomiting and nausea in all personnel within 1 to 2 hours. Probably no survivors from radiation sickness.
1000 to 5000	Incapacitation almost immediately. All personnel will be fatalities within 1 week.

EFFECTIVE: 05/26/89

13-27.7 Radiation Protection

The following factors should be considered when evaluating available protection.

(1) If all containers of radioactive material are sealed or closed and are INTACT it is unlikely that radioactive hazards are associated with the incident. Efforts should be made to protect the integrity of the containers during essential rescue, salvage and clean-up operations.

(2) If radioactive isotopes become loose from the container or are liberated by a handling accident the following

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 227

factors should be understood.

(a) DISTANCE. The distance between individuals and the isotope source appreciably decreases radiation intensity with this reduction being described by an "inverse R squared" relationship. In most cases, for example, the distance of 2 feet from the source will decrease the radiation to one-quarter its value at 1 foot; a distance of 10 feet from the source will decrease the radiation to one-hundredth its value at 1 foot.

(b) TIME. The time one spends in the radiation field should be kept to an absolute minimum. A 2-hour exposure in a radiation field will be twice as large as a 1-hour exposure.

(c) SHIELDING. Dense materials such as steel, concrete and dirt between the individual and the source can cut down the intensity of gamma radiation. Most gamma-emitting radioisotopes emit radiation of less than one million electron volts per gamma ray. Generally, the radiation may be cut in half by 1 1/2 inches of steel, 4 1/2 inches of concrete, 7 1/2 inches of earth, or 10 inches of water.

(d) CONTAINMENT. Restriction of the radioisotopes to a limited area will help to establish boundaries for the hazard. Efforts should be made to keep the radioisotopes from scattering. If there is a fire associated with an incident, high pressure hoses might break open containers and widely distribute the radioisotopes. Vehicles and individuals repeatedly entering the area could track away any radioisotopes from incidents involving spills of radioactive materials. Such travel should be limited to that which is absolutely necessary.

(3) External and/or internal hazards can be present whenever radioactive materials are found. If it is not known what the hazards are, assume both to be present. To protect against internal hazards, personnel should wear breathing masks or some type of filter system over the nose or mouth. If possible, all personnel should be kept upwind from the scene of the incident and all smoking and eating should be prohibited in the restricted area. Personnel entering the area where there is radioactive dust should be wearing disposable or washable outer clothing.

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 228

EFFECTIVE: 07/25/97

13-27.8 Emergency Procedures for Accident or Incident

(1) Keep all but essential rescue and investigative personnel away from the immediate accident scene.

(2) Report the accident or incident immediately to the nearest Department of Energy facility or military base, whichever is appropriate.

(3) | Contact the Strategic Information Operations Center (SIOC) at FBIHQ, which will in turn contact the Hazardous Materials Response Unit (HMRU) of the Laboratory Division. |

| (4) | Keep sightseers away - 500 yards or more, if possible.

| (5) | Stay out of smoke or vapors if there is fire.

| (6) | Hold people who may have been exposed to the contamination in an area for appropriate examination by emergency personnel.

| (7) | Do not fight fires involving explosives except under the direction of an expert.

| (8) | Do not permit the taking of souvenirs.

| (9) | Keep unauthorized personnel from entering the scene.

EFFECTIVE: 07/25/97

| 13-28 | DELETED |

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 229

EFFECTIVE: 03/21/95

| 13-28.1 | Deleted |

EFFECTIVE: 03/21/95

| 13-28.2 | Deleted |

EFFECTIVE: 03/21/95

| 13-29 | MOVED TO 13-7.6.1 |

EFFECTIVE: 07/25/97

| 13-29.1 | Moved to 13-7.6.1 |

EFFECTIVE: 07/25/97

| 13-29.2 | Moved to 13-7.6.1 |

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 230

EFFECTIVE: 07/25/97

13-29.3 Moved to 13-7.6.1

EFFECTIVE: 07/28/97

13-30 COMPUTER ANALYSIS AND RESPONSE TEAM (CART)

EFFECTIVE: 02/28/97

13-30.1 General Information

(1) Since 1984, when the FBI Laboratory began examining computer-based evidence, the widespread use of computers and the rapidly developing technology of computer systems, have combined to dramatically increase the volume and complexity of computer evidence seized by FBI Agents. Today, FBI Agents routinely encounter computers in cases dealing with health care fraud, child pornography, terrorism, murder, drugs, financial institution fraud, public corruption, and in almost every other investigative classification for which the FBI is responsible.

(2) A real danger exists that well-intentioned efforts on the part of untrained field investigators can affect important evidence and may either render it unavailable to the investigator or inadmissible at the time of trial. Another danger is that the FBI will incur some civil liability for damage or destroyed computer data belonging to a subject or a third party. In 1992, the Laboratory Division's Computer Analysis and Response Team (CART) was formed to address these problems.

(3) The primary mission of CART, whether in the field or in the Laboratory, is to provide the investigator who encounters computer evidence with reliable, comprehensive, and timely

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 231

information and technical support necessary to the investigation and prosecution of the case. These mission objectives are met through a mutually supporting task organization consisting of:

(a) A state-of-the-art forensic capability comprised of computer scientists and engineers, CART, centrally located in the Laboratory Division;

(b) A network of specially trained and equipped Field Examiners (FEs), assigned to selected field offices and serving regional requirements.

In a typical case:

1. The case Agent who expects to encounter computer-based information (usually in executing a search warrant) consults with an FE who is trained and equipped to handle most situations. The FE will determine whether or not he/she can operate independently or needs CART HQ assistance.

2. At the search site, the CART Examiner will determine what computer systems should be seized and brought back to the office for examination. If the warrant does not allow the seizure of equipment, the CART Examiner should be able to copy the data onto medium suitable for examination at the field office. CART HQ will be on stand-by to offer consultation should unsuspected circumstances be encountered.

3. After the equipment is seized and transported to the field office, the FE will conduct triage to determine if the examination can be handled in the field office or if all, or part, must be sent to the Laboratory Division for examination. Every effort will be made to examine the evidence in the field office.

4. The FE in consultation with the case Agent will determine what data is necessary from the seized computer and in what format to best present the data.

5. The FE will recover the necessary data using techniques and protocols developed by CART and provided to the FE by CART. These utilities reside on specialized hardware platforms which have also been provided to the FE by CART. The examiner will be familiar with these procedures and trained in their use under CART direction.

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 232

6. At trial, the FE will be able to describe and defend his/her actions. If questions arise regarding the protocols used, CART will provide, when needed, experts who can explain CART's protocols.

(4) FEs are assigned to serve regions. These regions represent the best allocation of resources based on analyses of evidence submissions to CART and in consultation with the Criminal Investigative Division (CID) concerning investigative priorities.

EFFECTIVE: 02/28/97

13-30.2 Authorization/Approval for Conducting Exams/Searches (See MIOG, Part II, 13-30.4.)

(1) No action with respect to original computer evidence should be taken without consulting with one of the certified Computer Analysis and Response Team (CART) Examiners on the field list or CART at FBIHQ. In addition, no review of computer evidence should be performed without the supervision and/or consultation of a CART examiner.

(2) The following guidelines govern requests for CART support:

Any Agent who requires an examination of computer evidence or requires search assistance must contact their regional Field Examiner (FE). During emergency situations, if an FE is not able to be contacted, the CART Program Manager or Unit Chief should be contacted. After hours, contact CART through the FBIHQ switchboard operator. All requests for search assistance or computer examinations must be forwarded as a lead to the appropriate FE by an electronic communication (EC) or teletype. The EC should be sent to the field office of the FE and the Laboratory Division, Attention: CART. The first CASE ID# must be 66-HQ-C1155003 with the second CASE ID# as the substantive Universal Case File Number (UCFN). The EC should be titled "Computer Analysis and Response Team, Field Examiner Operations." If desired, the title of the case may be included as a dual-captioned title or included in the synopsis field of the EC. Whenever possible, FEs should be telephonically contacted prior to sending a written communication and that FE should be named in the attention line of the EC.

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 233

EFFECTIVE: 02/28/97

13-30.3 Responsibilities of the Case Agent

(1) The case Agent is normally the first person to realize that Computer Analysis and Response Team (CART) support may be helpful to the investigation. In this regard, it is important for the case Agent to understand certain aspects of computer evidence searches and examinations and to be fully aware of the existing policies concerning computer evidence searches and examinations. A case Agent has the following responsibilities in connection with computer evidence searches and examinations:

Before an affidavit in support of a search warrant is written, the case Agent should consult with their regional CART Field Examiner (FE) to ensure proper justification is given for seizing the equipment and software needed to properly analyze the seized computer evidence. The case Agent should attempt to identify the types of computers, networks, and operating systems in use at the location to be searched. This will help the FE to determine what assets will be needed to conduct the search and process the evidence. The case Agent should advise the FE as to the types of electronic records believed to be contained on the evidence to be seized. This information is required in determining what equipment should be seized as well as how the examination of the evidence will be conducted.

(2) By providing the above information, the case Agent will maximize the results of the search warrant and ensure the forensic examination of their evidence will proceed in a quick and efficient manner.

EFFECTIVE: 02/28/97

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 234

13-30.4 Submission of Evidence

(1) When it has been determined that evidence needs to be shipped either to a regional Field Examiner (FE) or the FBI Laboratory, the evidence must be processed through the field office's Evidence Control Technician (ECT). The ECT will ensure that proper chain of custody rules are followed. For assistance in packing computer evidence for shipping, the case Agent should contact the ECT in their field office.

(2) The evidence should be accompanied by an electronic communication (EC) as described in MIOG, Part II, 13-30.2, Authorization/Approval for Conducting Exams/Searches.

EFFECTIVE: 02/28/97

13-30.5 Types of Computer Analysis and Response Team Support

(1) The Computer Analysis and Response Team (CART) can provide timely and accurate examinations of computers, diskettes, optical disks, tape backups, and other electronic media. CART can provide on-site field support as needed for execution of search warrants and examinations of computer systems which cannot be sent to a regional Field Examiner (FE) or the FBI Laboratory. CART can also provide on-site consultation with investigators and prosecutors in the development of strategies for the seizure of computer records and equipment. CART examiners will provide testimony as to examination procedures and results.

(2) In addition to the retrieval of records, CART capabilities include but are not limited to the retrieval of deleted, erased, and hidden data, the ability to break passwords and encryption schemes, and the examination of computer code to determine the effect of that code.

EFFECTIVE: 02/28/97

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 235

13-30.6 Field Examiner Program

EFFECTIVE: 02/28/97

13-30.6.1 Selection of Field Examiners

(1) Computer Analysis and Response Team (CART) Field Examiners (FEs) are selected by the CART Program Manager and scientific staff from among candidates nominated by Special Agents in Charge (SACs) based on education, training, experience, desire to participate in the program, and willingness to travel extensively while servicing needs of Bureau offices within the FE's region. Candidates with formal education in science or engineering will be preferred. Investigative skills and experience complement the forensic work and Special Agents are preferred as FEs.

(2) Selectees will have sufficient academic background and experience towards qualifications as an expert witness and to communicate technical matters effectively to nontechnical audiences. They will be technically innovative, demonstrate excellent problem-solving abilities, and be able to work independently. They will be available to devote at least 50 percent of their time to FE-related duties to ensure their special skills are used sufficiently to retain proficiency. They must meet the certification requirements of the Laboratory Division and CART and be able to serve at least two years as an FE.

EFFECTIVE: 02/28/97

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 236

13-30.6.2 Training and Certification of Field Examiners

(1) Continuous education and training will be provided by the Laboratory Division's Computer Analysis and Response Team (CART) in the form of yearly in-service courses, commercially available training at the Field Examiner's (FE) home city, unique law enforcement courses provided by such professional organizations as the International Association of Computer Investigative Specialists (IACIS) and the Federal Law Enforcement Training Center (FLETC), etc. This continuous training will be sponsored and paid for by the FBI Laboratory or Government Employees Training Act (GETA) funds as appropriate.

(2) The CART training program will provide examiners with a broad base of computer knowledge for performing effective searches and proper forensic examinations and ensure that examiners are qualified and prepared to testify in court.

(3) CART training consists of two phases. The first phase, known as the general-education phase, lasts one to two years and ensures all examiners share a common knowledge base and qualifications. The second phase, known as the continuing-education phase, allows examiners to hone their skills and gain exposure to many technologies. The continuing-education phase continues throughout the examiner's career.

(4) The general-education phase culminates when the examiner receives his/her CART certification. Certification hinges on several factors. First, the examiner must complete all of the commercial training required. Second, the examiner must demonstrate technical proficiency. FEs accomplish this during a Lab Practicum at the FBI Laboratory. Finally, the FE must successfully complete moot court at a CART In-Service.

EFFECTIVE: 02/28/97

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 237

13-30.6.3 Field Examiner Equipment

For each Field Examiner (FE), hardware and software modules are provided by the Laboratory Division. This equipment remains on the inventory of the Laboratory Division but is assigned to the individual FE. Likewise, the software is assigned to individual FEs in their own names. When an FE leaves the program his/her equipment and software will either be reassigned to another FE or will be returned to the Laboratory Division.

EFFECTIVE: 02/28/97

13-30.6.4 Field Examiner Work Space

Field Examiners (FEs) have several unique requirements for their work space. The most important requirement is a secure work space to store evidence as it is being examined. Therefore, a secure room with access controlled by the FE is preferred. There should be adequate electrical service to support simultaneous operation of several computer systems. There should also be adequate ventilation to dissipate the heat generated by multiple computer systems. A telephone line is required in the FE's space to facilitate electronic communication between the FE and Computer Analysis and Response Team (CART), FBIHQ.

EFFECTIVE: 02/28/97

13-30.6.5 Reporting Procedures for Field Examiners

Upon completion of a forensic examination, the Field Examiner is required to send an FD-302 report and any documents printed to the case Agent for inclusion into the substantive case file. A copy of the FD-302 report should also be sent to the 66-HQ-C1155003 control file.

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 13 - 238

EFFECTIVE: 02/28/97

Sensitive
PRINTED: 02/18/98

**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.**



U.S. Department of Justice
Federal Bureau of Investigation

MANUAL OF INVESTIGATIVE OPERATIONS AND GUIDELINES

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 14 - 1

SECTION 14. FINGERPRINT IDENTIFICATION

14-1 HISTORICAL DATA CONCERNING FBI CRIMINAL JUSTICE
INFORMATION SERVICES (CJIS) DIVISION (FORMERLY THE
IDENTIFICATION DIVISION)

The insistent demand by police officials for one cooperative system for the compilation and exchange of criminal identification data on a national scale led to the formation of the FBI Identification Division on July 1, 1924. The fingerprint files from the Leavenworth Penitentiary and the National Bureau of Criminal Identification, which totaled 810,188 records, became the foundation of the FBI fingerprint card repository. The Identification Division and the Criminal Justice Information Services (CJIS) Division merged 5/1/93. The merger was to eliminate duplication and better conform to the new organizational structure. This consolidation of services enhances communications and services to local, state, federal, and international criminal justice agencies. (See MIOG, Part I, Section 32.)

EFFECTIVE: 12/13/95

14-2 FBI CRIMINAL JUSTICE INFORMATION SERVICES (CJIS) DIVISION
RECORDS SYSTEM

EFFECTIVE: 03/10/94

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 14 - 2

14-2.1 Categories of Individuals Covered by the System

- (1) Individuals fingerprinted as a result of arrest or incarceration.
- (2) Persons fingerprinted as a result of Federal employment applications, military service, alien registration and naturalization processes, and individuals desiring to have their fingerprints placed on record with the FBI for personal identification purposes.

EFFECTIVE: 05/25/90

14-2.2 Categories of Records in the System

- (1) Criminal fingerprint cards and related criminal justice information submitted by authorized agencies having criminal justice responsibilities.
- (2) Civil fingerprint cards submitted by Federal agencies and civil fingerprint cards submitted by persons desiring to have their fingerprints placed on record for personal identification purposes.
- (3) Fingerprint cards relating to missing persons and unidentified dead persons which are submitted by authorized agencies having criminal justice responsibilities.
- (4) Identification records sometimes referred to as "rap sheets" which are compilations of criminal history information pertaining to individuals who have criminal fingerprint cards maintained in the system.
- (5) A name index pertaining to each individual whose fingerprints are maintained in the system. The criminal records and the civil records are maintained in separate files. The criminal records are contained in either an automated file or a manual file depending on date of birth (refer to 14-10.1.2). The civil records are contained in a manual file. Both the criminal and civil files have an alphabetical name index related to data contained therein.

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 14 - 3

EFFECTIVE: 05/25/90

14-3 AUTHORITY FOR MAINTENANCE OF THE SYSTEM AND USE OF
SYSTEM'S RECORDS

EFFECTIVE: 05/25/90

14-3.1 Statutory Authority for FBI | Criminal Justice Information
Services (CJIS) | Division

The system is established, maintained, and used under authority granted by Title 28, United States Code (USC), Section 534; Public Law 92-544 (86 Stat. 1115); Public Law 94-29 (89 Stat. 140); Public Law 95-405 (92 Stat. 874); and Public Law 99-399 (100 Stat. 853). The authority is also codified in Title 28, Code of Federal Regulations (CFR), Section 0.85 (b) and (j), and Sections 20.1-20.38.

EFFECTIVE: 03/10/94

14-3.2 Uses of Records Maintained in the | Criminal Justice
Information Services (CJIS) | Division

The FBI operates the | CJIS | Division Records System to perform identification and criminal history record information functions for Federal, state, and local criminal justice agencies, and for noncriminal justice agencies, and other entities, where authorized by Federal statute, state statute pursuant to Public Law 92-544, Presidential Executive Order, or regulation of Attorney General of the United States. In addition, identification assistance is provided in disasters and for other humanitarian purposes. Record requests are also processed in accordance with Public Law 94-29, known as the Securities Acts Amendments of 1975; Public Law 95-405, known as the Futures Trading Act of 1978; and Public Law 99-399, known as the Omnibus Diplomatic Security and Anti-Terrorism Act of 1986.

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 14 - 4

EFFECTIVE: 03/10/94

14-4 DISSEMINATION GUIDELINES FOR FBI|CRIMINAL JUSTICE
INFORMATION SERVICES (CJIS)|DIVISION RECORDS| (See MAOP,
Part II, 9-2.8 & 9-3.1.1.)|

EFFECTIVE: 03/10/94

14-4.1 Authorized Dissemination

EFFECTIVE: 09/26/90

14-4.1.1 FBI Criminal History Records Made Available: (See MIOG,
Part II, 14-5.1.)

(1) To criminal justice agencies for criminal justice
purposes free of charge.

(2) To federal agencies authorized to receive them
pursuant to federal statute or Executive order. Effective 1/3/94, an
\$18 user fee may be charged for processing fingerprint cards submitted
by federal government agencies for nonlaw enforcement, noncriminal
justice licensing and employment purposes. A user fee ranging from
\$2.00 to \$8.00 may be charged for name-check requests submitted by
federal agencies for national security purposes. The fee will vary
for the name-check requests depending upon whether a paper or magnetic
tape format is used.

(3) To officials of federally chartered or insured
banking institutions to promote or maintain the security of those
institutions and, if authorized by state statute and approved by the
Attorney General, to officials of state and local governments for
purposes of employment and licensing (Public Law 92-544); to certain
segments of the securities industry for record checks on persons
involved with the transfer of securities (Section 14(f) (2) of Public
Law 94-29); to the Commodity Futures Trading Commission for record
checks on persons applying for licenses as commodities brokers (Public

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 14 - 5

Law 95-405); and to nuclear power plants for record checks on persons with unescorted access to nuclear power plants or individuals granted access to Safeguards Information by power reactor licensees (Public Law 99-399). Effective 1/3/94, a user fee of \$24.00 per inquiry (non-Federal applicant fingerprint card submissions) is being charged for this service.

| (4) Effective 7/1/94, a user fee of \$18.00 will be charged to federal criminal justice agencies for processing applicant fingerprint cards for firearms and related permits. Effective 10/1/94, a user fee of \$24.00 will be charged to state and local criminal justice agencies submitting applicant fingerprint cards for firearms and related permits. |

EFFECTIVE: 12/02/94

| 14-4.1.2 | Deleted |

EFFECTIVE: 09/26/90

14-4.2 Unauthorized Disseminations

The exchange of FBI criminal history records authorized by 14-4.1 is subject to cancellation if dissemination is made outside the receiving departments or related agencies. Such misuse may also be a violation of the Privacy Act of 1974 (see Part I, Section 187 of this manual). FBIHQ should be advised of such unauthorized or illegal uses without undue delay.

EFFECTIVE: 09/26/90

14-5 INDIVIDUAL'S RIGHT TO ACCESS FBI CRIMINAL HISTORY RECORDS

EFFECTIVE: 09/25/91

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 14 - 6

14-5.1 Access to the Record (See MIOG, Part II, 14-4.1.1 & 14-23.)

Any individual may obtain a copy of his/her FBI identification record by submitting to the FBI Criminal Justice Information Services (CJIS) Division a written request, accompanied by satisfactory proof of identity, and a certified check or money order in the amount of \$18.00 made payable to the Treasurer of the United States. Satisfactory proof of identity is defined as full name, date and place of birth, and a set of rolled-in inked fingerprint impressions. For full details refer to Title 28, CFR, Sections 16.30-16.34, or Departmental Order 556-73, a copy of which is on file in each field office. The CJIS Division is available to fingerprint any person in the Washington, D.C., area who wishes to obtain a copy of his/her identification record. In the field, local agencies are usually available which will fingerprint persons for employment, licensing, and other purposes. Each field office should ascertain the identities of such agencies in its area where requesters may be referred. However, where fingerprinting services are not otherwise available; or, where available but a person who wishes to obtain a copy of his/her identification record is experiencing difficulty in obtaining his/her fingerprints, the field office should fingerprint the person.

EFFECTIVE: 03/10/94

14-5.2 Challenge to Information in FBI Identification Record

If, after reviewing his/her identification record, the subject thereof believes that it is incorrect or incomplete in any respect and wishes changes, corrections or updating of the alleged deficiency, he/she should make application directly to the agency which contributed the questioned information. The contributor shall promptly notify the FBI of any corrections necessary, and, upon receipt of such a notification, the FBI will make any changes necessary in accordance with the corrections supplied by the contributor of the original information. The subject of a record may also direct his/her challenge as to the accuracy or completeness of any identifiable entry on his/her record to the FBI. The FBI will then forward the challenge to the agency which submitted the data requesting that agency to verify or correct the challenged entry.

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 14 - 7

EFFECTIVE: 05/14/93

14-6 NOTIFICATION OF PENDING LEGISLATION OR PROJECT REQUESTS

EFFECTIVE: 09/25/91

14-6.1 Pending Legislation

Field offices should advise FBIHQ, Attention:
| Criminal Justice Information Services (CJIS) | Division, of any pending
legislation that might curtail or restrict the legal right of state or
local criminal justice officials to fingerprint arrested persons.
| Field offices should also advise the | CJIS | Division of the passage of
any law, ordinance, or regulation requiring fingerprinting for
licensing or local/state employment.

EFFECTIVE: 03/10/94

14-6.2 Project Requests

| Field offices should promptly advise the | CJIS | Division of
any requested fingerprinting projects. Information concerning the
availability of such services should be addressed to FBIHQ, Attention:
| CJIS | Division. The field should make no commitments to handle any
"project" involving submission of fingerprints to the | CJIS | Division.

EFFECTIVE: 03/10/94

14-7 INKED FINGERPRINT IMPRESSIONS - TAKING

EFFECTIVE: 03/23/92

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 14 - 8

14-7.1 General Instructions

(1) The Criminal Justice Information Services (CJIS) Division, to date, accepts fingerprint images made from black printer's ink, specific chemical fingerprinting methods, and specific models of live-scan fingerprinting systems.

(2) The booklet, "The Science of Fingerprints," if carefully read, should thoroughly acquaint even a novice with the process of inked fingerprints. With the exception of the actual ink preparation, the principles provided also apply to taking chemically produced and live-scan generated fingerprints. Live-scan fingerprints cannot be used for obtaining fingerprint images from deformed fingers.

(3) Frequently officials fail to comply with all the instructions and illegible prints result. Accurate classification depends upon the existence of the focal points known as cores and deltas, between which ridges may be traced and/or counted. Each finger must be fully rolled from one nail edge to the other. Practice with the fingerprinting method selected will reveal the best possible fingerprint images. It is imperative that properly prepared prints be furnished the CJIS Division in order that errors may be reduced to the minimum.

EFFECTIVE: 03/10/94

14-7.2 Common Faults

- (1) Failure to properly cleanse the subject's hands or the equipment before inking or scanning the fingers.
- (2) Failure to fully roll the impressions in the correct finger block.
- (3) Uneven inking.
- (4) Overinking.
- (5) Applying too much or too little pressure when rolling fingers.
- (6) Fingers excessively moist.

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 14 - 9

- (7) Fingers excessively dry.

EFFECTIVE: 03/23/92

14-7.3 Major Case Prints

The Latent Fingerprint Section, Laboratory Division will retain major case fingerprint cards submitted to the CJIS Division by the FBI and other federal agencies, which are appropriately recorded and included on arrest fingerprint card (Form FD-249). The Latent Fingerprint Section will review and examine the fingerprint card and palm prints. If the Latent Fingerprint Section has no interest in the subject, the prints are forwarded to the Special Processing Unit, Identification Services Section, CJIS Division, for handling. Major case prints submitted by all other agencies are returned to the contributor.

EFFECTIVE: 12/13/95

14-7.3.1 Equipment

The necessary equipment consists of the regular fingerprint inking material and fingerprint cards, plain 8- by 8-inch cards, and cylindrical object three inches or more in diameter. Place an 8- by 8-inch white card on the cylinder. This card is then held in place by rubber bands.

EFFECTIVE: 03/23/92

14-7.3.2 Procedure

- (1) Set of fingerprints taken in the usual manner.
- (2) Record main palm print of right hand. With a roller, roll ink on the inking plate so that the entire roller is covered with a thin and even amount of ink. Take the subject's right hand and apply the ink with the roller directly to the subject's hand. The entire surface of the palm and fingers should be inked. Take the subject's inked hand and place the heel of the palm on the card at the

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 14 - 10

lower edge. Then by using the cylindrical object placed on a desk as a roller, the inked palm print can be taken. The right hand, including the fingers, should be taken. The fingers are kept stiff and outstretched in the process of rolling the cylinder. Fingerprints are taken as a part of the process so that the palm prints can receive proper attention in the Latent Fingerprint Section, Laboratory Division, for filing purposes.

(3) Record impressions of the outer edges (little finger and thumb sides) of the palm. After the usual impression is made on the card with the right palm lying flat, the ridges under the little finger and thumb should be inked to the bottom of the palm and out to the smooth skin. Remove the card from the holder and lay flat on the table. The right side of the palm is placed at a 45-degree angle to the right of the previously printed right palm and rolled onto the card. Next the left side of the right palm is placed at a 45-degree angle to the left of the already recorded main palm print and rolled onto the card.

(4) Prints of the sides, lower joints, and tips of the fingers of right hand obtained as follows, after having placed the card on a smooth flat surface and securing by means of tape or thumb tacks:

(a) Ink the fingers from side to side for their entire length.

(b) First, an impression is made by laying the finger on its left side (45-degree angle) and raising it up to the nail.

(c) A second impression is made just to the right of the first impression laying the finger flat and raising inward to the nail.

(d) A third print is made just to the right of the second impression by laying the finger on its right side and raising to the nail.

(e) A fourth impression is made above the other three impressions by placing the tip only on its left side and rolling completely to the right, producing a rolled print of the tip only.

(f) Lastly, to the immediate right of the four impressions, record a fully rolled print of the entire areas of the lower joints of the finger. To accomplish this, hold the finger

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 14 - 11

horizontally and place one side of the finger straight down on the card. Then, roll the finger 180 degrees to the other side, ensuring that all areas of the lower joints are clearly recorded. In recording the rolled impression of the lower joints of each finger, the direction of the roll should be the same as when recording a set of rolled fingerprints on a regular fingerprint card--that is, roll the thumbs toward the subject's body and the other fingers away from the subject's body.

(g) The end results consist of five different impressions of each finger, i.e., two side-to-tip impressions, one flat-to-tip impression, one tip impression, and one fully rolled impression of the lower joints. Prints of the same finger should be grouped on the card and identified as to right thumb, right index, etc. As many finger groups as possible may be placed on the same card and several cards may be used, if necessary; however, prints should be recorded on one side only.

(5) The same process is followed with the left hand.

(6) If more than one impression of any area is made to ensure legibility, all prints should be submitted for comparison.

(7) Every card, regardless of the type of print appearing on it, must bear the subject's name, the name of the person taking the prints, and the date taken.

EFFECTIVE: 12/13/95

14-7.4 Live-Scan Electronically Produced Fingerprint Impression

(1) On November 10, 1988, the Identification Division (now CJIS Division) published the document, "Minimum Image Quality Requirements for Live-Scan, Electronically Produced, Fingerprint Cards." This document established the criteria that live-scan fingerprint cards must meet to be accepted for processing and retention in the FBI's identification records system.

(2) Since that time, the CJIS Division and Underwriters Laboratories, Inc., have performed an aggressive series of tests to ensure that the requirements are realistic, and that fingerprints produced on live-scan systems support the CJIS Division's processing needs.

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 14 - 12

(3) As a result of these tests, live-scan fingerprint cards produced on specific equipment configurations are now being accepted for CJIS Division processing and retention. Appropriate announcements are made as live-scan systems are evaluated and accepted for CJIS Division use.

(4) On August 30, 1991, the Identification Division (now CJIS Division) published a revision to the requirements document. The revision more accurately reflects the fingerprint processing needs of the FBI.

EFFECTIVE: 03/10/94

14-8 FINGERPRINT CARD DATA

EFFECTIVE: 03/23/92

14-8.1 Submitted by FBI

EFFECTIVE: 03/23/92

14-8.1.1 Subjects Incidental to Arrest

When fingerprinting an arrestee, at least two sets of fingerprints should be taken on the criminal fingerprint card (Form FD-249). Both cards should be filled out completely with particular attention given to the following:

(1) The card should reflect the local FBI office as the contributor.

(2) Set forth complete charge in narrative form in the "Charge" block; statute citation should go on the back of the fingerprint card.

(3) Date of arrest.

(4) Full name and descriptive data.

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 14 - 13

(5) Check appropriate "Photo Available" block on back of card; retain photo in field office file (do not attach to the fingerprint card).

(6) Show the local United States Marshals Service (USMS) Originating Agency Identifier Number (ORI#) and address in the "Send Copy To" block on the back of the fingerprint card (local USMS ORI# can be obtained from the USMS or through an inquiry of the NCIC). This notation ensures that the USMS office assuming custody of the arrestee will receive a copy of the Criminal Justice Information Services (CJIS) Division response, i.e., either the subject's criminal record or a notification that he/she had no prior criminal record. The USMS should be provided the duplicate set of prints and should be advised that the original fingerprint card has been forwarded to the FBI/CJIS Division. This will assure the USMS that they will receive the results of the criminal history record check of the CJIS Division and will eliminate their need to fingerprint the arrestee. This also applies to situations in which a Federal prisoner (who is incarcerated in an area where there is no deputy marshal) is released at a hearing or arraignment before the marshal can obtain the prisoner's fingerprints. (See MIOG, Part II, 14-8.2.)

(7) Disposition, if known, or submit it promptly when ascertained.

EFFECTIVE: 03/10/94

14-8.1.2 Suspects Only

(1) "Suspect" to be indicated in space marked "Charge" on fingerprint card.

(2) Fingerprints returned to field office after search and to be filed in 1-A section of investigative case file.

(3) If identification is made with a previous arrest record, a copy of record will be furnished to the field at time fingerprint card returned.

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 14 - 14

EFFECTIVE: 03/23/92

14-8.1.3 Informants

(1) Use criminal fingerprint card (FD-249) and forward to Criminal Informant Unit, Intelligence Section, Criminal Investigative Division, for referral to the CJIS Division. b2

(2) Contributor is FBI field office.

(3) Place the word "inquiry" in "Charge" space on face of card.

(4) Full name and descriptive data.

(5) Prints are retained by the CJIS Division if classifiable [REDACTED]

EFFECTIVE: 03/10/94

14-8.1.4 Juveniles

Juveniles may be fingerprinted in accordance with the provisions of Title 18, USC, Section 5038 (see Part II, Section 4 of this manual).

EFFECTIVE: 03/23/92

14-8.1.5 FBI Applicants (See MIOG, Part I, 67-11.3.8, 67-17.1.7.)

FBI support applicants, who are favorably recommended, are to be fingerprinted at the time they are interviewed. FBI Special Agent applicants are to be fingerprinted at the time of their panel interview. Cards are to be submitted to FBI Headquarters, Attention: Personnel Division, along with application, interview sheets, questionnaires and examination papers. In every instance, applicant for FBI position should be fingerprinted by FBI personnel.

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 14 - 15

EFFECTIVE: 04/21/94

14-8.2 Submitted by U.S. Marshals Service

Primary duty of U.S. Marshals Service (USMS) is to fingerprint every Federal prisoner (except juveniles, see 14-8.1.4) without delay as soon as custody is assumed. USMS should be shown as contributor together with date of arrest, charge, and other data. Reverse side of card should be marked to designate copy of reply to interested FBI field office or offices. However, a defendant turned over to the custody of the USMS will not be fingerprinted, provided the arresting agency assures that it has already done so and has included the USMS in the distribution of the criminal history in the "Send Copy To" block of the FD-249 (see Section 14-8.1.1).

EFFECTIVE: 09/25/91

14-8.3 Submitted by Other Criminal Justice Agency for FBI

Where subject is fingerprinted by another criminal justice agency for the FBI pursuant to arrest for which Federal process outstanding, FBI field office should be shown as contributor, together with date of arrest, charge, and descriptive data. Fingerprint card should be marked for copy of reply to local criminal justice agency if latter interested.

EFFECTIVE: 09/25/91

14-8.4 Submitted by Local Criminal Justice Agency on a Local Charge

When subject is fingerprinted by a local criminal justice agency on a local charge, such as car theft, and FBI interested as possible ITSMV violation, local criminal justice agency should be shown as contributor, together with local charge, date of arrest and descriptive data. Copy should be indicated for appropriate FBI field office by indicating in the "Send Copy To" block on the back of the fingerprint card, the field office Originating Agency Identifier Number (ORI#) and address.

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 14 - 16

EFFECTIVE: 09/25/91

14-9 FINGERPRINT CARDS - TYPES

EFFECTIVE: 09/25/91

14-9.1 Distributed to Criminal Justice Agencies Without Charge

EFFECTIVE: 09/25/91

14-9.1.1 Criminal Fingerprint Card (FD-249)

This card is used by criminal justice agencies to record the finger impressions of those persons who have been arrested or incarcerated in a penal institution. The criminal card includes information regarding the arrest charge, the disposition, and other information relating to the physical description. Space is provided for the FBI number and should be indicated when it is known. Spaces are also provided for the contributor of the fingerprints to indicate whether or not a reply is desired and if a collect wire reply or collect telephone reply is desired. Due to the requirements of the Criminal Justice Information Services (CJIS) Division's automated services system, when a contributor places an FBI number on the fingerprint card, it is also necessary to submit a full set of fingerprints.

EFFECTIVE: 03/10/94

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 14 - 17

14-9.1.2 Applicant Fingerprint Card (FD-258)

This fingerprint card is used in submitting fingerprints to the CJIS Division on persons directly employed in or applying for criminal justice positions or in those instances where authorized by Federal statute, Presidential Executive Order, state statute pursuant to Public Law 92-544, or regulation of the Attorney General of the United States.

EFFECTIVE: 03/10/94

14-9.1.3 Personal Identification Card (FD-353)

This card is used solely for recording finger impressions of those persons who voluntarily submit their fingerprints for purposes of identification only. These cards are available to anyone who desires to forward his/her fingerprints to the CJIS Division for retention. With regard to the fingerprints of children who have been printed by parents for identification purposes, the parents are urged to retain the child's prints which should be forwarded to the appropriate law enforcement authorities only if the child becomes missing. They are not searched against the criminal file. Personal identification fingerprint cards are filed in the civil file of the CJIS Division.

EFFECTIVE: 03/10/94

14-9.1.4 Personnel Fingerprint Card (FD-380)

This card is used exclusively for the taking of fingerprints of FBI personnel at the time they enter on duty. It is distributed to FBI field offices only.

EFFECTIVE: 09/25/91

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 14 - 18

14-9.2 Not Distributed by FBI but Processed in the Criminal
Justice Information Services (CJIS) Division

EFFECTIVE: 03/10/94

14-9.2.1 Office of Personnel Management (OPM) Fingerprint Card

This card (SF-87) used for taking of fingerprints of U.S. Government employees who come within purview of Government security program.

EFFECTIVE: 09/25/91

14-9.2.2 Armed Forces Fingerprint Card

This card (DD-2280) used by Army, Air Force, Marine Corps, and Navy for taking of fingerprints of military personnel.

EFFECTIVE: 09/25/91

14-9.2.3 U.S. Coast Guard Fingerprint Card

This card (DD-2280) used for personnel of U.S. Coast Guard. Identification Division (now CJIS Division) has filed since 11/15/48 a copy of these fingerprint cards as part of its civil fingerprint file. Coast Guard maintains a separate fingerprint file.

EFFECTIVE: 03/10/94

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 14 - 19

14-9.2.4 Alien Registration Fingerprint Card (See MIOG, Part II,
14-10.2.1 & 14-10.2.2.)

This card (AR-4) was used by State Department and U.S. Immigration and Naturalization Service. Identification Division (now CJIS) has filed these fingerprint cards since 1940 when Alien Registration Act went into effect concerning fingerprinting of aliens. The fingerprinting requirement in the Act was rescinded in 1986 and, therefore, cards are no longer being received for filing. No other fingerprint file is maintained on alien registrations.

EFFECTIVE: 03/10/94

14-10 FILES IN THE CRIMINAL JUSTICE INFORMATION SERVICES (CJIS) DIVISION

EFFECTIVE: 03/10/94

14-10.1 Criminal File

EFFECTIVE: 09/25/91

14-10.1.1 Fingerprint Card File

The first retain fingerprint card received on persons arrested or incarcerated by local, state, and/or Federal authorities is assigned an FBI number. This card is filed in the Technical Section Master Criminal Fingerprint File by the fingerprint classification formula. This file is divided into male and female sections as well as age group. When a subsequent set of retain fingerprints is submitted and found to be identical with the first arrest in the CJIS Division's automated services system, the retain print will be maintained on microfilm. If the record has not been fully automated, the record will be fully automated before processing of the retain fingerprint card is complete. All wanted, flash and

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 14 - 20

missing persons notices are placed in the subject's computerized criminal name record. Unidentified missing person notices are returned to the sender. Unidentified missing person fingerprint cards are filed in the criminal file, which is indexed by the fingerprint classification formula.

EFFECTIVE: 08/18/94

14-10.1.2 Criminal Name Indices (See MIOG, Part II, 14-2.2(5) & 14-12.2.)

The name and descriptive information (e.g., aliases, sex, race, date and place of birth, social security number, etc.) appearing on criminal fingerprint cards submitted to the CJIS Division are indexed in the division's criminal name indices. All such data relating to offenders born on or after 1/1/29 is computerized. Data relating to offenders born prior to 1/1/29 is still maintained on name index cards and searched manually. If the current retain criminal card is found to be identical to a manual record, the subject's record will be maintained in the CJIS Division's automated services system. A match on the basis of name and other descriptors cannot be reported as a positive identification without a subsequent fingerprint comparison.

EFFECTIVE: 08/18/94

14-10.2 Civil File

EFFECTIVE: 03/23/92

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 14 - 21

14-10.2.1 Fingerprint Card File

This file contains fingerprint cards of military personnel, Federal employees, aliens, miscellaneous applicant-type fingerprints, and fingerprints submitted for personal identification. With the exception of the aliens and personal identification cards, these cards are placed in this file provided no criminal card is located in the criminal file. In the case of personal identification fingerprint cards and alien registration fingerprint cards, no search is made by either name or fingerprint classification and the cards are automatically filed in the civil file. This file is divided into male and female.

EFFECTIVE: 03/23/92

14-10.2.2 Civil Name Indices

Names appearing on fingerprint cards of military personnel, Federal employees, aliens, miscellaneous applicant-type fingerprints, and fingerprints submitted for personal identification are indexed on 3- by 5-inch cards. On this index card appear name, race, height, weight, date of birth, fingerprint classification, registry number (military service, alien registration, etc.) and submitting agency. This file is divided into male and female. (Refer to 14-9.2.4--No new alien fingerprint cards are being added to file.)

EFFECTIVE: 03/23/92

14-10.3 Missing Person Fingerprint File (See MIOG, Part I, 7-14.8(4), 79-1.2; Part II, 16-16.3(2).)

This file contains fingerprint cards of persons reported missing to law enforcement agencies and entered into the National Crime Information Center (NCIC) Missing Person File under any of the NCIC entry criteria. The criteria are set forth in the NCIC OPERATING MANUAL, Part 8, Section 1, Subsection 1.1, Page 8-1. The fingerprint card for a person reported as missing is kept in the CJIS Division Information Services Section's (ISS) (formerly Technical Section) Master Criminal Fingerprint File until advised by the contributor to remove the card, or until the missing person reaches the age of 99.

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 14 - 22

EFFECTIVE: 05/13/96

14-10.4 FBI Number

All criminal fingerprint cards which are to be retained in the CJIS Division files are given an FBI number if one has not been assigned previously. A number is assigned upon receipt of the first set of prints. FBI numbers are assigned in numerical sequence and no distinction is made between males and females. Assignment of an FBI number does not mean that an individual has an arrest record because certain civil fingerprint cards are assigned FBI numbers. When FBI number is known for an individual, it should be referred to in correspondence. An FBI number will be found:

(1) On microfilmed 3- by 5-inch index cards in the manual name index files.

(2) Deleted

(3) In the CJIS Division's automated services system.

(4) On "master" fingerprint card in the manual fingerprint card file of the ISS.

(5) On other fingerprint cards filed in folders called jackets which contain a variety of criminal history records for an individual.

(6) Deleted

(7) On fingerprint cards/records on microfilm.

EFFECTIVE: 08/18/94

14-10.5 Deleted

EFFECTIVE: 03/23/92

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 14 - 23

14-10.5.1 Deleted

EFFECTIVE: 03/23/92

14-10.5.2 Deleted

EFFECTIVE: 03/23/92

14-10.5.3 Deleted

EFFECTIVE: 03/23/92

14-10.6 Dead File (See MIOG, Part I, 79-1.2; & Part II,
14-15.2.)

(1) Effective 10/1/88, the Identification Division (now Criminal Justice Information Services (CJIS) Division) will deactivate an identification record and move the record to its Dead File only when a current fingerprint(s) submission which the CJIS Division knows was taken from the deceased body is matched to the record or a Fingerprint Identification Indicator (FII) submission is received from a state in conjunction with the National Fingerprint File (NFF). When a fingerprint(s) taken from a deceased individual or an FII from an NFF state is received and matched to fingerprints on file in the CJIS Division's Criminal File, the subject's record is removed from the active file and placed in the Criminal Dead File and later filmed. Since 1/3/84, all criminal deceased name records have been entered in the former Identification Division's Automated Services System (IDAS) (now CJIS) and retained for seven years, if the year of birth is 1929 or after. Also, effective 10/1/88, when a fingerprint(s) of a deceased individual is matched to fingerprints in the former Identification Division's (now CJIS) Civil File, the civil print is retained in the Civil Dead File for seven years with a stamped notation on the back as to why the record was deactivated and moved to the Dead File. A fingerprint card of an unidentified deceased person which is received at the CJIS Division as "John Doe," "Jane Doe," or "Unknown" will be searched in the Criminal, Civil, and Missing Person Fingerprint Files; and, if no identification is effected, the fingerprint card will be retained for a period of seven years and then destroyed.

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 14 - 24

(2) The processing of fingerprint cards for deceased persons whose identities are known will be rejected at point of receipt. The CJIS Division will accept and process all known deceased fingerprint cards that are accompanied by correspondence or a notation on the fingerprint card itself seeking positive verification of entitlement to veterans benefits.

EFFECTIVE: 03/10/94

14-11 PROCESSING OF FINGERPRINT CARDS IN THE CRIMINAL JUSTICE
INFORMATION SERVICES (CJIS) DIVISION

Fingerprint cards received in the CJIS Division are in the nature of inquiries demanding prompt replies. All fingerprints received are handled on a priority basis consistent with urgency in a particular case. Generally speaking, arrest-type fingerprints from criminal justice agencies are given top priority followed by various categories of applicant-type fingerprints. Processing involves the following:

- (1) Deleted
- (2) Recording the number of prints received on a daily basis.
- (3) Indicating any special handling, such as wire answer or search of military files.
- (4) Record the date of receipt of the fingerprint card by assigning a Process Control Number.
- (5) Search all incoming fingerprint cards through the Automated Name Search. If no tentative identification is effected, an Automated Technical Search is performed. A manual name and technical search is performed on those subjects with a date of birth prior to 1932.
- (6) Those tentatively identified with prior records are verified by comparison of the finger impressions.
- (7) Deleted

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 14 - 25

(8) When an identification has been effected and verified, the complete record is assembled, consolidated, and necessary replies forwarded to the interested agencies.

EFFECTIVE: 03/10/94

14-12 REQUESTING RECORDS FROM THE CRIMINAL JUSTICE INFORMATION
SERVICES (CJIS) DIVISION (See MAOP, Part II, 7-2.1.)

EFFECTIVE: 03/10/94

14-12.1 Requirements for Positive Identification - One of the
Following:

(1) Actual comparison of the fingerprints.

(2) Submission of name plus FBI number. The Interstate Identification Index (III) should be accessed initially to determine if an arrest record is available through the III before an inquiry is made of the CJIS Division (see Section 14-12.3.3).

(3) Submission of name plus local arrest, commitment, registry, applicant, or military service number. There are exceptions in this category, such as, common names, which may make a search of the voluminous automated or manual name file impractical.

EFFECTIVE: 03/10/94

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 14 - 26

14-12.2 Possible Identification

A possible identification of a name and general descriptive data may be made by searching the Interstate Identification Index (III) or the automated or manual name file (depending on date of birth, refer to 14-10.1.2). While good results may often be obtained when only general information is available, specific identifiable information produces better results and considerable savings of time and effort.

EFFECTIVE: 09/25/91

14-12.3 Procedures for Requesting Records for Field Offices

EFFECTIVE: 09/25/91

14-12.3.1 Submission of Fingerprint Card by Field Office

(1) Preprinted fingerprint cards bearing contributor and ORI number are furnished by the CJIS Division.

(2) Only the field office or agency to which ORI number is assigned should use this card, and CARD SHOULD NOT BE EXCHANGED BETWEEN OFFICES OR AGENCIES.

(3) Do not delay submission of fingerprint cards pending final disposition of case.

(4) Reply will be furnished to office or agency appearing in ORI space on card, and this agency will be listed on identification record as the arresting agency.

(5) Cover letters need not be used.

(6) FBI number, when available, should be placed on card in space designated.

(7) Full identifying data to appear in spaces provided.

(8) Investigative file number, when available, is placed in "your no. OCA" space on the face of the card.

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 14 - 27

(9) Note on back of card any special handling desired before a specific date, as such eliminates the necessity of a letter or teletype.

EFFECTIVE: 03/10/94

14-12.3.2 Notation on Fingerprint Card Submitted by Another Agency

(1) Specifically requests copy of record be forwarded to interested field office.

(2) No cover letter necessary.

(3) If FBI Agent present at time individual involved in FBI investigation is fingerprinted by another agency, ensure above notation is placed, and best obtainable set of prints forwarded to CJIS Division.

(4) Each field office should have a definite arrangement with U.S. Marshal, as well as criminal justice agencies of larger cities, for ensuring above notation placed on back of fingerprint card when warranted.

EFFECTIVE: 03/10/94

14-12.3.3 Form FD-9 (See MIOG, Part I, 26-3(2) & Part II, 14-12.1.)

(1) If an NCIC computer terminal is readily available, the Interstate Identification Index (III) should be accessed to determine if an arrest record is indexed for your individual before submission of FD-9. If the individual inquired upon has a date of birth of 1956 OR LATER and no record is located in III, no record exists in the FBI's CJIS Division and no submission of an FD-9 is needed. If the individual has a date of birth PRIOR to 1956 and no record is located, an FD-9 should be submitted to the FBI's CJIS Division because an arrest record may exist which is not automated and indexed in the III. Refer to your NCIC OPERATING MANUAL, Part 10, which includes the III User's Guide for specific guidelines for accessing III.

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 14 - 28

(2) When a large volume of record checks is needed and descriptive data can be obtained from an existing automated file, an alternative to using the III or the FD-9 is Name Searching by Machine Readable Data (MRD). The data is formatted into the CJIS Division standard format and then Name Checks can be processed by magnetic tape and results provided automatically.

(3) The following instructions pertain to the submission of Form FD-9:

(a) Name and arrest number or other number under which fingerprints have been submitted.

(b) FBI number if known.

(c) All known aliases.

(d) Fingerprint classification, if FBI number not known.

(e) No file copy of FD-9 necessary.

(f) Notation made in field office file showing request.

(g) FD-9 returned to field office with results.

1. No record, so noted on form.

2. If identified, copy of record attached to form.

3. Serialize and place in file.

(h) FD-9 can be submitted in legible hand printing.

EFFECTIVE: 03/10/94

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 14 - 29

14-12.3.4 Form FD-165 (See MIOG, Part I, 137-9.)

This form serves a dual function and is used to place a Bureau field division stop whenever the field requests a wanted for questioning and/or interview, without a federal warrant or, whenever the field requests a flash be placed for informants, applicants for federal pardons, Pretrial Diversion, etc. (See MIOG, Part I, 73-8.3, and Correspondence Guide-Field, 3-13.)

(1) Causes a stop to be placed against the CJIS Division's criminal record file when wanted for questioning and/or interview if fingerprints exist. If no fingerprints exist on the subject, then a stop is placed in the automated name indices file.

(2) Causes a stop to be placed against the CJIS Division's criminal record file when a flash is requested for informants, applicants for federal pardons, Pretrial Diversion, etc., if fingerprints exist. If no fingerprints exist, the FD-165 is returned to the originating field office. When a flash is requested for an informant and no fingerprints exist, a name stop is placed.

(3) At the time a stop is placed, the FD-165 can also be used to request the identification record on the subject. The identification record will be forwarded to the office submitting the FD-165. Thereafter, this record can be accessed through the III for any additional requests for the identification record.

EFFECTIVE: 11/18/96

14-12.3.5 Request for Photographic or Laminated Copy of Fingerprint Card by FBI Field Office (See MIOG, Part II, 21-23(22).)

(1) Direct airtel, memorandum, or teletype to FBIHQ, Attention: CJIS Division.

(2) FBI number and number of copies needed should be indicated in request.

(3) If fugitive, the Office of Origin should ensure fugitive's FBI number is entered in his/her Wanted Person File record in NCIC before requesting copies of the fingerprint card.

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 14 - 30

EFFECTIVE: 03/10/94

14-13 PHRASEOLOGY OF RECORDS FURNISHED BY THE CRIMINAL JUSTICE
INFORMATION SERVICES (CJIS) DIVISION

EFFECTIVE: 03/10/94

14-13.1 Identifiable Records

Since fingerprint records furnished by the CJIS Division under FBI numbers contain civil as well as criminal notations, they should be referred to as "identification," rather than "criminal," records.

EFFECTIVE: 03/10/94

14-13.2 Nonidentifiable Records

When a search is made against the criminal fingerprint file and no record is found, the CJIS Division will use the phraseology, "No arrest record FBI." FBIHQ and field offices likewise should use such phraseology in their communications when applicable.

EFFECTIVE: 03/10/94

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 14 - 31

14-13.3 "Bureau" Page

When information transcribed for FBI use only, such as data pertaining to a previously processed "Return" fingerprint card, i.e., the contributor of the fingerprint card, the subject's name, the date on the card, and reason fingerprinted, etc., is added to an identification record, it is placed on a special page called the "Bureau" page. At the bottom of this page in capital letters will be the notation "THIS PAGE SHOULD NOT BE DISSEMINATED OUTSIDE THE FBI." Persons forwarding copies of identification records to sources outside the FBI should be governed accordingly. Be aware that "Bureau" pages are not transmitted with III responses to on-line information requests made through NCIC.

EFFECTIVE: 12/10/91

14-14 CERTIFICATION OF IDENTIFICATION RECORDS AND FINGERPRINTS

Identification records will be certified by the Assistant Director or one of the Inspector-Deputy Assistant Directors of the Criminal Justice Information Services (CJIS) Division upon issuance of a court order requiring certification. Such records are typed with or without abbreviations, as long as consistent throughout document, and the certification is in accordance with Title 28, USC, Section 1733. Fingerprints also can be certified under the same citation. Requests for certifications should be limited to court cases or other special situations requiring the production of such a record. (See Correspondence Guide-FBIHQ, 1-2.1.)

EFFECTIVE: 03/10/94

14-15 FORMS FOR SUBMITTING, OBTAINING, AND VERIFYING
IDENTIFICATION INFORMATION

EFFECTIVE: 12/10/91

14-15.1 Final Disposition Report (R-84)

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 14 - 32

EFFECTIVE: 12/10/91

14-15.1.1 Use by Field Offices (See Correspondence Guide-Field,
3-61.)

(1) Reporting final dispositions of criminal cases in which fingerprint cards have been previously submitted and retained by the Criminal Justice Information Services (CJIS) Division.

(2) Serves as a follow-up to a specific arrest.

(3) Only one disposition form should be used to record the dispositions against any one individual.

(4) Only the original need be sent.

(5) Deleted

(6) One copy retained in field office file.

(7) In any case, where a field office takes credit on an FD-515 for the arrest or conviction of an FBI subject in connection with violations of a federal law, the Office of Origin of this case must ensure that the CJIS Division is advised of the final disposition or any amended disposition. This can be accomplished by forwarding a Final Disposition Form (R-84) to the CJIS Division. If the Office of Origin has determined that another field office or other criminal justice agency has already submitted the disposition to the CJIS Division, it is not necessary to forward the R-84. However, the Office of Origin must document in the investigative file the identity of the agency or auxiliary office which submitted the R-84, and similarly note such information in the "Remarks" section of the FD-515. (See MAOP, Part II, 3-5.4 & 4-6.)

EFFECTIVE: 07/19/95

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 14 - 33

14-15.1.2 Use by Local and State Criminal Justice Agencies

Submitted in each case at whatever level - law enforcement, prosecutor, or court - upon receipt of final disposition.

EFFECTIVE: 03/23/92

14-15.1.3 Not Used

(1) If final disposition known at time fingerprints submitted to CJIS Division, then disposition data should be recorded on fingerprint card thus eliminating need for R-84.

(2) If subject not fingerprinted, there is no arrest record against which disposition data can be posted.

(3) If the fingerprint was returned by the CJIS Division as unclassifiable, etc., and the fingerprints were not resubmitted by the contributor.

(4) If reporting new arrest information, since such information must be furnished on a fingerprint card.

EFFECTIVE: 03/10/94

14-15.1.4 Data for Preparation of Form

(1) Contributor of fingerprints.

(2) Name and number under which fingerprints submitted to FBI, and State Identification number, if available.

(3) If the FBI arrested the arrestee, the form should reflect the field office file number. U.S. Marshal's number should be furnished in every instance in which the U.S. Marshal has fingerprinted a prisoner and assigned a number. If this number is not available in the FBI field office, it must be obtained from the U.S. Marshal's office.

(4) Date arrested or charged.

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 14 - 34

(5) Original charge for which arrested or committed. If penal code citations are used, they should be supplemented with a brief explanation of the type of charges(s); i.e., ITSMV, burglary, etc.

(6) Final disposition and Date thereof:

(a) Include dispositions for all counts of the indictment(s)

(b) If sentence imposed relates to a charge other than the charge for which arrested, state this and also show how disposition relates to original charge.

(7) FBI number, if known.

(8) Sex

(9) Fingerprint classification, if available.

(10) Age or date of birth

(11) Submitting agency.

EFFECTIVE: 03/23/92

14-15.1.5 Return of Form to Contributor

(1) A disposition form should include sufficient information to allow the CJIS Division to handle it without referring to previous submissions. If the required information is not furnished, the disposition form is either returned to the contributor with reason(s) for the return indicated or it may be destroyed.

(2) The subject's arrest fingerprint card showing the offense quoted on the disposition form must be in the CJIS Division's Criminal File in order to post the disposition. If no fingerprints for the offense are on file in the CJIS Division's Criminal File, the disposition form will be appropriately disposed of.

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 14 - 35

EFFECTIVE: 03/10/94

14-15.1.6 FD-10 in Lieu of Final Disposition Report (R-84)

FD-10 is used by FBI field office to request dispositions from a local criminal justice agency (if request is for New York City, send two copies of FD-10 to the New York Division of Criminal Justice Services, Executive Park Tower, Stuyvesant Plaza, Albany, New York 12203-3764, rather than the New York City Police Department). (See MIOG, Part II, 23-3.1(2).)

(1) Place notation of request in investigative file.

(2) Upon return of FD-10, note pertinent information in investigative file.

(3) Forward to CJIS Division in lieu of R-84 if final disposition is set forth or its unavailability is so stated.

(4) Office of origin has responsibility of sending FD-10 and advising auxiliary offices, if necessary, of any pertinent data obtained.

(5) FBI number should always be shown when available.

EFFECTIVE: 03/10/94

14-15.1.7 Accountability for Dispositions

b2 All missing dispositions on identification records received by the field must be accounted for. SAC may, at his/her discretion, authorize an exception in "nonfugitive-prosecutive" matters where FBI interests are best served by not making a dispositional inquiry; e.g., [REDACTED]

EFFECTIVE: 09/26/90

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 14 - 36

14-15.2 Death Notice (R-88) (See MIOG, Part II, 14-10.6.)

This form, previously furnished to criminal justice agencies, was used to report the death of an individual whose fingerprints are on file in the CJIS Division. This form has been discontinued. Correspondence, including the R-88 form, containing a fingerprint impression(s) that the CJIS Division matches to a record, will not cause the identification record to be placed in the CJIS Division's Dead File unless the CJIS Division is positive that the incoming fingerprint(s) is an impression(s) taken from the body of the deceased person. Unconfirmed deceased information, i.e., not supported by a print(s) from the body, will be added to the record to show that the subject of the record was reported deceased on a particular date by a specific agency. The record will remain active and be subject to dissemination upon request. No cover letter is necessary when the R-88 form is used; however, its continued use is discouraged. Submission of the individual's fingerprints taken from the body of the deceased on the arrest fingerprint card (Form FD-249) is the best method of advising the CJIS Division of the death of an individual with a criminal record.

EFFECTIVE: 03/10/94

14-15.3 Deleted

EFFECTIVE: 03/23/92

14-15.4 Fugitive Airtel (FD-65) (See MIOG, Part II, 21-4; MAOP, Part II, 7-2.1.)

Submitted when subject becomes an FBI fugitive. This form provides FBIHQ, Criminal Investigative Division, with notification of subject's fugitive status. This form also provides the Savannah Information Technology Center (SITC) with notification of the fugitive's status and provides it with the basic background to conduct appropriate record checks available through the SITC. The SITC will provide the Office of Origin with additional background information, if available, resulting from these record checks. The Office of Origin uses this form to enter the fugitive warrant into the National Crime Information Center (NCIC) Wanted Person File; this results in

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 14 - 37

the automatic entry of the warrant information into the subject's automated criminal identification record and/or name indices file if such a record exists. If no fingerprint file exists on the subject, then a notice is placed in the CJIS Division's automated name indices file only.

EFFECTIVE: 10/11/94

14-15.4.1 Data for Preparation of Form

(1) Title appearing on form should contain the names of all fugitives involved in the case in accordance with MAOP, Part II, Section 10-16.7 through 10-16.7.2.

(2) The original, marked for the attention of the Criminal Investigative Division, should be sent immediately after fugitive process is obtained.

(3) Deleted

(4) Do not delay the submission of the form to obtain additional descriptive information not readily available.

EFFECTIVE: 03/23/92

14-15.4.2 Data for Supplemental Submission

(1) Pertinent additional descriptive information obtained subsequent to initial submission.

(2) Mark appropriate block on form.

(3) Refer to date of initial submission.

(4) If the information previously furnished is no longer accurate, insert either the new information or the word "delete" in the appropriate spaces on the form.

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 14 - 38

EFFECTIVE: 03/23/92

14-15.4.3 No Initial Submission

An initial fugitive airtel is not necessary in cases involving parole or mandatory release violators or deserters. However, a supplemental form should be submitted to show any changes, additions, or deletions to identifying data furnished in correspondence from FBIHQ initiating the investigation.

EFFECTIVE: 04/19/91

14-15.4.4 No Supplemental Submission

It is not necessary to submit a supplemental form when the subject's FBI number and fingerprint classification are furnished by FBIHQ. However, these items should be modified in the subject's NCIC Wanted Person File entry when a positive identification is indicated via Form 1-374.

EFFECTIVE: 04/19/91

14-15.4.5 Results of Submission

(1) When NCIC provides the CJIS Division with the warrant information which has been entered into the Wanted Person File, the wanted notice on any Federal fugitive is routinely placed in the CJIS Division criminal record or in the automated name indices if no record exists.

(2) Arrest and disposition data should be promptly forwarded to the CJIS Division in all fugitive matters. Any photographs of the fugitive should not be furnished to the CJIS Division but should be retained in the field office files.

(a) Six months after an individual is declared a fugitive, the office of origin must review its files to determine desirability of requesting background data from the CJIS Division. SAC must personally approve each such request. If it is believed that background information in a subject's identification record might

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 14 - 39

cause prompt apprehension, request may be made at any time provided SAC personally approves same.

(b) Background data furnished from subject's identification record is forwarded by Form 1-374, the pertinent portion of which should be included in the next investigative report. Descriptive data furnished by CJIS Division may be duplicated for inclusion in investigative report. These instructions do not alter the policy of quoting complete identification record of all subjects in an investigative report. (See MAOP, Part II, 10-17.11.1.)

EFFECTIVE: 03/10/94

14-15.5 FBI Field Office Wanted-Flash-Cancellation Notice (FD-165)

EFFECTIVE: 04/19/91

14-15.5.1 Submitted for the Placing of Flash Notice in Criminal Justice Information Services (CJIS) Division when:

(1) Federal arrest warrant has not been issued.

(2) Background Investigation - Pardon Attorney's Office investigation is being conducted. (See MIOG, Part I, 73-8.3; Part II, 14-15.5.3.)

(3) Arrestee is in the Pretrial Diversion Program. (See MIOG, Part II, 14-15.5.3.)

EFFECTIVE: 11/18/96

14-15.5.2 Submitted for the Cancellation of Flash Notice when:

Need no longer exists in matters referred to in (1) above. Submit promptly.

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 14 - 40

EFFECTIVE: 04/19/91

14-15.5.3 Not Submitted for Cancellation when:

(1) Involves matter referred to in 14-15.5.1 (2) above.
Such flashes are automatically removed by FBIHQ upon notification from
Pardon Attorney or after five years, whichever occurs first. (See
MIOG, Part I, 73-8.3.)

(2) Involves matter referred to in 14-15.5.1 (3) above.
For instructions regarding removal of flashes in these instances, see
14-16.7(2).

(3) Fugitive airtel (FD-65) has been submitted to FBIHQ,
since FD-65 automatically takes precedence over any prior flash
notices.

EFFECTIVE: 11/18/96

14-15.5.4 Preparation of Form for Placing Flash Notice

(1) Make duplicate of original for field office file.

(2) No yellows necessary.

(3) Indicate on form if fingerprint classification of
subject desired.

EFFECTIVE: 03/23/92

14-15.5.5 Preparation of Form for Cancelling Flash Notice

(1) No field office file copy necessary.

(2) Stenographer should mark field office file copy of
original submitted form to show date cancellation notice submitted and
initial and date this notation.

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 14 - 41

EFFECTIVE: 03/23/92

14-15.6 Criminal Justice Agency Wanted-Flash-Cancellation Notice
(I-12)

This form is available to all local, state, and Federal
criminal justice agencies. It is not to be used by FBI field offices.

EFFECTIVE: 05/14/93

14-15.6.1 Use of Form

(1) Alleviates necessity of preparing a letter to the
CJIS Division.

(2) Same form is used to place or cancel a wanted or
flash notice.

(3) Deleted

(4) A flash notice will only be placed when fingerprints
supporting flash offense are on file in CJIS Division or submitted
with the I-12. FBI number must be quoted on the I-12 if prints not
being submitted with the I-12.

(5) Deleted

(6) Deleted

EFFECTIVE: 05/13/96

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 14 - 42

14-15.6.2 Preparation of Form

The form should be completely filled in so that the identification record for the subject can be located. FBI number should be given if known. If not known, fingerprints should be submitted.

EFFECTIVE: 03/23/92

14-15.7 Deleted

EFFECTIVE: 07/19/95

14-16 ACKNOWLEDGMENT OF FINGERPRINTS BY CRIMINAL JUSTICE
INFORMATION SERVICES (CJIS) DIVISION

EFFECTIVE: 03/10/94

14-16.1 If Submitted Fingerprints are Identical with a Prior
Record (an "Ident")

When a search through the identification files discloses prior record, the fingerprint currently received is acknowledged by an FBI identification record which sets forth in detail the fingerprint record available on the individual and furnishes an FBI number which should be quoted in all subsequent communications. Copies desired for other agencies should be indicated by the contributor on the fingerprint card and not in a cover letter. Requests for additional copies should be kept to a minimum.

EFFECTIVE: 12/10/91

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 14 - 43

14-16.2 If Submitted Fingerprints are not Identical with a Prior Record (a "Nonident")

When a search fails to reveal prior arrest data, an 8 1/2- x 11-inch nonident response which reads, "A search of the fingerprints on the above has failed to disclose prior arrest data" is furnished to the contributor of the fingerprint card. Copies of this response are forwarded to the agencies which will subsequently assume custody of the individual and to the FBI field office when requests for such copies are noted on the fingerprint card by the contributor. Copies will also be furnished to the State Bureaus, except when acknowledging fingerprints from a Federal agency. Beginning in February, 1983, State Bureaus participating in the Interstate Identification Index program began receiving nonident responses on-line via the NCIC network.

EFFECTIVE: 12/10/91

14-16.3 Fingerprints Submitted Involving Nonserious Offenses

All criminal fingerprint cards showing only nonserious charges are returned to the contributor without being searched through the CJIS Division files. However, when a fingerprint card bearing such data in the "charge" block is submitted to resolve a question of identity or for a current investigative purpose, it is searched through the files of the CJIS Division and both it and the results of the search are returned to the contributor. An agency which requested a flash or wanted notice and the contributor of the current fingerprints are notified if a match is made. Fingerprint cards returned to a contributor are not made a part of the FBI identification record.

EFFECTIVE: 03/10/94

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 14 - 44

14-16.3.1 Examples of Nonserious Offense Return Fingerprint Cards
(not all inclusive)

- (1) Juvenile offenders as defined by state law (unless tried as an adult).
- (2) Charge of drunkenness and/or vagrancy.
- (3) Certain public order offenses.
 - (a) Disturbing the peace.
 - (b) Curfew violation.
 - (c) Traffic (except arrest for manslaughter, driving under the influence of drugs or alcohol, and hit and run).
- (4) Charges of "suspicion" or "investigation" (unaccompanied by criterion charge).

EFFECTIVE: 12/10/91

| 14-16.4 | Deleted |

EFFECTIVE: 03/23/92

14-16.5 Fingerprints Submitted by Local, State, and Federal
Criminal Justice Agencies

EFFECTIVE: 03/23/92

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 14 - 45

14-16.5.1 Multiple Submissions

Agents in daily contact with local, state and Federal criminal justice agencies should be alert to detect instances of multiple fingerprinting of the same individual by two or more agencies on the same or a related offense. This causes unnecessary work by the [CJIS] Division and could be eliminated by a notation on the reverse side of the fingerprint card requesting additional copies of record(s) for agencies which might otherwise fingerprint the individual for the offense.

EFFECTIVE: 03/10/94

14-16.5.2 Unacceptable Submissions which Request that Copy of Record Be Mailed to FBI Field Office

(1) When fingerprints bearing the notation "Send copy to FBI office" are received from a local, state, or Federal criminal justice official and these fingerprints are not acceptable for [CJIS] Division files, a copy of a form letter returning the prints to the contributor will be designated for the field office indicated on the fingerprint card. Stamped on the field office copy of this form letter is the following statement: "If this individual is subject of Bureau case, you should follow to ensure that acceptable fingerprints are submitted to FBIHQ. If prints cannot be obtained, advise FBIHQ by letter giving reason."

(2) There will be occasions when new prints are not readily obtainable because subject is no longer in custody, charges have been dismissed, or it would not be feasible to insist on fingerprints. This information and your recommendations should be forwarded to FBIHQ in a UACB letter.

(3) When dealing with local, state, or Federal criminal justice agencies, remember that if an acceptable set of fingerprints had been received, the reply would have been mailed in the form of an identification record with copies to the appropriate field offices if the subject had prior criminal prints on file. If the [CJIS] Division had no prior criminal history record for the subject, the reply would have been in the form of a "nonident" response.

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 14 - 46

EFFECTIVE: 03/10/94

14-16.6 Mail and Wire Service

EFFECTIVE: 11/21/89

14-16.6.1 First-Class Mail

All written acknowledgments to requests received in the
| CJIS | Division are sent by first-class mail. In addition to this
standard procedure, answers forwarded in excess of 350 miles are
transported by air. If requested by submitting agency, the
acknowledgment is sent by registered mail.

EFFECTIVE: 03/10/94

14-16.6.2 Wires on Wanted

Wires are sent via the National Law Enforcement
Telecommunications System, Inc. (NLETS) when NCIC agency identifiers
(ORIs) are available; otherwise, wires are sent collect.

EFFECTIVE: 11/21/89

14-16.6.3 Special Handling

A notation on the reverse side of the fingerprint card in
the space provided to indicate "special handling" is sufficient and no
cover letter is necessary.

EFFECTIVE: 11/21/89

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 14 - 47

14-16.6.4 Not Automatically Forwarded

Current copies of arrest records are not forwarded automatically to agencies which had previously submitted fingerprint cards unless agency has posted a wanted or flash notice against the record.

EFFECTIVE: 11/21/89

14-16.7 Fingerprints Submitted Involving Pretrial Diversion
Program (PDP)

(1) In the event the fingerprint card precedes the FD-165, the PDP offense should be indicated on the form. The U.S. Attorney determines the eligibility of an offender for the PDP, and then refers the case to the Chief Pretrial Services Officer. In cases not under FBI investigative jurisdiction, the PDP Coordinator submits the divertee's fingerprints to the FBI CJIS Division on the criminal fingerprint card (Form FD-249), together with an I-12 Flash Notice indicating diversion, the expiration date of the diversion period, and a request that the Pretrial Services be notified if an arrest occurs during the supervised diversion period. The charge should be indicated in the "Charge" block of the fingerprint card and "Pretrial Diversion" in the "Disposition" block. Upon completion of the diversion period, the Chief Pretrial Services Officer will submit a Final Disposition Report (R-84) to the CJIS Division. This information will be added to the divertee's identification record to indicate "Successful Completion - Charges Dropped."

(2) In a diversion case under the FBI's investigative jurisdiction, the Office of Origin must ensure that the subject's fingerprint card (FD-249) is submitted to the CJIS Division, together with an FD-165 Flash Notice indicating the diversion and the expiration date of the diversion period, and requesting that the FBI field office be notified if an arrest occurs during the supervised diversion period. The "Charge" should be indicated in the charge block of the fingerprint card and "Pretrial Diversion" in the disposition block. The Office of Origin must also ensure that the CJIS Division is advised by FD-165 to cancel the flash if the diversion period is terminated at any time prior to its expiration. Upon completion of the diversion period, the Office of Origin must ensure that a Final Disposition Report (R-84) is submitted to the CJIS Division. This information will be added to the divertee's identification record to indicate "Successful Completion -

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 14 - 48

Charges Dropped." (See MIOG, Part II, 14-15.5.3(2).)

(3) The CJIS Division will retain the PDP information and disseminate this information to all authorized recipients of the record for the period of the diversion and for three years after the successful completion of the diversion period. If the PDP is revoked, proper notification should be submitted to CJIS Division via Form R-84 indicating the PDP has been revoked and the date of revocation. If no information is received by the CJIS Division indicating the diverttee failed to successfully complete the diversion period, the CJIS Division will handle the record as if the diversion period was successfully completed. After the three-year period, there will be no further dissemination of the information pertaining to the Pretrial Diversion. Once the three years have expired after the successful completion of the diversion program, any fingerprint cards regarding the diversion will be expunged from the CJIS Division file and destroyed. If an additional arrest fingerprint card is received by the CJIS Division within the period of diversion or the three years following the diversion period, the Pretrial Diversion record will not be expunged and will be retained indefinitely.

(4) Fingerprint card submissions involving PDP CHILD PORNOGRAPHY CASES are permanently retained by the CJIS Division. The record of the Pretrial Diverttee's involvement with CHILD PORNOGRAPHY will not be expunged and is subject to dissemination regardless of whether the Pretrial Diverttee successfully completed the Pretrial Diversion Period. In each case this is based upon a Pretrial Diversion agreement between the diverttee and the U.S. Attorney's Office which provides that the FBI may maintain a permanent record of the fingerprint card and of the diverttee's involvement in the PDP as a result of the CHILD PORNOGRAPHY CASE.

EFFECTIVE: 12/02/94

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 14 - 49

14-16.8 Fingerprints Submitted Involving Federal Youth Corrections Act

(1) With the enactment of the Sentencing Reform Act of 1984 (a part of the Comprehensive Crime Control Act of 1984, Public Law 98-473 which was signed into law on October 12, 1984), the Federal Youth Corrections Act was repealed. The Department of Justice has taken the position that the repeal of the Act is applicable only to offenses committed after the date of enactment. Although the Act may still be applied to crimes committed prior to October 24, 1984, if Judges so choose, Government attorneys should argue in individual cases that Judges should not exercise their discretion to impose sentence under the Act.

(2) When an individual has been sentenced under the provisions of the Federal Youth Corrections Act, the United States Parole Commission (USPC) is authorized to grant an "unconditional discharge" before the expiration of the maximum sentence imposed (Title 18, USC, Section 5021). In such case, the USPC automatically sets aside the conviction and issues the youthful offender a "Certificate Setting Aside Conviction."

(3) Upon receipt of a copy of the certificate setting aside the conviction, the FBI/CJIS/Division, with concurrence of the United States Department of Justice, returns the corresponding fingerprint card(s) to the original contributor(s) if the FBI identification record has not been automated. If the FBI identification record is an automated record, the corresponding fingerprint card(s) is removed from CJIS/Division's Criminal File and destroyed. The return/destruction of the fingerprint card(s) results in the complete expunction of the arrest and conviction data from FBI/CJIS/Division's Criminal File.

EFFECTIVE: 03/10/94

14-17 EXPUNGEMENT OF FINGERPRINTS BY THE CRIMINAL JUSTICE
INFORMATION SERVICES (CJIS) DIVISION

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 14 - 50

EFFECTIVE: 03/10/94

14-17.1 Fingerprints Submitted by Federal Criminal Justice
Agencies

The U.S. Department of Justice has advised that arrest fingerprints taken by a Federal agency or by a non-Federal agency at the request of a Federal agency are official U.S. Government records. As such, they cannot be destroyed, except upon the issuance of a Federal court order. USAs have been instructed to vigorously oppose motions to expunge Federal criminal history records unless the USA is convinced that the interests of justice require that a record be expunged. For example, expunction may be appropriate when an arrest is based upon a case of mistaken identity. Complete instructions pertaining to requests for expunctions (fingerprints and photographs) relating to Federal cases are found in Department of Justice Memorandum Number 765 to All United States Attorneys, dated March 6, 1972, captioned "Motion for discovery, or expungement of, arrest records held by FBI."

EFFECTIVE: 11/21/89

14-17.2 Fingerprints Submitted by Local and State Criminal Justice
Agencies

(1) The FBI/CJIS/Division is the central repository for fingerprint cards submitted by local or state criminal justice agencies. Therefore, a request from the submitting agency to delete arrest data from an FBI identification record will be complied with. The corresponding fingerprint card(s) results in the complete expunction of the arrest data from the Criminal File.

(2) The CJIS/Division limits notifications regarding expungements to the agency which contributed the arrest data being deleted and the state identification bureau servicing that agency. An exception to this general rule is made when a court order directing the expungement/sealing of an arrest specifically states that all prior recipients of the identification record are to be notified of the deletion and/or furnished with a current identification record.

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 14 - 51

EFFECTIVE: 03/10/94

14-18 FINGERPRINT CLASSIFICATION FORMULA

EFFECTIVE: 11/21/89

14-18.1 Henry Classification

EFFECTIVE: 11/21/89

14-18.1.1 Submission Accompanying Request for Record

Supplementing request for identification records with the fingerprint classification formula assists in making a search, particularly in the case of common names. In quoting fingerprint classifications in requests, care should be exercised not to confuse letters with numerals or small letters with capital letters.

EFFECTIVE: 11/21/89

14-18.1.2 Examples

- (1) Small letters and capital letters.

6 1aUta 10
1 Tr

- (2) Letters and numerals.

8 0 5 U IOI 16
I 19 W MII

IOI

The portion of the classification MII would read as inner, outer, inner, over meeting, inner, inner. The booklet, "The Science of Fingerprints," should be consulted for assistance in this matter.

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 14 - 52

EFFECTIVE: 11/21/89

14-18.2 NCIC Classification

EFFECTIVE: 05/25/90

14-18.2.1 Derivation

NCIC fingerprint classification is derived from description of each fingerprint beginning with right thumb, which is #1 and continuing through finger #10, with left thumb being #6. Two characters are used in describing each pattern. The designation of the arch is AA; the tented arch is TT. The ulnar loop is described by using the actual ridge count. For example, the number 08 and 15 represent ulnar loops with eight and fifteen ridge counts, respectively. Radial loops are described with their actual ridge count plus fifty. For example, 62 would refer to a 12 count radial loop. Whorls are designated by type and tracing with the first character indicating type, and the second the tracing, i.e., P for plain whorl; C for central pocket loop; D for double loop and X for accidental type whorl; I for inner; M for meeting; and O for outer tracings. For example, a double loop whorl with inner tracing would be designated by the letter DI. Missing fingers are indicated by the characters XX and mutilated or completely scarred patterns are indicated by the letters SR.

EFFECTIVE: 05/25/90

14-18.2.2 Example

The following is an example of NCIC fingerprint classification when #1 is an ulnar loop, 7 count; #2, radial loop, 16 count; #3, plain arch; #4, tented arch; #5, plain whorl, inner tracing; #6, double loop whorl, meeting tracing; #7, central pocket loop whorl, outer tracing; #8, accidental whorl with meeting tracing; #9, finger is missing; and #10, pattern mutilated and/or completely scarred:

07 66 AA TT PI DM CO XM XX SR

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 14 - 53

EFFECTIVE: 05/25/90

14-19 CRIMINAL JUSTICE INFORMATION SERVICES (CJIS) DIVISION'S
AUTOMATED SERVICES SYSTEMS

The CJIS Division's automated services computerized system has, in part, replaced the traditional manual fingerprint card processing functions within the CJIS Division.

EFFECTIVE: 03/10/94

14-19.1 Three-Phase Plan

EFFECTIVE: 05/25/90

14-19.1.1 Phase I

This phase of automation was implemented in August, 1973. It provided for the computerization of the names, physical descriptors, and arrest data appearing on the incoming fingerprint cards of first-time offenders, and for the computer generation of "No Record" responses to the contributors of the cards. Once the records were entered into automated files, they could be updated with subsequent arrest and disposition data, and computer-printed rap sheets could be generated in response to requests for such records.

EFFECTIVE: 09/25/91

14-19.1.2 Phase II

This phase became operational in October, 1979. It provided expanded Phase I capabilities, as well as automated name searching of the computerized arrest record file.

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 14 - 54

EFFECTIVE: 09/25/91

14-19.1.3 Phase III

This phase became operational in June, 1989. It provides greatly enhanced Phase I and Phase II capabilities, as well as the ability to perform automated on-line name and fingerprint searches. This system permits a much shorter processing time.

EFFECTIVE: 09/25/91

14-19.2 Automatic Fingerprint Reader System (AFRS)

An automatic fingerprint reader system (AFRS) is a computerized system which will electronically scan and read a fingerprint, enhance its ridge structure, and detect and record, in digital form, the characteristic minutiae data in a processing time of less than one second per fingerprint. The prototype of this system was called FINDER (contraction of FINGERprint reader). However, this name is a proprietary term belonging to the company that developed FINDER, and is no longer used by the FBI except as a historical reference. There are five production model AFRSs in the CJIS Division. These systems were used to convert the massive file of master criminal fingerprint cards of all criminal subjects having 10 finger impressions who were born on or after 1/1/29. Current incoming fingerprint cards of all individuals are read by the AFRSs if an ident is not made against the Automated Name Search and, using other specialized computers developed to perform high-speed matching, are searched against the master criminal fingerprint card digital file at computer rates of speed.

EFFECTIVE: 03/10/94

14-20 INTERNATIONAL EXCHANGE OF FINGERPRINTS

EFFECTIVE: 09/25/91

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 14 - 55

14-20.1 History

The international exchange of fingerprints and related identification data was inaugurated in 1932.

EFFECTIVE: 09/25/91

| 14-20.2 Submission Requirements | (See MIOG, Part II, 14-20.3.) |

(1) Individual's fingerprints must be submitted to the
| Criminal Justice Information Services (CJIS) | Division in duplicate.

(a) One copy is searched, acknowledged, and retained
| in the files of the | CJIS | Division.

(b) Other copy and available criminal history
information are transmitted to the country of birth for storage in its
files.

(2) Fingerprints must be legible to be referred to
foreign bureaus.

(3) Exact date and place of birth.

(4) Last known foreign address.

(5) Names of parents.

(6) Mother's maiden name.

(7) Names and addresses of any relatives residing in the
country concerned.

EFFECTIVE: 03/10/94

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 14 - 56

14-20.3 Necessity for Personal Data

(1) Except in United States and British possessions, the personal data outlined above (3) through (7) are necessary to ensure a thorough search.

(2) Foreign inquiries unsupported by fingerprints will be handled.

EFFECTIVE: 12/20/82

14-20.4 Acknowledgment of Foreign Search

(1) Foreign search information received by the [CJIS] Division is transmitted to the original contributor of the prints for any action deemed advisable.

(2) Follow-ups are maintained in all instances until cases are completed.

EFFECTIVE: 03/10/94

14-21 SURVEYS OF FINGERPRINT BUREAUS

The [Criminal Justice Information Services (CJIS)] Division will conduct surveys and assist in the establishment of a fingerprint identification bureau in a local criminal justice agency. It is desired that the SAC advise FBIHQ, Attention: [CJIS] Division, concerning the request for survey or establishment of a fingerprint bureau in a local agency. Any additional facts concerning a local agency's needs for survey or whether it can be performed by an Agent in the office should also be submitted. FBIHQ will determine whether it should be performed by an Agent in the field office or by one of the [CJIS] Division's technical experts.

EFFECTIVE: 03/10/94

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 14 - 57

14-22 FBI LITERATURE CONCERNING CRIMINAL JUSTICE INFORMATION
SERVICES (CJIS) DIVISION WORK AND FUNCTIONS

EFFECTIVE: 03/10/94

14-22.1 "The Science of Fingerprints"

This booklet is not available for general distribution to criminal justice agencies; however, it is available to the field for distribution, free of charge, to class members in basic fingerprint schools handled by FBI personnel if the student does not already possess a copy. Requests by criminal justice agencies for more than one copy will not be processed by the FBI. To obtain multiple copies of this booklet, a criminal justice agency should address a letter to the Superintendent of Documents, Government Printing Office, Washington, D.C. 20402, and enclose the necessary remittance.

EFFECTIVE: 12/20/82

14-22.2 Other Literature

FBIHQ has available for distribution to criminal justice agencies literature concerning all phases of identification matters, latent prints, and the Latent Fingerprint Section. These pamphlets are reprints of articles which have appeared in the FBI Law Enforcement Bulletin.

EFFECTIVE: 11/21/89

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 14 - 58

14-23 SUMMARY OF THE SERVICES OF THE CRIMINAL JUSTICE
INFORMATION SERVICES (CJIS) DIVISION

(1) Will process criminal, law enforcement/criminal justice, applicant and personal identification cards. Applicant cards for other than law enforcement/criminal justice agencies, will be processed for a fee. (Refer also to 14-4.1.1 and 14-5.1.)

(2) Deleted

(3) Will place wanted notices, flash notices and missing person notices in the CJIS Division, Automated Services System.

(4) Deleted

(5) Deleted

(6) Deleted

(7) Deleted

(8) Will handle fingerprint cards for international exchange.

(9) Deleted

(10) Deleted

EFFECTIVE: 08/18/94

14-24 FBIHQ SUPERVISION

EFFECTIVE: 11/21/89

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 14 - 59

14-24.1 Request for Information

- (1) During workday (8 a.m. to 4:30 p.m.) call extension [REDACTED] ba
- (2) During nonworkday and on workday before 8 a.m. and after 4:30 p.m., call extension [REDACTED]
- (3) Direct written request to office of Inspector-Deputy Assistant Director (Operations), Room 11262, JEH Building.

EFFECTIVE: 03/23/92

14-24.2 Request for Fingerprint Cards and Jackets

Due to their voluminous number and the necessity to have them immediately available, fingerprint cards and jackets are not sent outside the CJIS Division, except to the Investigative Operations and Support Section of the Laboratory Division and the Violent Crimes/Fugitive Unit of the Criminal Investigative Division. Personnel from these work areas are to obtain and handle them as follows:

- (1) If FBI number not known, call extension [REDACTED] or direct written request to Room 11262, JEH Building.
- (2) If FBI number is known, call [REDACTED] to obtain jacket.
- (3) Cards or jackets will have attached 7- by 8-inch pink card (Form 1-210) containing instructions regarding handling and transfer. This form also serves as a routing slip to return card or jacket to the CJIS Division, and should not be removed.
- (4) To transfer individual criminal fingerprint card, call extension [REDACTED]
- (5) To transfer individual civil fingerprint card, call [REDACTED]
- (6) To transfer a fingerprint jacket, call [REDACTED]

The above transfers are necessary even though the card or jacket is

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 14 - 60

being forwarded to an individual or section in the CJIS Division for handling prior to being filed. Cards and jackets shall not be held more than one week; however, if necessary to retain longer, recharge by telephoning above-referred-to numbers. Cards and jackets are to be returned to the CJIS Division in a routing envelope.

Microfilming of fingerprint cards is being done to save space within the CJIS Division. If a requested jacket or fingerprint card is on microfilm, a copy of the microfilmed record or fingerprint card will be made and sent in answer to the request. Microfilmed jackets are complete copies of the original hardcopy jackets. Microfilmed fingerprint cards are complete copies of the original fingerprint card. Copies of microfilmed jackets or fingerprint cards do not have to be returned. They may be disposed of (e.g., destroyed) in a secure manner.

EFFECTIVE: 12/13/95

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 15 - 1

SECTION 15. LATENT FINGERPRINT IDENTIFICATION

- 15-1 DUTIES OF LATENT FINGERPRINT SECTION (See MIOG, Part I, 7-14.9(1)(b), 7-14.11(8), 9-7(3), Section 32, 91-17.3(1), 91-18, 145-2(3), 192-16.1(1), 192-16.3(1), Part II, 13-6.4.5 & 13-17.)

All work pertaining to the development and comparison of latent prints, the comparison of infant footprints, automated latent fingerprint searching, the National Unidentified Latent File, and the examination of fingers and hands of deceased individuals, is handled in the Latent Fingerprint Section. Senior fingerprint specialists of the Section form the nucleus of the FBI Disaster Squad which assists in the identification of victims of major disasters. The Section handles all court testimony needed in regard to fingerprint examinations and also conducts training classes regarding fingerprint matters.

EFFECTIVE: 09/24/93

15-2 FILES

EFFECTIVE: 11/21/89

- 15-2.1 Automated Searching of Latent Fingerprints (See MIOG, Part I, 91-18.1, 145-2(3), 192-16.2.)

(1) Automated Fingerprint Identification System (AFIS) technology has provided the Latent Fingerprint Section (LFPS) the capability to conduct computer-based latent fingerprint searches against the FBI database of 28 million criminals' 10-print fingerprints. This process is known as ALFS (Automated Latent Fingerprint Search), which was previously referred to as ALSA3. The Criminal Justice Information Services Division (CJIS) maintains the automated criminal 10-print fingerprint database, which is now called Identification Automated Searches.

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 15 - 2

(2) |The ALFS provides a means to solve crimes by searching unidentified latent fingerprints against the known fingerprint records of criminals. This capability is intended to be a last effort to solve a crime from a fingerprint standpoint. The traditional practice of naming suspects/subjects from the investigative process, along with the acquisition of elimination fingerprints from victims and others, is expected to continue. It is not necessary to specifically request an ALFS search as each case submitted for latent fingerprint examination is evaluated by the LFPS to determine if it meets the criteria for initiating a search. However, if it is known at the time of submitting the case that there are no suspects developed and the only purpose of submitting the case is for an ALFS search, then the request should be specifically stated. |

(3) |When requesting an ALFS search, it should be understood that not all latent fingerprints are suitable for this type of search. Although the latent fingerprints may be of value for identification purposes by a fingerprint specialist, it may not be sufficient for the computer-based search. The ALFS search relies on the ability of the fingerprint specialist to determine an approximate fingerprint classification and finger position of the latent fingerprint and the availability of a physical description of the suspect(s). |

(4) To better facilitate the ALFS search, submit all physically descriptive information known about the suspect(s). The physical descriptors which can be utilized in an ALFS search include sex, race, age range, height range, weight range, eye color, hair color, place of birth (state or country), and scars, marks and tattoos (the location on the body). All these physical descriptors are not necessary to conduct an ALFS search, but as much of this information as known should be included in your correspondence.

(5) ALFS searches may also be restricted to specific geographic areas (on state or country level) and any crime-type category.

(6) Before the LFPS fingerprint specialist determines that an ALFS search can be performed, it may be necessary to contact the requesting office for further clarification or additional information to more efficiently use this capability.

(7) The ALSM (Automated Latent System Model) capability has been discontinued and is no longer available. ALSM was strictly a model and plans are being made to provide a similar yet more robust

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 15 - 3

capability within the future Integrated Automated Fingerprint Identification System (IAFIS).|

EFFECTIVE: 07/21/95

15-2.2 National Unidentified Latent File

This file consists of classifiable latent fingerprints developed and remaining unidentified in certain types of Bureau cases having an unknown subject. Categories in this file consist of Bank Robbery, Bank Burglary, Bank Larceny, Bank Matters-Devices, Interstate Transportation of Stolen Property-Checks, Major Theft (ITSP), Theft From Interstate Shipment, Police Killings, Airline Threats, Interstate Transportation of Obscene Material, Interstate Transportation of Stolen Motor Vehicle, Kidnaping, Sabotage, Espionage, Explosives, Extortion, Hobbs Act and Terrorism. The inked fingerprints or major case prints of subjects received in the Latent Fingerprint Section in connection with these violations are compared with the latent prints in the specific type of violation. For example, the fingerprints or major case prints of subjects submitted in a current bank robbery case are compared with the latent prints remaining unidentified in the bank robbery section of the National Unidentified Latent File. (See MIOG, Part I, 91-9(1) and 91-18.2.)|

EFFECTIVE: 05/14/93

15-3 LATENT PRINT EXAMINATIONS

EFFECTIVE: 11/21/89

15-3.1 Examination of Evidentiary Materials - Bureau Cases, State and/or Local Facilities

EFFECTIVE: 11/21/89

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 15 - 4

15-3.1.1 Utilize Technical Expertise of FBI's Latent Fingerprint Section

Materials of evidentiary value located at crime scenes, or otherwise obtained during our investigative activities, offer invaluable potential for investigative information and probative results. The laboratory facilities in the Latent Fingerprint Section and technical expertise of FBI latent fingerprint personnel are recognized as the finest in the world. These technical fingerprint experts are devoted 100 percent to the science of latent print technology. Also, the file data base of persons represented in the fingerprint files of the FBI Criminal Justice Information Services Division is far greater than that available to state and/or local authorities. For these reasons the technical superiority of the Latent Fingerprint Section should be utilized in Bureau cases requiring latent print examinations.

EFFECTIVE: 04/01/96

15-3.1.2 Joint Jurisdiction

Instances may arise in matters of joint jurisdiction where state and local crime laboratories handle materials obtained by local criminal justice agencies prior to our involvement, or have custody of items located during their investigations of concurrent violations. Such situations call for the exercise of diplomacy and good judgment to avoid creating the impression that the FBI lacks respect for the investigative, technical or scientific competence of local authorities. However, the laboratory facilities in the Latent Fingerprint Section and technical expertise of FBI latent fingerprint personnel are recognized as the finest in the world and should be utilized if at all possible. It should be borne in mind that the Latent Fingerprint Section utilizes laser and other light sources for the detection of latent prints, and this should be taken into consideration, inasmuch as local authorities may not have access to these light sources. In matters of joint Federal/local jurisdiction, we must be positive to ensure that in the event of Federal prosecution, the U.S. Attorney may be certain that the more stringent Federal safeguards for the handling of evidence have been followed. Processing by the Latent Fingerprint Section will offer this guarantee.

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 15 - 5

EFFECTIVE: 05/14/93

15-3.1.3 Conditions to Be Met for Use of State or Local Facilities

When circumstances and good judgment dictate that consideration be given to utilizing state or local fingerprint technicians and/or crime laboratory personnel in Bureau cases, the following conditions must be met before your decision is made:

(1) The SAC must be fully aware of the facts of the case and the nature of the examination(s) to be conducted. Inasmuch as the Latent Fingerprint Section utilizes a laser and other light sources as the initial process in the detection of latent prints, consider whether this technique is available at the local or state level.

(2) Extenuating circumstances must exist which justify SAC approval of the utilization of state/local facilities and personnel.

(3) As soon as time permits, the FBI Laboratory Division should be contacted to assure that all necessary examinations are being performed. Bear in mind, that concurrent violations frequently require different elements of proof. State and local facilities must therefore be alerted to the nature of Bureau requirements so that nothing will be done to the evidentiary material that will destroy its usefulness from our standpoint. They should also be made aware of our willingness to consult with them on scientific and technical aspects of their examinations as well as provide additional examinations that may not be possible locally.

(4) In each case where local examinations are conducted, a copy of the report of same should be furnished the FBI Laboratory Division when such becomes available.

EFFECTIVE: 09/24/93

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 15 - 6

15-3.1.4 Negative Aspects of Preliminary Local Analyses

Under no circumstances should "curbstone" opinions be sought of local scientific or technical personnel to assess the potential value of evidentiary materials prior to submitting these items to FBIHQ for examination. Any preliminary local analyses could cause alteration and/or contamination of these materials and a possible conflict of opinion due to variation in testing procedures. This could severely hamper the effectiveness of our efforts, as well as possible unduly complicate the "chain of custody."

EFFECTIVE: 08/17/84

15-3.2 Searching for Latent Prints

The search for latent prints should be conducted in a systematic, intelligent manner. Articles bearing or suspected of bearing impressions must be handled with care as most impressions are extremely susceptible to injury. The slightest contact with another surface will usually be sufficient to destroy them; consequently, it is not an adequate safeguard if the person handling such articles merely protects his/her hands with gloves. By doing so, he/she may prevent impressions of his/her own hands being left, but even his/her gloved hands must not come in contact with a surface which might bear impressions. |Avoid handling articles when wearing thin skintight rubber-type gloves since it is possible that latent impressions can be left due to the thinness and tightness of the gloves.| If an article must be handled, it should be done in such a way that the hands whether bare or protected, do not touch a receptive surface. Should that be impossible, the part of the article which it is desired to handle should first be examined for visible and latent impressions. The light from a flashlight or the lights of a fingerprint camera are sometimes helpful in locating latent prints as the light reflected at an angle often shows the presence of latent prints. Latents should be searched for in the following circumstances:

(1) Surfaces and articles which might have been handled by the criminal at the scene of the crime. |Circumstances may warrant examining certain areas of a victim's body for latent prints left on the skin.|

(2) Property recovered in any circumstance if it is believed to be the proceeds of theft.

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 15 - 7

(3) Vehicles, weapons, tools, and other articles which may have been used in the commission of a crime even though they are recovered at a distance from the crime.

When impressions have been caused by a substance which contrasts in color with the surface on which they are made, they will usually be visible, though they may not be conspicuous. Such impressions would result from a dirty, oily or bloody hand coming in contact with a relatively clean surface. If the impressions have been made in plastic substances, such as wax, clay, etc., they will, of course, be visible.

EFFECTIVE: 08/17/84

15-3.3 Development of Latent Impressions (See MIOG, Part II, 15-4.1.)

(1) All evidence that is not too bulky or valuable to be shipped should be submitted to the Latent Fingerprint Section, Laboratory Division, for latent print examination. Examination with the laser is the initial process used for detecting latent prints; that is, it should be used before treatment with fingerprint powders or chemicals. After the laser examination and prior to the utilization of fingerprint powders, Latent Fingerprint Section specialists can enhance the possibility of developing latent prints on certain nonporous articles, such as plastic bags and other pliable plastics, by subjecting them to fumes from cyanoacrylate glue. Consideration should be given to contacting field office Evidence Response Team (ERT) members for possible treatment of nonporous items with cyanoacrylate glue prior to submitting to the Latent Fingerprint Section. ERT members also are knowledgeable in the packaging of specimens for shipment to the Laboratory.

(2) The powders in use at the present time are gray, black, aluminum, "dragon's blood," and bronze. Black and gray powders should be generally used inasmuch as they most often give the best results. Black powder is used on surfaces with a light background and gray powder on dark surfaces. It is desirable to emphasize that in many instances it is not necessary that any powder be applied to a latent impression to develop it, as sometimes these impressions appear clearly. Visible prints should be photographed before any attempt is made to improve by powdering. Conventional powders are to be used to bring the print to a point where it may be photographed or otherwise recorded. Fluorescent powders should not be routinely used and only

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 15 - 8

considered after conventional powders prove nonproductive. The visualization of fluorescent prints requires a special light source and the photography of such prints is more time consuming. Further, surfaces processed with fluorescent powders should be thoroughly cleaned as the presence of fluorescent powder cannot be readily detected without the aid of a light source and may pose a health risk if subsequently handled. Any item which bears a latent print in blood (or resemblance of a latent print in blood) should not be examined using powders, but should be submitted to the Latent Fingerprint Section. All visible latent prints on items to be shipped to the Latent Fingerprint Section should be photographed before shipment. Where a print may show distinctly in the oil and grease on an automobile, no powder should be used. Where powders are utilized, those which contrast in color with the surface should be used. Mirrors and highly polished surfaces photograph black, and this must be kept in mind in selecting the proper powder to use. Powders should generally be used only on nonporous surfaces such as metal, glass and porcelain. Powder generally should not be used on paper, cloth or unfinished wood, since these specimens are chemically treated by the specialists of the Latent Fingerprint Section.

(3) Some chemicals which are used to develop latent prints are irritating to eyes, nose and throat when not used under proper conditions and will stain skin and clothing. Use of these chemicals requires close observation by a trained technician to ensure proper development of all latent prints. If a human body is to be examined for latent prints on the skin, the examination should be done immediately utilizing the cyanoacrylate powder method or any other available process. When porous-type evidence is too bulky or valuable to be shipped, a request can be made for field processing by a latent fingerprint specialist. In an instance of field processing of a crime scene by a specialist of the Latent Fingerprint Section, a Special Agent must provide security by remaining with the specialist during the processing unless appropriate security is being provided by another agency.

EFFECTIVE: 11/21/97

15-3.4 Photographing Latent Prints

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 15 - 9

EFFECTIVE: 08/17/84

15-3.4.1 The Fingerprint Camera

(1) Photographs of latent prints will show more contrast in the ridge detail than most lifts will of the same impression. It is recommended that a medium format camera, i.e., Mamiya, be used. It is not necessary to photograph the latent prints at their natural size (1:1). A fingerprint camera that has a fixed focus, its own self-contained light source and uses 120 film may also be used. If necessary, a small format 35mm camera can be used in lieu of a medium format camera. Due to its negative size, medium format cameras will produce higher quality photographs. Photograph all latent prints whether they are of good quality or not (no field evaluations).

(2) The first frame of each roll of film should depict the photographic log showing the roll number, subjects for the film and the camera settings.

(3) Each latent print should be photographed individually for better clarity. The following steps should be utilized when photographing latent prints: (a) all latent prints must be photographed with an identification tag, (b) the identification tag must include a scale, reference number, location of prints, and initials, (c) the identification tag should be placed on the same plane as the latent print, (d) fill the frame completely with the latent prints and the identification tag, (e) photograph latent prints that are close to one another in one frame, if possible, especially if they are simultaneous prints, (f) use T-Max 400 film, (g) set the f/stop to f/8, (h) adjust the shutter speed setting until the green light appears, (i) make two exposures of each latent print by bracketing--the first exposure should be what the camera suggests with the green light and the second exposure should be one stop overexposed by adjusting the shutter speed dial, and (j) maintain a photographic log. The information should correspond with the latent print log and the evidence recovery log.

EFFECTIVE: 07/21/95

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 15 - 10

15-3.4.2 Recording Location of Latent Prints

Care must be exercised to see that all latent prints developed and photographed for possible use are marked properly so that they may be identified readily. It is advisable to record in the notebook of the investigator the exact location where the latent prints were found - position on a safe door, car window, etc. Noting these facts may affect the entire presentation of the case, and all photographs or exhibits should contain reference thereto. Latent prints should be lifted after photographing whenever possible.

EFFECTIVE: 08/17/84

15-3.5 Lifting of Latent Impressions

Sometimes, due to poor contrasts, reflections of light, multicolored surfaces, or the physical location of a latent print, it is not possible to photograph the impression effectively. In all such cases, latent prints should be lifted. Latent prints should also be lifted even though photographs have been made of the impression. A black rubber lift is used for lifting latent prints where gray or aluminum powder was used in developing the latent print. The white rubber lifting tape is used for the black, dragon's blood and bronze powders. A piece of the tape large enough to cover the entire latent print to be lifted is selected. The lift must be marked properly for identification purposes. Approved transparent tape may be similarly used with the exception that the tape should be mounted on a black or white card contrasting with the color of powder used. Rubber tape generally gives better results than transparent tape on curved or uneven surfaces.

EFFECTIVE: 05/11/87

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 15 - 11

15-3.6 Elimination Prints

The fingerprints of all persons who have legitimately handled the articles must be taken for comparison with any latent prints. If latent palm prints are developed, it will be necessary also to take palm prints for elimination purposes. Consideration should be given to obtaining the prints of a deceased individual before interment. Agents should be extremely careful in handling objects so as not to leave their own prints thereon. If inadvertently handled, such information should be indicated in letter transmittal. All fingerprints submitted for elimination purposes, or as suspects, should have the necessary descriptive data on the cards. Major case prints submitted for elimination purposes, or as suspects, should appropriately be taken on separate cards. The palm prints should never be taken on the reverse side of a fingerprint card.

EFFECTIVE: 05/11/87

15-4 SUBMISSION OF EVIDENCE

EFFECTIVE: 05/11/87

15-4.1 Letters Submitting Evidence or Articles for Examination (See MIOG, Part I, 91-9(1) & Part II, 15-3.3.)

(1) Three copies of a letter submitting photographs or the lifts of latent impressions, as well as articles to be examined, should be forwarded to FBI Headquarters. The letters and packages should be addressed in the usual manner, marked "Attention: Laboratory Division, Evidence Control Center." When evidence is transmitted as an enclosure to correspondence, an evidence envelope (FD-632) should be used as the enclosure envelope. After the information is completed on the envelope, place the evidence in the envelope and seal, and staple the completed correspondence to the yellow flap of the envelope. In each instance where the evidence is too bulky to be sent enclosed, yellow transparent tape should be placed over the address label on each package. A copy of the letter should be placed in the package, and the original letter and a copy should be sent separately. Letters transmitting evidence and requesting examinations should set forth briefly all pertinent material and information which would be of value to the specialist in the course of the examination. Evidence to

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 15 -- 12

be transmitted to the Latent Fingerprint Section for examination should not be powdered for the development of latent impressions. Fragile articles should be carefully packed and the package marked fragile. On the inside wrapper of the object to be sent, the gummed labels of the Latent Fingerprint Section designating the enclosure as "Evidence" should be used.

(2) In any case where it is known that an article or specimen to be submitted may have been contaminated by a person infected with, or suspected of being infected with, acquired immune deficiency syndrome (AIDS), tuberculosis, or hepatitis, the Latent Fingerprint Section must be contacted prior to submission to determine if the examination will be conducted.

EFFECTIVE: 04/01/96

15-4.2 Latent Fingerprint Section Reports (See MAOP, Part II, 10-13.13.)

Each auxiliary office should request FBIHQ to furnish original latent fingerprint reports and, if appropriate, the evidence to the office of origin upon completion of the latent examinations.

EFFECTIVE: 09/24/93

15-4.3 Submission of Fingerprint Cards (or Major Case Prints) for Comparison

In submitting fingerprint cards for comparison with latent fingerprints in connection with any specific case, a letter should also be directed with the fingerprints to the Laboratory Division, Evidence Control Center, requesting such comparison. When fingerprint cards are submitted for comparison purposes with any latent fingerprints, the criminal-suspect or noncriminal-elimination nature of these prints should be indicated. Criminal prints that do not contain the necessary data for retention in the Criminal Justice Information Services Division files, as well as suspect and elimination prints, are returned to the contributor.

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 15 - 13

EFFECTIVE: 04/01/96

15-4.4 Preservation of Specimens During Shipment

(1) In sending exposed films to the Latent Fingerprint Section, Laboratory Division, in connection with latent fingerprint cases, the outside of the package should be marked "undeveloped films," in order that they may be handled properly at FBIHQ. All articles, with the exception of paper specimens, should be packed for transfer in such a manner that surfaces which bear latent impressions cannot come into contact with any other surface or substance. The most effective method to do this is to mount the articles on a baseboard. The board can then be fastened inside a stout container. With reasonable ingenuity, practically any article can be secured so that its surfaces are protected. Absorbent material, such as newspapers, cotton, or cloth, should never be placed next to the article. Generally, when photographic negatives and photographs of latent prints are submitted by the field, they will be retained in the Latent Fingerprint Section. Other material submitted for latent fingerprint examination will be returned unless the letter covering the submission of the evidence requests its destruction.

(2) In the event it is necessary to transmit the fingers, hands, or feet of a deceased individual to the Latent Fingerprint Section for examination, they should be placed in a container of 70 percent solution of alcohol, and this should be stated in accompanying correspondence. Entire hands should not be submitted unless there is a special need to do so. When submitting the fingers, each finger should be amputated and placed in an individual container, and appropriately labeled (right thumb, right index, etc.). Requirements for labeling, marking and shipping of body parts should be determined by contacting the carrier.

EFFECTIVE: 11/21/97

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 15 - 14

15-5 REQUESTS FOR COPIES OF LATENT PRINTS

Inasmuch as all latent fingerprint comparisons are to be conducted by the experts of the Latent Fingerprint Section, requests for photographic copies of latent prints will not be honored unless the letter requesting such photographs states specifically the use to which these photographic copies are to be placed.

EFFECTIVE: 05/11/87

15-6 LIAISON WITH U.S. AND PROSECUTING ATTORNEYS

Maintain close liaison with U.S. and Prosecuting Attorneys to ensure prompt notification of trials or changes in trial dates involving testimony of latent fingerprint specialists. Communications regarding such are to be marked for Attention: Latent Fingerprint Section, Laboratory Division, and should refer to the pertinent latent case number(s).

EFFECTIVE: 09/24/93

15-7 COURT DECISIONS

EFFECTIVE: 05/11/87

15-7.1 Latent Fingerprint Testimony

Latent fingerprint testimony is universally accepted today by the courts of all civilized countries. Field offices should advise the Latent Fingerprint Section, Laboratory Division of any current decisions involving any phase of fingerprint testimony. In this country, such testimony is accepted in Federal, state and military courts when it is shown that the witness is a competent expert because of his/her experience and knowledge of the subject matter. Numerous court decisions in this country uphold the validity and competence of such testimony, several of which hold as follows:

(1) Holt v. U.S., 218 U.S. 245, 1910, the U.S. Supreme Court in considering the contention of the defendant's counsel that

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 15 - 15

the taking and use of fingerprints of a person and the use of same at the trial of the accused is a violation of the constitutional provision against self-incrimination held, "the prohibition of compelling a man in criminal court to be a witness against himself is a prohibition of the use of physical or moral compulsion to extort communications from him, not an exclusion of his body as evidence when it be material."

(2) Duree, et al., v. U.S., 297 Fed 70, 1924, District Court of U.S. for Western District of Oklahoma held that photographs of latent prints on a bottle were admissible in evidence.

(3) Newton Grice v. Texas, 142 T.C.R. 4, 1941, Supreme Court of Texas held that testimony by a competent fingerprint expert concerning a latent fingerprint which was identified as the fingerprint of the accused, was in itself sufficient evidence to authorize the jury's finding of the accused guilty of burglary, even in the absence of collateral evidence.

EFFECTIVE: 09/24/93

15-7.2 Latent Palm Print Testimony

(1) Davis v. Dunn, 90 Vt. 253, 259, 98A, 81 Ann Cas., 1918D, 994, 1916, court stated, "This knowledge (identification by use of fingerprints) of the courts goes so far as to enable them to say, without proof, that the imprint of the palm side of the human hand, when fairly taken, presents reliable; individual, and unchanging characteristics of the papillary ridges."

(2) Supreme Court of the State of Nevada held in State v. Kuhl, 175 Pac 190, 1918, that an expert may testify positively as to the identity of two palm impressions rather than be limited to his/her belief or judgment. Further, that "all the learned authors, experts, and scientists on the subject of fingerprint identification agree that these patterns, formed by the papillary ridges on the inner surface of the human hand and the sole of the foot, are persistent, continuous and unchanging from a period in the existence of the individual extending from some months before birth until disintegration after death."

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 15 - 16

EFFECTIVE: 05/11/87

15-7.3 Latent Footprint Testimony

In the case of Commonwealth v. Oscar Bartolini, 299 Mass. 503, 1938, the Supreme Court of Massachusetts (3-1-38) held that there was no error in permitting a witness to testify as an expert witness where it is shown that, "There was ample evidence of special study and knowledge by the witness of the subject of footprints as well as of fingerprints." The Court also recognized the fact, "That footprints, like fingerprints, remain constant throughout life and furnish an adequate and reliable means of identification."

EFFECTIVE: 09/25/91

15-8 SERVICES OF DISASTER SQUAD

EFFECTIVE: 09/25/91

15-8.1 Limitations of Assistance

The FBI Disaster Squad assists in the fingerprint identification of casualties in major disasters. A request for the assistance of the FBI Disaster Squad will be honored if it originates from one of the following: the ranking law enforcement official having jurisdiction over the disaster scene; the medical examiner, coroner, or other ranking official, such as the Mayor or Governor; an official of the U.S. Department of Transportation (National Transportation Safety Board or Federal Aviation Administration); or an official of the U.S. Department of State in foreign disasters involving American citizens. Unless complete background information is needed in a case wherein the FBI has investigative jurisdiction, utilization of Agent personnel should be minimal, such as to assist the Disaster Squad at the scene. The FBI's participation will be limited to identifying as many of the casualties as possible by fingerprints. This limitation should be clearly explained to the requesting official at the time the request for the Disaster Squad's assistance is received in order that the requester will be on notice of the extent of FBI services that can be expected.

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 15 - 17

EFFECTIVE: 09/25/91

15-8.2 Action to Be Taken By Field Office Covering Disaster Site

- (1) Advise FBIHQ by telephone of disaster and whether services of the Disaster Squad have been requested.
- (2) FBIHQ will give instructions as to which office will be designated office of origin for identification phase of case if conflict exists.

- (3) Assign experienced Agent personnel to disaster scene to develop any information indicating a federal violation within the Bureau's investigative jurisdiction.

- (4) If transportation facility involved, establish close liaison with company office so as to obtain, as quickly as possible, passengers' full names and descriptions. Office covering point of origin of transportation carrier usually in best position to do this.

- (5) Furnish names and descriptive data immediately to the Criminal Justice Information Services Division so search can be made for fingerprints which may be in our files.

EFFECTIVE: 04/08/96

15-8.3 Suggested Action to Be Taken at Scene by the Official Having Jurisdiction Over the Disaster

- (1) Institute uniform body numbering system and tag remains of each casualty with assigned number. Severed portion of remains should be maintained in a separate area and labeled as to location where found.

- (2) During search of disaster scene for casualties, personal effects not definitely attached to bodies should be labeled and kept separate. Personal items removed from bodies, such as clothing, rings, etc., should be placed in individual containers and identified by number corresponding with body number. Identity of person performing this task should be recorded. FBI personnel are not to assume custody of personal valuables.

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 15 - 18

(3) Encourage use of a single central morgue. In absence of adequate conventional morgue facilities, consider gymnasium, armory, or similar large, well-lighted, well-ventilated structure and availability of a refrigerated truck.

(4) Each casualty should be fingerprinted, photographed, and a detailed physical description taken prior to release of body, regardless of means used to identify remains.

(5) Ensure that detailed and careful search is made of casualty at morgue to record jewelry, clothing, scars, marks, tattoos, and any other identifying factors. Property removed from each victim should be kept in a separate container appropriately documented where found.

(6) Suggest that services of a dentist be obtained for detailed charting of the teeth.

(7) Suggest complete pathological examination of remains with particular emphasis on evidence of previous removal or repair to internal organs, age estimate, and physical build.

(8) Relatives visiting scene or morgue should be interviewed by local officials.

EFFECTIVE: 09/25/91

15-8.4 Instructions for Auxiliary Offices

(1) Deleted

(2) Deleted

(3) In cases where FBI has investigative jurisdiction in the disaster, auxiliary offices will be expected to immediately forward items such as dental charts and fingerprints. In these instances, the cooperation of commercial aircraft personnel should be obtained to expedite delivery to the FBI Disaster Squad at the scene. Use envelopes bearing postage indicia.

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 15 - 19

EFFECTIVE: 09/25/91

15-8.5 Commercial Airlines

If commercial airlines involved in disaster, see also Part I, Section 149, of this manual for instructions regarding investigations under destruction of aircraft or motor vehicle statutes.

EFFECTIVE: 09/25/91

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 9/22/98 BY SP5 JLP

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 16 - 1

SECTION 16. TECHNICAL SERVICES

| 16-1 COMMUNICATIONS SERVICES | (See MAOP, Part II, 10-5.) |

Communications services include the transmission and receipt of official information in textual or graphical form through the use of secure and nonsecure teletype and facsimile systems.

EFFECTIVE: 07/15/93

| 16-1.1

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Sensitive
PRINTED: 02/18/98

XXXXXX
XXXXXX
XXXXXXFEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

39

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 552Section 552a☒ (b)(1)☐ (b)(7)(A)☐ (d)(5)☒ (b)(2)☐ (b)(7)(B)☐ (j)(2)☐ (b)(3)☐ (b)(7)(C)☐ (k)(1)☐ (b)(7)(D)☐ (k)(2)☒ (b)(7)(E)☐ (k)(3)☐ (b)(7)(F)☐ (k)(4)☐ (b)(4)☐ (b)(8)☐ (k)(5)☐ (b)(5)☐ (b)(9)☐ (k)(6)☐ (b)(6)☐ (k)(7)

- ☐ Information pertained only to a third party with no reference to the subject of your request or the subject of your request is listed in the title only.

- ☐ Documents originated with another Government agency(ies). These documents were referred to that agency(ies) for review and direct response to you.

Pages contain information furnished by another Government agency(ies). You will be advised by the FBI as to the releasability of this information following our consultation with the other agency(ies).

Page(s) withheld inasmuch as a final release determination has not been made. You will be advised as to the disposition at a later date.

Pages were not considered for release as they are duplicative of _____

Page(s) withheld for the following reason(s): _____

- ☒ The following number is to be used for reference regarding these pages:

MIOG Pt II Sec 16 p2-40

XXXXXXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X for this page X
XXXXXXXXXXXXXXXXXXXX

XXXXXX
XXXXXX
XXXXXX

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 16 - 41

b2
b7E

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

EFFECTIVE: 12/14/93

16-7.1.7 Administrative Unit

The Administrative Unit coordinates budget formulation and fiscal management of ES programs, provides support services to the ES including coordination, security and control of section space, telecommunications services, including secure and commercial telephones, facsimile and COMSEC, mail and courier service, automotive fleet management, inventory, personnel, procurement services, draft system, shipping and receiving; and other administrative support activities necessary for routine operation of the ES.

EFFECTIVE: 12/07/93

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 16 - 42

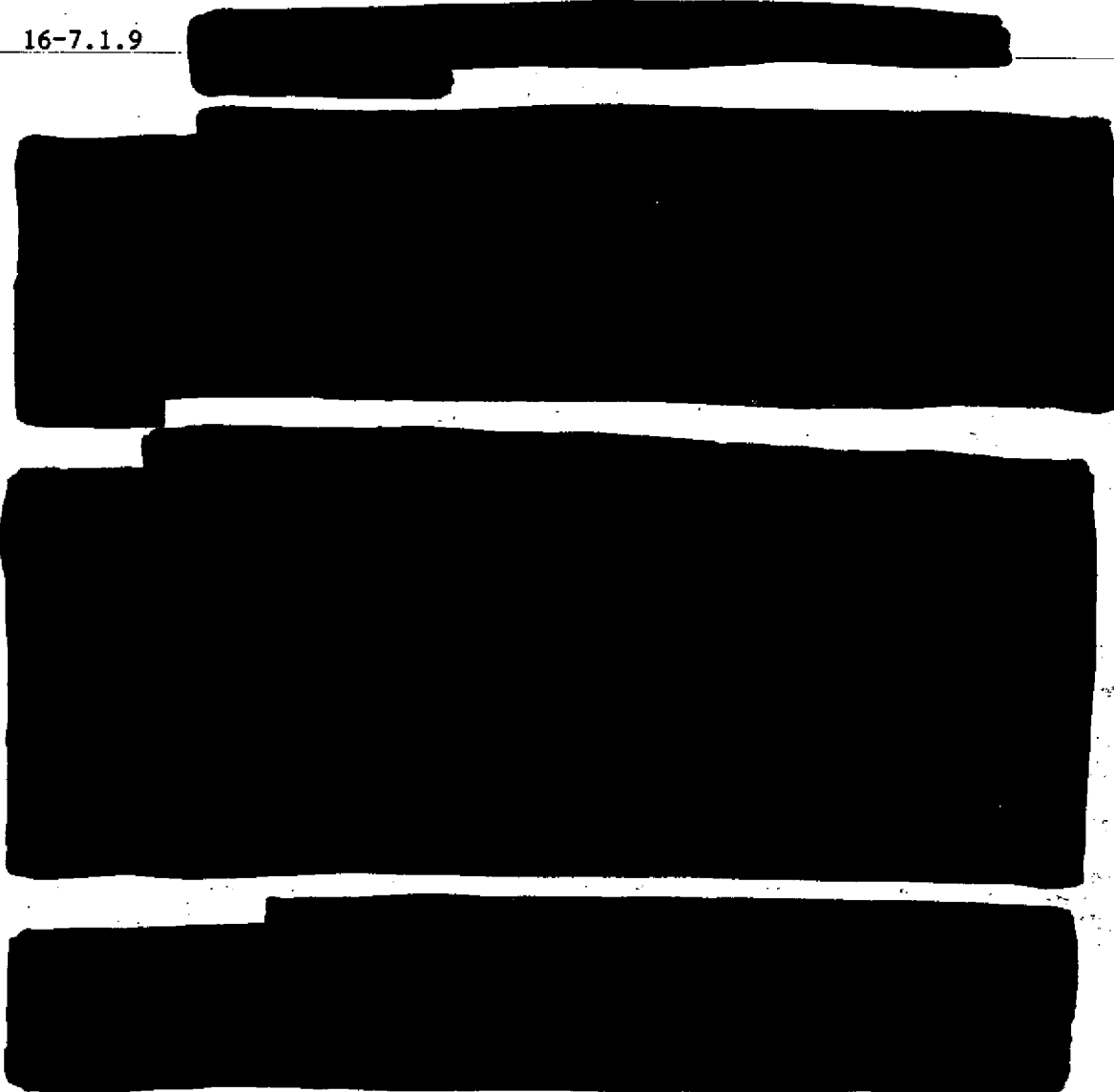
16-7.1.8 Advanced Telephony Unit (ATU)

The mission of the ATU is to formulate strategies, initiate development of methodologies and ensure the ability of the FBI to perform court-ordered electronic surveillance with respect to the emerging and future telecommunications technologies.

EFFECTIVE: 09/25/91

16-7.1.9

b2
b7E

A large rectangular area of the document is completely redacted with black ink. To the left of this redacted area, the handwritten notations "b2" and "b7E" are visible. The redaction covers the majority of the lower half of the page, starting below the "EFFECTIVE" date and ending just above the footer.

XXXXXX
XXXXXX
XXXXXXFEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

8 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 552Section 552a☒ (b)(1)☐ (b)(7)(A)☐ (d)(5)☒ (b)(2)☐ (b)(7)(B)☐ (j)(2)☐ (b)(3)☐ (b)(7)(C)☐ (k)(1)☐ (b)(7)(D)☐ (k)(2)☒ (b)(7)(E)☐ (k)(3)☐ (b)(7)(F)☐ (k)(4)☐ (b)(4)☐ (b)(8)☐ (k)(5)☐ (b)(5)☐ (b)(9)☐ (k)(6)☐ (b)(6)☐ (k)(7)

- ☐ Information pertained only to a third party with no reference to the subject of your request or the subject of your request is listed in the title only.
- ☐ Documents originated with another Government agency(ies). These documents were referred to that agency(ies) for review and direct response to you.

Pages contain information furnished by another Government agency(ies). You will be advised by the FBI as to the releasability of this information following our consultation with the other agency(ies).

Page(s) withheld inasmuch as a final release determination has not been made. You will be advised as to the disposition at a later date.

Pages were not considered for release as they are duplicative of _____

Page(s) withheld for the following reason(s): _____

- ☒ The following number is to be used for reference regarding these pages:

M106 Pt II Sec 16 p 43-50

 XXXXXXXXXXXXXXXXXXXX
 X Deleted Page(s) X
 X No Duplication Fee X
 X for this page X
 XXXXXXXXXXXXXXXXXXXX
XXXXXX
XXXXXX
XXXXXX

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 16 - 51

[REDACTED]

b2
b7E

[REDACTED]

(2) Technically Trained Agent Training Program

This program is responsible for training all field TTAs, the continued upgrading of the technical training curriculum, and for administering the TTA On-the-Job Training Program. These responsibilities include provisioning all training for TTAs, designing and evaluating new courses, identifying technical training facilities and equipment as appropriate. The program is responsible for maintaining the high level of technical knowledge required by field TTAs.

(3) Electronics Technicians Management Program (See MIOG, Part I, 67-10.10; MAOP, Part I, 11-16.3.1.)

This program is responsible for the management of the ET Program in the field. These responsibilities include maintaining field ET Program staffing levels, ET staffing for major case/crisis response incidents, specialty transfer requests, evaluation of the field ET Programs, and assisting in the recruitment, evaluation, and hiring of ETs for the field and FBIHQ. This program also oversees the activities of the Electronics Technician Advisory Committee.

(4) Electronics Technicians Training Program

This program is responsible for training of all field ETs and the continued upgrading of the training curriculum. These responsibilities include providing all radio and data communications training for field ETs, designing and evaluating new courses, and identifying technical training facilities, vendors, and equipment as appropriate. This program is responsible for maintaining the high level of technical knowledge required by field ET personnel.

Manual of Investigative Operations and Guidelines
Part II

(5) Computer Specialist Management Program

(6) Computer Specialist Training Program

(7)

Sensitive

PRINTED: 02/18/98

XXXXXX
XXXXXX
XXXXXXFEDERAL 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 552Section 552a☐ (b)(1)☐ (b)(7)(A)☐ (d)(5)☒ (b)(2)☐ (b)(7)(B)☐ (j)(2)☐ (b)(3)☐ (b)(7)(C)☐ (k)(1)☐ (b)(7)(D)☐ (k)(2)☒ (b)(7)(E)☐ (k)(3)☐ (b)(7)(F)☐ (k)(4)☐ (b)(4)☐ (b)(8)☐ (k)(5)☐ (b)(5)☐ (b)(9)☐ (k)(6)☐ (b)(6)☐ (k)(7)

- ☐ Information pertained only to a third party with no reference to the subject of your request or the subject of your request is listed in the title only.

- ☐ Documents originated with another Government agency(ies). These documents were referred to that agency(ies) for review and direct response to you.

Pages contain information furnished by another Government agency(ies). You will be advised by the FBI as to the releasability of this information following our consultation with the other agency(ies).

Page(s) withheld inasmuch as a final release determination has not been made. You will be advised as to the disposition at a later date.

Pages were not considered for release as they are duplicative of _____

Page(s) withheld for the following reason(s): _____

- ☒ The following number is to be used for reference regarding these pages:

MIDG PE II Sec 16 p 53

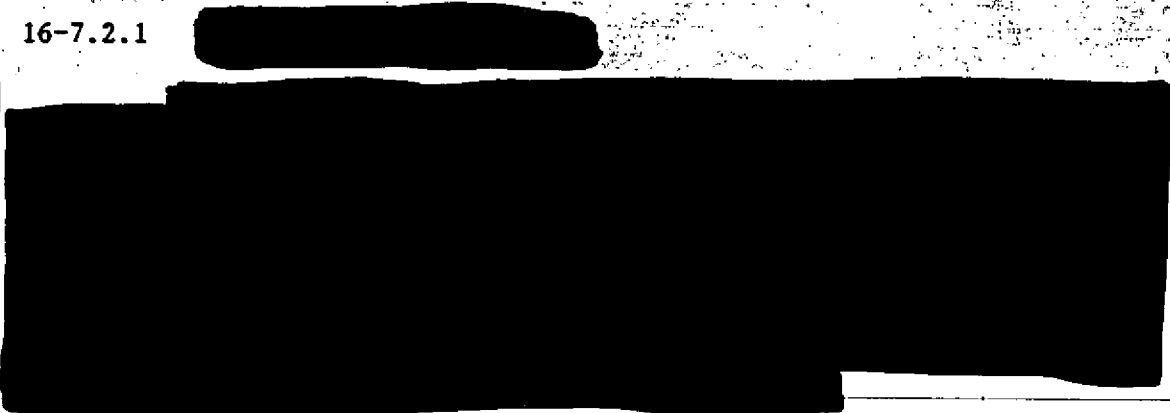
 XXXXXXXXXXXXXXXXXXXX
 X Deleted Page(s) X
 X No Duplication Fee X
 X for this page X
 XXXXXXXXXXXXXXXXXXXX
XXXXXX
XXXXXX
XXXXXX

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 16 - 54

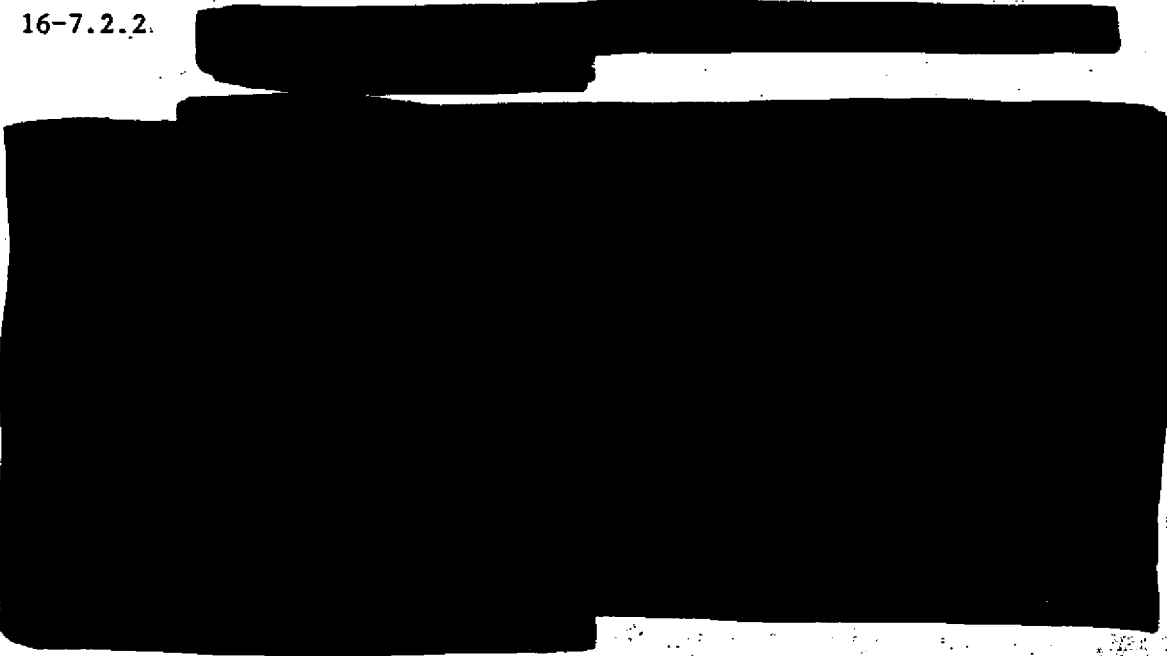
16-7.2.1



b2
b7E

EFFECTIVE: 02/10/97

16-7.2.2.



(2) The Technical Operations Section (TOS) strongly recommends that each field office establish a GS-14 Technical Supervisor (TS) position as part of its overall office management structure. This position should be filled by an experienced TTA, capable of overseeing all technical investigative activities within the field office. The field inspection process, on-site technical investigative program reviews, and management

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 16 - 55

feedback received from field offices with a TS already in place, clearly validate the organizational benefits derived through consolidating office technical investigative resources under one Supervisory Special Agent with a proven technical investigative background. As a minimum, the TOS recommends, in all but the largest field offices, that the TS be assigned management oversight for all TTA, ET, and CS personnel. The assignment to the TS of additional office technical support personnel may be warranted based upon the size of the field office.

EFFECTIVE: 12/06/96

16-7.2.3

[REDACTED]

b2
b7E [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Sensitive
PRINTED: 02/18/98

XXXXXX
XXXXXX
XXXXXXFEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET14

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 552Section 552a☒ (b)(1)☐ (b)(7)(A)☐ (d)(5)☒ (b)(2)☐ (b)(7)(B)☐ (j)(2)☐ (b)(3)☐ (b)(7)(C)☐ (k)(1)☐ (b)(7)(D)☐ (k)(2)☒ (b)(7)(E)☐ (k)(3)☐ (b)(7)(F)☐ (k)(4)☐ (b)(4)☐ (b)(8)☐ (k)(5)☐ (b)(5)☐ (b)(9)☐ (k)(6)☐ (b)(6)☐ (k)(7)

- ☐ Information pertained only to a third party with no reference to the subject of your request or the subject of your request is listed in the title only.

- ☐ Documents originated with another Government agency(ies). These documents were referred to that agency(ies) for review and direct response to you.

Pages contain information furnished by another Government agency(ies). You will be advised by the FBI as to the releasability of this information following our consultation with the other agency(ies).

Page(s) withheld inasmuch as a final release determination has not been made. You will be advised as to the disposition at a later date.

Pages were not considered for release as they are duplicative of _____

Page(s) withheld for the following reason(s): _____

- ☒ The following number is to be used for reference regarding these pages:

MIDG Pt II Sec 16 p.56-69

 XXXXXXXXXXXXXXXXXXXX
 X Deleted Page(s) X
 X No Duplication Fee X
 X for this page X
 XXXXXXXXXXXXXXXXXXXX
XXXXXX
XXXXXX
XXXXXX

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 16 - 70

16-7.3.3

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

EFFECTIVE: 02/10/97

16-7.3.4 Loan of Electronic Surveillance Equipment (See MIOG, Part II, 10-9.14 & 10-10.10.)

(1) Loan of Electronic Surveillance Equipment to State and Local Law Enforcement Agencies.

(a) By Department Order 890-80, dated 4/29/80, the Attorney General delegated to the Assistant Attorney General, Criminal Division, Department of Justice (DOJ), the authority to approve loans of electronic surveillance equipment to state and local law enforcement agencies for use in their investigations (i.e., not joint FBI investigations). Under this delegation, the loan of such equipment is to be made only in exceptional circumstances and to be consistent with federal and state laws, as well as with state and local law enforcement regulations.

(b) The Office of Enforcement Operations within the

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 16 - 71

Criminal Division of the DOJ has been assigned the responsibility of coordinating requests received for electronic surveillance equipment. That Office defines electronic surveillance equipment as any equipment which would be used in Title 18, USC, Section 2510, et seq. (Title III) - or consensual electronic coverages.

(c) The Departmental Order specifies that the loan of electronic surveillance equipment to state and local law enforcement agencies is to be discouraged and is to be permitted only:

1. in furtherance of the federal government's interests in the investigation and prosecution of violations of state criminal law that are of federal concern;
2. in compliance with all applicable provisions of federal, state and local law;
3. without interfering with state and local control of state and local law enforcement; and
4. without duplication of other federal programs of assistance to state and local law enforcement.

(d) Except in an emergency, requests for loan of electronic surveillance equipment will not be approved until the head of state or local law enforcement agency certifies in writing that the agency:

1. has authority under state and local law to borrow the equipment on the terms required by the Order;
2. has valid legal authority under state and local law to conduct the particular electronic surveillance for which the equipment is requested;
3. cannot obtain the requested equipment from other law enforcement agencies within the state; and
4. does not have available to it funds provided by the Law Enforcement Assistance Administration or its successor agency to obtain the requested equipment.

(e) Requests must contain a copy of a written opinion of the chief legal officer to the state or local government indicating compliance with conditions (d)1. and (d)2.

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 16 - 72

(f) The field office must advise FBIHQ when requesting approval to loan electronic equipment (be it either a routine or an emergency request) whether there is a current need for equipment within its division; whether, in the SAC's opinion, it is within the interest of the United States to loan the requested equipment in the specific criminal investigation; and whether the agency involved has previously violated the terms of any loan of electronic surveillance equipment by the FBI.

(g) The Deputy Director, FBI, will formally request the Assistant Attorney General, Criminal Division, DOJ, to permit the FBI to loan the equipment only after receipt of the state or local request with its attachments and the comments of the field office concerning that request.

(h) In an emergency, if the head of the state or local law enforcement agency involved represents that an emergency exists, that the need for electronic surveillance equipment exists, and that he/she is authorized under state law to conduct emergency electronic surveillance specifying the provision of state law upon which he/she is proceeding, the Deputy Director, FBIHQ, may grant the emergency request. The field office should expeditiously contact FBIHQ to explain why advance approval is not possible and secure the necessary approval, confirming both by teletype. The emergency loan, like the nonemergency loan, must be made pursuant to a written agreement. However, the Order provides that the written certifications required from the state or local agency may be provided following the actual loan, if submitted to the Assistant Attorney General, Criminal Division, DOJ, within FIVE (5) work days of the loan. Therefore, FBIHQ must receive the certifications in time to present them to the Assistant Attorney General, Criminal Division, DOJ, no later than the close of business on the fifth business day following the loan.

(i) The actual loan of the electronic surveillance equipment, in both routine and emergency circumstances, must be made pursuant to a written agreement between the FBI (SAC or designee) and the requesting state or local law enforcement agency. This agreement must identify the equipment to be loaned, describe the target of the surveillance, and detail the purpose (i.e., goal) of the surveillance to be conducted. It must also provide:

1. that the loan of the equipment is subject to the needs of the FBI and the equipment must be returned whenever requested;

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 16 - 73

2. that the loan of the equipment is limited to no longer than the duration of the authorized surveillance for which it is requested, or 90 days, whichever is less;

3. that the equipment may be used only for the validly authorized surveillance for which it was requested;

4. that the agency will not permit any other person or governmental entity to use the equipment;

5. that no FBI personnel may install the equipment and no FBI personnel may participate in the surveillance; and

6. that the agency will reimburse the United States for all loss or damage to the equipment. Any dispute over the amount of loss or damage will be resolved by the Assistant Attorney General, Criminal Division, DOJ, whose resolution will be final.

(j) Routine request should be by electronic communication (EC) to FBIHQ, Information Resources Division, Technical Operations Section, and should enclose both a written request from the head of the local or state law enforcement agency and the written opinion of the chief legal officer of the local or state government. Emergency requests should be by telephone, confirmed by EC, and followed by an EC, enclosing the necessary documents.

(2) Use of FBI technical equipment in Joint Cases where state and local law enforcement agencies obtained authority for its use (See MIOG, Part II, 10-10.3| (8).)|

(a) A Joint Case, for purposes of this section, is an investigation in which there exists significant FBI interest in the subject or subjects of local investigation and substantial FBI investigative resources have been utilized and/or will be utilized in the planned investigation with the local agency.

(b) FBIHQ authority must be obtained prior to any use of FBI electronic surveillance equipment or personnel in furtherance of any order or authority obtained by state or local law enforcement agencies. Should approval be granted for such use, the pertinent local or state order or authority must contain specific language authorizing FBI participation, whether the assistance is in installation, monitoring, or whatever is appropriate.

(c) In requesting FBIHQ authority, the field office

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 16 - 74

is to set forth the following information:

1. A synopsis of the investigation conducted to date by FBI and local agency involved, to include dates FBI case was opened, as well as when joint investigation was initiated.

2. Specific SAC comments as to the value of the assistance to the FBI investigation and extent of federal control over local electronic surveillance.

3. Exact nature of equipment to be utilized and technical assistance required, and whether equipment is on hand in the requesting division.

4. Specific comments of the Technical Advisor as to the ability of the local agency to properly utilize technical equipment requested.

5. That the local agency has valid legal authority under state or local law to conduct the electronic surveillance for which equipment will be utilized. Specific statute should be cited.

6. That the Chief Division Counsel or the Assistant United States Attorney has reviewed the affidavits and orders to be filed and concurs in their sufficiency.

7. That FBI policy in limiting disclosure as set forth in Part II, Sections 10-10.13 and 10-10.16, of this manual, will be honored in any subsequent local proceedings.

The above information is to be provided by appropriate communication to the attention of the Information Resources Division and to either the Criminal Investigative Division or the National Security Division.

(d) Any request for FBI assistance in execution of a locally obtained court order which requires physical entry (i.e., microphone installation) will be handled separately and will require significant justification. Emergency requests for such assistance are to be discouraged and likely will NOT be approved.

(3) Loan of Electronic Surveillance Equipment to Other Federal Agencies.

(a) The loan of FBI technical electronic surveillance equipment to other federal agencies is permissible on a

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 16 - 75

short-term basis. The loan of equipment must be subject to availability and must not negatively affect the technical investigative efforts of the FBI.

(b) For agencies of the Department of Justice (DOJ), specifically the Drug Enforcement Administration (DEA), material support and assistance, including the loan of technical equipment, should be handled on a local level, subject to the provisions stated above.

(c) For agencies other than DOJ, requests must be made on a Headquarters level, and the requesting agency must have electronic surveillance authority and capability.

(d) All technical equipment provided must be from existing field office stock.

EFFECTIVE: 02/28/97

16-7.3.5 Shipment of Technical Equipment and Parts Documentation

(1) Bureau Form FD-734 is designed to document shipments of technical equipment and parts between field divisions and the Information Resources Division for repairs, temporary assignments, and permanent transfer. This form consists of ten parts with carbon paper separating the parts and is stubbed at the top of the form. Designated routing and invoice numbers have been preprinted.

(a) From top to bottom pages are as follows:

Part One (Original) - white

Part Two (Program Manager) - blue - copy 1

Part Three (Supply Technician) - salmon - copy 2

Part Four (Property Accounting Systems Unit) -
pink - copy 3

Part Five (Bureau File Copy) - yellow - copy 4

Part Six (Duplicate Copy) - green - copy 5

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 16 - 76

Part Seven (Packing Slip) - goldenrod - copy 6

Part Eight (Return Receipt Copy) - white - copy

Part Nine (Duplicate Copy) - white - copy 8

Part Ten (Originator's File Copy) - white - copy

(b) Distribution of FD-734 form parts

Part	Designated Routing	Remarks
One	Original	Consignee (Administrative Officer)
Two	Program Manager	Consignee (Program Manager/Tech Coordinator)
Three	Supply Technician	Consignee (Property Custodian) Retention of this copy is required. For equipment received for permanent transfer, retain until equipment is reflected on the monthly inventory supplement. For equipment received for temporary assignment, retain copy until equipment returned.
Four	Property Accounting System	Send to FBIHQ. (Attach FD-514, data adjustment form, for permanent transfer of equipment.)
Five	Bureau File Copy	Send to FBIHQ. (Record on part five shipping data, such as

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 16 - 77

registered mail number,
name of airfreight
company, airbill
number, date, number of
cartons, weight, etc.)

Six Green Duplicate Copy Send to FBIHQ,
Attention of cognizant
section or unit. (For
information on the
movement of technical
equipment.)

Seven	Packing Slip	Enclose in box or carton. For multibox shipments a reproduction of the packing slip must be enclosed in each box indicating items of equipment contained therein.
-------	--------------	---

Eight	Return Receipt Copy	Enclose in box or carton, if multibox shipment box #1 is used. Initial and date to acknowledge receipt of shipment. Note any discrepancies. Return to sender.
-------	---------------------	--

Nine White Duplicate Copy Property Custodian of shipping division. Retention of this copy is required. For equipment shipped for permanent transfer, retain until transfer reflected on the monthly inventory supplement. For equipment shipped on temporary assignment basis, retain copy until equipment returned.

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 16 - 78

Ten	Originator's File Copy	Retained in files by employee authorizing shipment.
-----	---------------------------	---

(2) Bureau Form FD-750 is designed for documenting technical equipment shipments to various contractors for repair, modification, trade-in, or exchange in situations where field office has been given FBIHQ authority to transport technical equipment for aforementioned purposes. This form contains seven parts with carbon paper separating parts, and is stubbed at the form top. Each part is designated with bold printing, for easy distribution, and is numbered for reference.

(a) From top to bottom parts are as follows:

Part One (Original) - White
Part Two (Bureau File Copy) - Yellow
Part Three (Originator Acknowledgement Return Receipt
Copy) - Blue
Part Four (Vendor Acknowledgement Return Receipt
Copy) - Pink
Part Five (Freight Desk) - Salmon
Part Six (Packing Slip) - Goldenrod
Part Seven (Originator File Copy) - Green

(b) Distribution of form parts:

1. Original Copy: Route to field division
supply technician.

2. Bureau File Copy: Route to field division
[Administrative Officer.] Indicate pertinent shipping data.

3. Originator Acknowledgement Return Receipt
Copy: Upon return of the technical equipment at the field division,
record date of receipt, initials, and route copy to the supply
technician.

4. Vendor Acknowledgement Return Receipt:
Enclose this copy in package with technical equipment, attach a self-
addressed envelope for the contractor to return the receipt to the
field division.

5. Freight Desk: Retained by support personnel
tasked with the processing of surface freight, air freight, and

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 16 - 79

registered mail.

6. Packing Slip Copy: Enclose this copy in package with technical equipment for retention by the contractor.

7. Originator File Copy: Retain in files by employee authorizing the shipment.

EFFECTIVE: 12/14/93

16-7.4

b7E
b2
b1

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

XXXXXX
XXXXXX
XXXXXXFEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET4

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 552Section 552a☐ (b)(1)☐ (b)(7)(A)☐ (d)(5)☒ (b)(2)☐ (b)(7)(B)☐ (j)(2)☐ (b)(3)☐ (b)(7)(C)☐ (k)(1)☐ (b)(7)(D)☐ (k)(2)☒ (b)(7)(E)☐ (k)(3)☐ (b)(7)(F)☐ (k)(4)☐ (b)(4)☐ (b)(8)☐ (k)(5)☐ (b)(5)☐ (b)(9)☐ (k)(6)☐ (b)(6)☐ (k)(7)

- ☐ Information pertained only to a third party with no reference to the subject of your request or the subject of your request is listed in the title only.

- ☐ Documents originated with another Government agency(ies). These documents were referred to that agency(ies) for review and direct response to you.

Pages contain information furnished by another Government agency(ies). You will be advised by the FBI as to the releasability of this information following our consultation with the other agency(ies).

Page(s) withheld inasmuch as a final release determination has not been made. You will be advised as to the disposition at a later date.

Pages were not considered for release as they are duplicative of _____

Page(s) withheld for the following reason(s): _____

- ☒ The following number is to be used for reference regarding these pages:

MIDG Pt II Sec 16 p80-83

XXXXXXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X for this page X
XXXXXXXXXXXXXXXXXXXX

XXXXXX
XXXXXX
XXXXXX

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 16 - 84

[illegible]

EFFECTIVE: 07/28/97

16-7.5.3 Technical Update | Newsletter |

The Technical Operations Section will periodically publish a Technical Update Newsletter. The newsletter will provide operational information of interest to the TTAs, Electronics Technicians (ETs), and Computer Specialists (CSs). Information for the newsletter is solicited from Engineering Research Facility Program Managers and from field technical personnel.

EFFECTIVE: 02/10/97

16-7.6 [REDACTED]

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 16 - 85

EFFECTIVE: 02/10/97

| 16-7.6.1 | Deleted |

EFFECTIVE: 02/10/97

| 16-7.6.2 | Deleted |

EFFECTIVE: 04/05/94

16-7.6.3 New Agent Training

The ES will provide appropriate and current electronic surveillance training to new Agents. This training will be conducted within the structured New Agent Training curriculum.

EFFECTIVE: 09/25/91

| 16-7.7 |

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

XXXXXX
XXXXXX
XXXXXXFEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET3

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 552Section 552a☒ (b)(1)☐ (b)(7)(A)☐ (d)(5)☒ (b)(2)☐ (b)(7)(B)☐ (j)(2)☐ (b)(3)☐ (b)(7)(C)☐ (k)(1)☐ (b)(7)(D)☐ (k)(2)☒ (b)(7)(E)☐ (k)(3)☐ (b)(7)(F)☐ (k)(4)☐ (b)(4)☐ (b)(8)☐ (k)(5)☐ (b)(5)☐ (b)(9)☐ (k)(6)☐ (b)(6)☐ (k)(7)

- ☐ Information pertained only to a third party with no reference to the subject of your request or the subject of your request is listed in the title only.
- ☐ Documents originated with another Government agency(ies). These documents were referred to that agency(ies) for review and direct response to you.

Pages contain information furnished by another Government agency(ies). You will be advised by the FBI as to the releasability of this information following our consultation with the other agency(ies).

Page(s) withheld inasmuch as a final release determination has not been made. You will be advised as to the disposition at a later date.

Pages were not considered for release as they are duplicative of _____

Page(s) withheld for the following reason(s): _____

- ☒ The following number is to be used for reference regarding these pages:

MIOG Pt II Sec. 16 p86-88

XXXXXXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X for this page X
XXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXX
XXXXXX

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 16 - 89

b2
b7E
[REDACTED]
(10) Deleted

EFFECTIVE: 09/25/91

16-8.2.2 Requests for Examination of Evidence

All requests should be made after coordination with the TA in a written communication addressed to the Director, Federal Bureau of Investigation, "Attention: Technical Services Division, Engineering Section" under the case caption and should contain the following information:

(1) Reference to any previous correspondence submitted to the Technical Services Division.

(2) A list of evidence being submitted and if the evidence is enclosed or being sent under separate cover. (Note: Due to chain of custody requirements, evidence sent through the U.S. Postal Service (USPS) should be sent registered mail. If the submission must be sent on an expedite basis, a service which provides a protective or security signature service similar to USPS registered mail should be used.)

(3) Briefly describe the manner in which the recording was made; i.e., type of recorder or transmitter, if known, and perceived problem with the recording if enhancement is requested.

(4) The location and content of the pertinent conversation(s) on the tape and their approximate duration.

(5) A request stating the type of examination required including, if applicable, the number of copies needed and format (open reel or cassette).

(6) Any time limitation requiring expedite handling should be explained, such as a fixed trial date or life-threatening situations.

(7) The name and telephone number of the person to be contacted should any questions arise regarding the examination of evidence.

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 16 - 90

EFFECTIVE: 09/25/91

16-8.2.3 Marking of Recordings for Identification

- (1) Marking should be done with black indelible pen.
- (2) Marking should be done on the tape itself on the nonrecorded side. The tape is the evidence, not the reel, box or other container.

Cassette tapes should also be marked on the tape. This may be accomplished by carefully pulling out a loop of tape and placing identifying information on the back side of the tape at the beginning. The tape may be wound by hand back into the cassette case.

- (3) Identifying information should include unique identifiers and the date the recording was made.

- (4) Suitable identifying information should also be placed on the tape box, case, cassette label or container used to house the tape.

EFFECTIVE: 09/25/91

16-8.2.4 Submission of Recordings

Only the original recordings should be submitted for examination. One or more copies should be made for retention by the field office prior to submission of the original recordings.

- (1) Recordings should be packed in a sturdy cardboard box with no less than three inches of packing material on all sides. This will prevent accidental erasure in the remote event that the recording is exposed to a strong magnetic field while in transit.

- (2) If a recorder or other items are also submitted, they should be packed securely within the box to avoid damage in transit.

- (3) Seal the box with gummed tape and clearly mark the outside of the box with the word "EVIDENCE." (If any of the evidence in the box is to be subjected to a latent fingerprint examination, the evidence as well as the outside of the box should be clearly marked

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 16 - 91

with the word "LATENT.")

(4) Place a copy of the original written request for the examination in an envelope marked "INVOICE" and securely affix this envelope to the outside of the sealed box.

(5) Enclose the sealed box in wrapping paper and seal the wrapping paper with gummed tape. Prepare the address label, addressing the package to: FBI Engineering Research Facility, Audio/Video Processing Program, Building 27958A, Quantico, Virginia 22135. Cover the label with yellow transparent tape to identify the shipment as evidence.

(6) Ship the package by U.S. Postal Service (USPS) registered mail. If the shipment is sent by another carrier, ensure that a protective or security signature-type service is available and utilized similarly to USPS registered mail.

EFFECTIVE: 09/25/91

16-8.2.5 Tape Enhancement

Tape enhancement is the selective reduction of interfering noise on audio recordings to improve the intelligibility or ease of understanding the desired audio information.

(1) Best enhancement is obtained by processing the original recordings; therefore, if available, only the original recording should be submitted in accordance with instructions in 16-8.2.2 and 16-8.2.4.

(2) No alteration of the original recording occurs during the enhancement process. An enhanced copy of the information recorded on the original is produced.

(3) Enhanced recordings may be used for courtroom presentation in conjunction with the original tapes, and/or for intelligence or lead purposes.

(4) Deleted

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 16 - 92

EFFECTIVE: 09/25/91

16-8.2.6 Review and Presentation of Enhanced Recordings

(1) Review of all marginally intelligible recordings, including both original and enhanced versions, should be accomplished by using high quality recorders and earphones.

(2) Courtroom presentation of marginally intelligible recordings should be accomplished by means of a courtroom presentation system consisting of a quality tape recorder, amplifier and an earphone network which provides individual earphones to each of the jury members, the judge, witness box, defense, and prosecution. Loudspeakers should be provided for the spectator area but played at a level where they cannot be heard by a juror wearing earphones.

(3) The use of a courtroom presentation system will improve the ability of the jury to understand most recordings and should be considered whenever audio information is played in court.

EFFECTIVE: 05/26/89

16-8.2.7 Magnetic Tape Authenticity Examination

Magnetic tape authenticity examinations are conducted to establish that the recording was made as claimed or that no editing, stopping, erasing or other tampering of the tape occurred.

(1) Typically, magnetic tape authenticity examinations are conducted in response to allegations of tape tampering by the defense.

(2) Magnetic tape authenticity examinations may also be conducted to determine legitimacy of suspicious recordings offered by the defense.

Should the defense contend tampering has occurred on an evidence tape recording, every effort should be made to force the defense to precisely specify the areas in contention. This will significantly reduce the amount of time necessary to conduct examinations of the recording.

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 16 - 93

(3) Questions regarding tape authenticity should be directed to the Engineering Section of the Technical Services Division.

(4) Requests for tape authenticity examinations should be made only in the event that legitimacy of the tape cannot be established through chain of custody and appropriate testimony as to integrity of the recording by parties involved in production, copying, storage, transcription, etc.

EFFECTIVE: 05/26/89

16-8.2.8 Submission of Evidence

Submit in accordance with 16-8.2.2 and 16-8.2.4 above, and whenever possible, attempt to identify and locate the recorder used to produce the recording in question and ascertain whether any servicing, realignment or cleaning of the recorder has occurred since the recording was made. Maintain the recorder in its original condition for possible submission for examination or until the situation has been resolved.

EFFECTIVE: 05/26/89

16-8.2.9 Speaker Identification (Voiceprint) Examinations

Speaker identification examinations, using the spectrographic (voiceprint) method, are conducted to compare the recorded voice of an unknown individual to known recorded voice samples of suspects or to other unknown recorded voices. The examination is conducted by using both graphic (spectral) and aural (listening) analyses.

EFFECTIVE: 05/26/89

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 16 - 94

16-8.2.10 Speaker Identification Policy

(1) Decisions regarding speaker identification by the spectrographic method are not considered conclusive, since there is limited scientific research regarding the reliability of the examination under the varying conditions of recording fidelity, interfering background sounds, sample size, voice disguise, restrictive frequency range, and other factors commonly encountered in investigative matters.

(2) Speaker identification examinations are conducted solely for investigative guidance. No court testimony is provided.

(3) Speaker identification examinations are normally conducted by comparing an unknown recorded voice sample to a known recorded verbatim exemplar, where the suspect repeats exactly the same wording the unknown speaker used. Nonverbatim comparisons can be conducted in high priority cases with the explicit written approval of the SAC or appropriate Assistant Director; however, a definitive identification can normally only be reached in a small percentage of nonverbatim examinations. When nonverbatim examinations are requested, typed transcriptions of all voice samples must be provided.

(4) Speaker identification examinations are conducted for local law enforcement agencies provided they agree in writing to use the results solely for investigative guidance and will not request court testimony.

(5) Only original tape recordings should be submitted for examination.

EFFECTIVE: 05/26/89

16-8.2.11 Obtaining and Submitting Known Voice Exemplars

(1) Normally known voice exemplars will be verbatim, where the suspect repeats exactly the same wording the unknown speaker used. When verbatim samples cannot be obtained, attempts should be made to elicit as many of the same words and phrases, as possible, that were used by the unknown speaker.

(2) When recording the known voice sample, duplicate as closely as possible the recording conditions and equipment used to record the unknown voice sample, including the use of the same

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 16 - 95

telephones, if applicable.

(3) Recordings should be of high technical quality. Use standard recording tape; do not use extended play reel tapes with a thickness of less than 1.0 mil or cassettes of longer duration than 90 minutes (45 minutes per side). Tape recorder speed should be at least 1 7/8 inches per second.

(4) Verbatim typed transcriptions must accompany each recording.

EFFECTIVE: 05/26/89

16-8.2.12 Aural Comparisons

This type examination of a sound recording is made to determine if two different recordings had the same original.

EFFECTIVE: 05/26/89

16-8.2.13 Submitting Tapes for Aural Comparison

(1) The cover communication should describe the submitted tapes.

(2) The number of tapes submitted should be kept to a minimum.

(a) If possible, top hits and well-known artists should be submitted.

(b) If more than 10 tapes are submitted, ensure that the AUSA wants more than 10 counts.

(c) One copy of each tape is sufficient.

(3) Specify songs to be compared in the cover communication.

(a) This will ensure the proper "N" form is obtained.

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 16 - 96

(b) When a song is not requested, the song compared is picked at random.

EFFECTIVE: 05/26/89

16-8.2.14 Obtaining Known Copyrighted Sound Recordings

(1) The Technical Services Division, Engineering Section, does not maintain a reference file of copyrighted sound recordings.

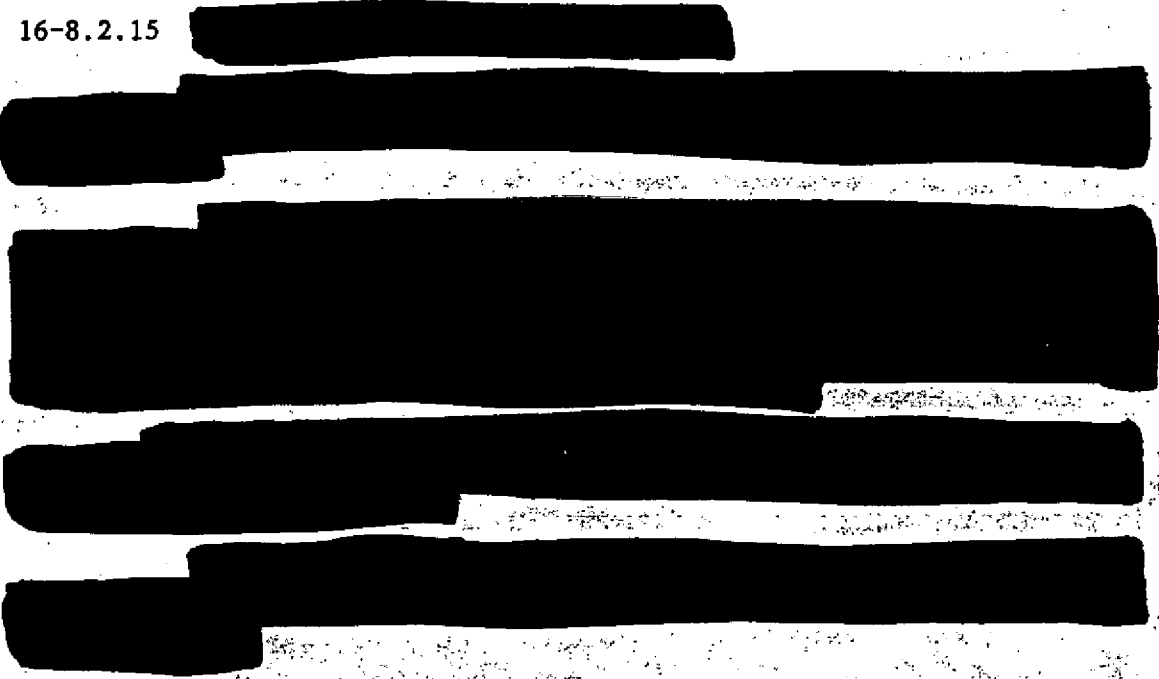
(2) An authorized copy of the copyrighted sound recording should be obtained from the manufacturer and submitted at the same time the questioned sound recording is submitted to Technical Services Division for examination.

(3) The authorized copy must be dated and initialed by the manufacturer's representative who will be available to testify as to the ownership of the copyright and the existence of any licensing agreements.

EFFECTIVE: 05/26/89

16-8.2.15

b2
b7E



Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 16 - 97

b2
b7E
[REDACTED]

EFFECTIVE: 09/25/91

| 16-8.2.16 Video Tape Examinations | (See 16-8.2(6).) |

The following types of video tape examinations are conducted by the Operational Support Unit (OSU), Engineering Section (ES), Technical Services Division (TSD): (If there is a question regarding the type of examination to be conducted or handling of video recordings, telephonically contact the OSU prior to submission of evidence.)

(1) Copyright - a determination is made as to whether a video recording is an original or a copy. Suspect recordings should be screened before submission to reduce the number of original recordings received. This can be by physical appearance, poor video quality, or informant information. Not more than five recordings should be submitted at one time.

(2) Duplication

(3) Enhancement

(4) Photographs of video images - (The specific location of the image on the recordings should be identified and the image described as completely as possible.)

(5) Standards conversion

EFFECTIVE: 05/13/93

~~SECRET~~

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 16 - 98

16-8.3

b2
b7E

[REDACTED]

[REDACTED]

b1

[REDACTED] (S)

EFFECTIVE: 09/25/91

16-8.4 Deleted

EFFECTIVE: 09/25/91

16-9 VOICE COMMUNICATIONS

Voice communications encompass the procurement and management of the Federal Telecommunications System (FTS), Wide Area Telecommunications Service (WATS), and local telephone systems and facilities.

EFFECTIVE: 07/23/90

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
EXCEPT WHERE SHOWN
OTHERWISE

CLASSIFIED BY: SP5 r/lus
REASON: 1.5 (C)
DECLASSIFY ON: X 1

7/9/98

~~SECRET~~

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 16 - 99

16-9.1 General Telephone Policy (See MIOG, Part II, 16-9.4.1 & 16-9.9.1.)

Whenever a telephone is utilized, the following should be kept in mind:

(1) All telephone calls made on standard telephones are subject to interception by foreign intelligence services. Consequently, no national security information should be discussed on these telephones.

(2) The use of the telephone services, equipment, or facilities (including calls over commercial systems which will be paid for by the FBI) shall be limited to the conduct of official business. Such official business calls may include emergency personal calls and calls which are determined to be in the interest of the Bureau. No other personal calls may be placed (except in circumstances identified in paragraphs (3) and (4) below) even if the employee's intention is to reimburse the FBI for the cost of the call.

(3) Use of the telephone systems for emergency personal calls may properly be authorized as being necessary in the interest of the Bureau if such use satisfies the following criteria. If possible, such calls should be made during lunch breaks, or other off-duty periods and:

(a) It does not adversely affect the performance of official duties by the employee,

(b) It is of reasonable duration and frequency, and

(c) It reasonably could not have been made at another time.

(4) Personal calls that must be made during working hours may be made over the commercial long distance network if the call is consistent with criteria in paragraph (3) and is:

(a) Charged to the employee's home telephone number or other non-Government number (third number call),

(b) Made to an 800 toll-free number,

(c) Charged to the called party if a non-Government number (collect call) or,

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines

Part II

PAGE 16 - 100

- (5) Abuse of the telephone privileges set forth above may result in disciplinary action that may include, but not be limited to, the reimbursement for the unauthorized calls.

Collection for unauthorized telephone calls shall be composed of two parts:

- (a) The value of the call based on commercial long distance rates rounded to the nearest dollar and,
-
- (b) A service (handling) charge of \$10.00 on each call to cover administrative costs, for example, to determine that the call was unauthorized and to process the collection.

- (6) It is essential that maximum economy be exercised but FBIHQ and field offices must be kept advised of those matters of importance. Therefore, good judgment must prevail.

- (7) Calls from within one field office territory to another or to FBIHQ should only be made with the approval of a field supervisor or above. However, approval is not needed where an agreement between adjoining offices has been previously reached.

- (8)

- (9) Changes in addresses and/or telephone numbers of the following must be reported immediately to FBIHQ: (See MAOP, Part I, 20-2.1.)

- (a) Field offices

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 16 - 101

(b) Resident agencies

(c) ASACs and higher

(10) Oversight of the telephone calling card program will rest with Property Procurement and Management Section (PPMS), Finance Division. The SAC or Assistant Director should submit a written request to FBIHQ, PPMS for the issuance of telephone calling cards. These requests should contain the names of the individuals to whom the cards are to be issued. PPMS will forward the telephone calling cards with Form FD-281. The PPMS will maintain the inventory records for the calling cards as issued personal property. Each calling card will have a unique number to enable identification of toll charges made by each individual. Each calling card is to be issued to an individual and the number shall not be given to other individuals for their use. A calling card may be retained by an individual upon transfer to another field office or headquarters if it can be determined that the card will be required in the new office. Once a calling card has been issued to an individual and it is no longer needed, the card should immediately be returned to FBIHQ for cancellation. A calling card may not be transferred to another individual.

(11) The monthly computer-generated bills for calling cards are received by FBIHQ and are paid quarterly with the FTS billing.

(12) Deleted

(13) Employees issued telephone calling cards through FBIHQ should not use personal telephone calling cards. Employees in field offices and divisions which do not have telephone calling cards issued through FBIHQ may use personal telephone calling cards and claim reimbursement through expense vouchers supported by proper receipts.

(14) Lost or stolen calling cards should be immediately reported to FBIHQ, Operations Management Section for cancellation and Property Procurement and Management Section for inventory control and issuance of another calling card.

EFFECTIVE: 03/07/94

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 16 - 102

16-9.2 Requests for Additional Telephone Facilities and/or Equipment

(1) Any facility or equipment involving substantial installation of \$100 or more, or monthly recurring charges of \$50 or more, or use of any equipment or facility involving change in Bureau policy, must be approved by FBIHQ before its installation or use may be arranged or scheduled by a field office. In an emergency situation in which time is of the essence, permission to install equipment or use a facility involving substantial costs or change in Bureau policy may be requested by contacting the Information Resources Division by telephone or other expedite means as warranted.

(2) Submit to FBIHQ on UACB basis request for minor additional communications facilities, such as a telephone instrument using an extension from your switchboard, or an additional telephone instrument in a resident agency when installation of additional telephone trunks or lines is not involved, furnishing justification and monthly costs, with installation not to be scheduled before requests can be received at FBIHQ and denial received if not approved.

(3) Speakerphones may be authorized, when individually justified, for use by SACs and ASACs. Additionally, one speakerphone may be authorized for use in a conference room or command post. The Bureau is governed by GSA regulations regarding the acquisition of speakerphones.

EFFECTIVE: 05/24/94

16-9.3 Procuring New Telephone Systems

Federal Property Management Regulations (FPMR) now require that all major changes to telecommunications facilities be procured competitively. This requires the advertising and distribution of system requirements and specifications, evaluation of responses, and submission of recommendations to GSA for approval. These procedures will require approximately 12 months for completion and must be negotiated by FBIHQ.

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 16 - 103

EFFECTIVE: 05/24/94

16-9.4 Federal Telecommunication System (FTS)

EFFECTIVE: 07/23/90

16-9.4.1 General FTS Policy

In addition to the general telephone policy mentioned in
| MIOG, Part II, | 16-9.1 above, the following pertains to FTS:

(1) In field offices equipped with Station Message Detail Recording (SMDR), direct FTS station access can be approved by the Special Agent in Charge. In field offices not equipped with SMDR, FTS calls are to be made through the office switchboard for the purpose of maintaining records of all outgoing FTS calls. Direct station access can be approved by the Special Agent in Charge provided that a record is made of all the outgoing FTS calls.

| (2) | Deleted |

(3) The FTS intercity network and other Government provided long distance telephone services are to be used only to conduct official business; i.e., if the call is necessary in the interest of the Government. These networks are to be used for placement of calls instead of the commercial toll network to the maximum extent practicable.

(4) FBI FTS telephone numbers are not to be published in FTS telephone directories, but may be furnished to other agencies.

(5) FBI FTS lines must not appear on GSA switchboards, or be available to GSA telephone operators except on "call sampling" or if dialed by GSA operator. Furnish FBI FTS account number [redacted] and telephone number of instrument you are using to GSA operator when call is sampled. Use no other number or variation of it. b2

(6) No FBI telephone calls are to be placed through GSA telephone operators except those switchboards where GSA operators cannot access or monitor the call after it is placed.

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 16 - 104

EFFECTIVE: 09/21/93

| 16-9.4.2 | Deleted |

EFFECTIVE: 09/21/93

16-9.4.3 FTS Billing

(1) Each FTS call made from a field headquarters and from each resident agency 24 hours a day, seven days a week will be billed on a time- and distance-sensitive, per-minute basis.

(2) All field office and resident agency FTS service and GSA-provided local service are billed directly to FBIHQ by GSA.

EFFECTIVE: 09/21/93

16-9.4.4 Requests for FTS Lines

(1) In field offices:

(a) All field offices are equipped with FTS service. If there are indications that additional FTS lines are required, call FBIHQ, Operations Management Section, and a traffic study will be implemented to determine the appropriate number of FTS lines to be installed.

(2) In resident agency:

(a) FTS service may be installed in all resident agencies. If there are indications that additional FTS lines are required, call FBIHQ, Operations Management Section, and a traffic study will be implemented to determine the appropriate number of FTS lines to be installed.

(b) If the resident agency does not have FTS

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 16 - 105

service, a request should be submitted to FBIHQ, Operations Management Section, showing the number of personnel assigned to the resident agency along with all commercial telephone numbers in the office and the purpose of each line.

(c) Deleted

EFFECTIVE: 09/21/93

16-9.4.5 FTS Calls to FBIHQ

Each field office using the FTS lines on its switchboard can direct dial any telephone station at FBIHQ without going through the FBIHQ switchboard operator. This is accomplished by dialing [REDACTED] plus the desired four-digit extension number. The FBIHQ supervisor receiving the FTS call has the capability of transferring all incoming calls to other extensions. ba

EFFECTIVE: 09/21/93

16-9.5 Wide Area Telecommunications Service (WATS)

WATS may be used only for calls of an official nature and authority required for its use is the same as that required for making long-distance telephone calls via toll facilities.

EFFECTIVE: 10/27/81

16-9.6 Foreign Exchange (FX) Trunk

FX service is a trunk facility between a PBX or Centrex system and a central office which is outside the local service area of the PBX or Centrex system. Such facilities provide the equivalent of local service to and/or from the distant exchange. FX lines must be authorized by FBIHQ.

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 16 - 106

EFFECTIVE: 01/31/78

16-9.7 Off-Premise Extension (OPX)

An extension off the switchboard to a remote off-premise location. OPX must be authorized by FBIHQ.

EFFECTIVE: 01/31/78

16-9.8 Tie Lines

Tie line is a private line communication channel of the type provided by communications common carriers for linking two or more switching points together. Tie lines must be authorized by FBIHQ.

EFFECTIVE: 01/31/78

16-9.9 Local Telephone Systems

EFFECTIVE: 01/31/78

16-9.9.1 Policy

In addition to the general telephone policy outlined in MIOG, Part II, 16-9.1 above, the following pertain to local telephone systems:

(1) Deleted

(2) When commercial long-distance (toll) facilities must be used, calls should normally be made station to station, directly dialed.

(3) Telephones in resident agencies are for the exclusive use of Resident Agents and should be private lines not connected with other offices or building switchboards. Tie lines with switchboards may be maintained in addition to private lines if approved by FBIHQ.

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 16 - 107

EFFECTIVE: 09/21/93

16-9.9.2 Listing of Telephone Numbers in Directories

(1) Field headquarters listings are to be "Federal Bureau of Investigation." (For city, business, building directories, and inscriptions on doors, the listing should be "Federal Bureau of Investigation, United States Department of Justice.") Listing should appear alphabetically under the Fs in the U.S. Government section of the telephone directory.

(2) Resident agencies listings should be included in the U.S. Government section, if available, and in those cases where there is no U.S. Government section, the listings should be included in alphabetical order in the white pages. (See MAOP, Part II, 1-3.9.)

(a) All resident agency locations should be equipped with a telephone answering recorder or voice mail system. This equipment can then be activated to advise the caller to call the field office number in an emergency situation when the resident agency is unmanned.

(b) In no instances shall the residence telephone number or address of an Agent be listed as an alternate or emergency number for the resident agency.

(3) For locations where there is no field office or resident agency, no telephone directory listing is required.

There is no objection to listing the field office telephone number in the alphabetical section of the directories, provided there is no charge for the listing.

(4) It is not required that SACs have their home telephone numbers listed in the telephone directory.

EFFECTIVE: 09/21/93

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 16 - 108

16-9.9.3 Annual Telecommunications Equipment Reports (FD-344)

Each April compile Annual Telecommunications Equipment and Cost Report, using Forms FD-344 and 344a. Mail report, in duplicate, to reach FBIHQ no later than middle of May. If major changes are made in telephone system between regular annual submissions of this report, FBIHQ records should be brought up to date with submission of pertinent changes to last report submitted.

EFFECTIVE: 01/31/78

16-9.9.4 Billing

Field headquarters' bills should be checked against the Station Message Detail Recording (SMDR), if available, before they are approved for payment. Likewise, toll calls for a resident agency should be certified as to correctness by the Senior Resident Agent before the bills are processed for payment.

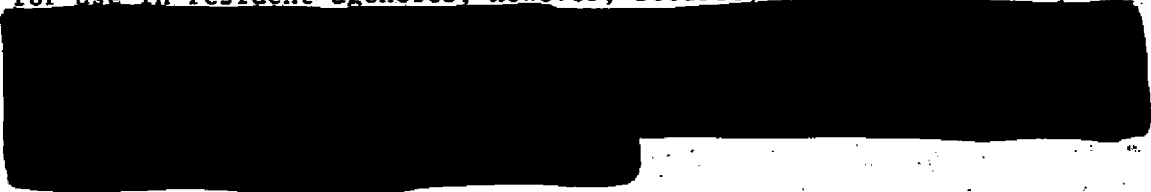
EFFECTIVE: 09/21/93

16-9.10 Telephone Answering Devices (See MIOG, Part II, 16-9.9.2; MAOP, Part II, 1-3.9 (3).)

Telephone answering devices provide the caller with a prerecorded announcement identifying the called party and inviting the caller to leave a message. The message(s) can be extracted upon return to the office or accessed remotely from any other telephone by use of a uniquely coded remote access keyer.

(1) Telephone answering devices will be most applicable for use in resident agencies; however, security considerations require

b2



(2) Requests for telephone answering devices should be

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 16 - 109

submitted to FBIHQ with detailed justification.

EFFECTIVE: 09/21/93

16-9.11 Use of FBIHQ Telephones

EFFECTIVE: 07/23/90

16-9.11.1 Computer Record of Calls Made

Each user should be aware that all calls placed from FBIHQ, Washington, D.C. and some field offices on either the commercial or FTS networks are automatically billed to the user's station. This billing information, which is computer controlled, prints out identifying data similar to that which appears on each individual's home telephone toll bill. In addition, the printout will show the time the call was placed and the length of the call. At FBIHQ, the resulting billing information will be furnished to each division for verification and control. Each field office with SMDR should furnish the resulting billing information to each squad supervisor for verification and control. All FTS and FTS/WATS calls are charged to the Bureau on a per-minute, time- and distance-sensitive rate, 24 hours a day, seven days a week.

EFFECTIVE: 09/21/93

16-9.11.2 Local Calls

Local calls may be placed after dialing "9" to access an outside line.

EFFECTIVE: 07/23/90

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 16 - 110

16-9.11.3 FTS Calls

Individuals who have unrestricted telephones are able to direct dial field offices and other Government telephones on the FTS network. This is accomplished by dialing the FTS access number, usually "8" followed by the FTS ten-digit telephone number. The FTS telephone number for each field office is included on the Field Office Mailing List.

EFFECTIVE: 09/21/93

16-9.11.4 WATS Calls

All long-distance commercial and residential telephone numbers within continental United States may be direct dialed through the FTS network (FTS-WATS) by dialing the FTS access code, usually "8", followed by the ten-digit commercial telephone number. These calls are charged as FTS rather than as commercial toll calls.

EFFECTIVE: 09/21/93

16-9.11.5 Deleted

EFFECTIVE: 05/24/94

16-9.11.6 FBIHQ Office Reorganization/Expansion

(1) When an office is to be reorganized, expanded or moved, a written request must be furnished to the Information Resources Division. The request must be received at least ten working days prior to actual date service is required to allow ample time for surveys, order preparation, and scheduling of telephone company technicians.

(2) If the telephone work requires the movement or

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 16 - 111

installation of telephone outlets in the floors or ductwork, then prior separate arrangements must be made with the Facilities Management Unit, Personnel Division, to ensure that the outlets are installed prior to the requested telephone service date.

(3) If the telephone work involves the installation of new furniture, then the written request should be received at least 20 working days in advance of the installation date. Floor plans should accompany the memorandum to assist telephone company personnel in moving telephone cables.

(4) Moves to off-site locations require at least 30 working days' advance notice due to the additional requirements to purchase equipment and engineer circuits.

EFFECTIVE: 04/21/94

16-9.11.7 Quarterly Telephone Reports

Offices equipped with SMDR must submit a quarterly printout of ALL outgoing calls made from the field headquarters for the periods January-March, April-June, July-September, and October-December. The printouts are to reach FBIHQ, Attention: Operations Management Section, by April 10, July 10, October 10, and January 10, respectively, for the appropriate quarter.

EFFECTIVE: 09/21/93

16-10 COMPUTER ASSISTANCE TO THE FIELD (See MIOG, Part II, 10-4.)

In any investigation within FBI jurisdiction, experienced Automated Data Processing (ADP) personnel assigned to the Investigative Automation Support Section, Information Resources Division, are available, where warranted to:

(1) Provide on-site assistance in the examination of records maintained on data processing equipment, including but not

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 16 - 112

limited to, execution of search warrants.

(2) Supervise on-site preparation of listings or reports from automated records, including but not limited to, execution of search warrants.

(3) Arrange for the processing of automated (machine readable) files and large quantities (in excess of 1,000) of nonautomated records. Examples of nonautomated records are checks, deposit slips, bank statements, payroll records, other financial documents, telephone toll records and bills.

(a) Types of work previously requested have been sequencing, selecting, comparing, preparing accounting schedules, and/or mathematical computations.

(b) Some examples of schemes where processing of records have been beneficial are floats, kiting, lapping, skimming, padding of payrolls, double billing, land fraud and welfare fraud.

(4) Implement the Investigative Support Information System (ISIS) to support major FBI investigations. There are two versions of ISIS: 1. Online - where computer terminals are installed at the field office for instantaneous data loading and retrieval, and 2. Offline - where data encoded at the field office is sent to FBIHQ for processing and a hardcopy listing returned to the field. The version of ISIS used to support an investigation is dependent upon the requirements of the case and the availability of ISIS resources. ISIS provides the ability to control, access and correlate all information that is generated by major investigations. ISIS has proven beneficial for file review prior to interviews, determining pending leads, writing reports and preparing for trial proceedings, in addition to investigative purposes.

(5) Implement ISIS reactive capability for immediate support of a major case(s). ISIS has the ability to be operational online at the site of the major case within forty-eight hours of the decision to support the case. The ISIS reactive capability is utilized at the request of the Director and/or Deputy Director and the Assistant Director - Criminal Investigative Division.

EFFECTIVE: 06/01/94

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 16 - 113

16-10.1 Requests for Computer Assistance

All requests for computer assistance should be in a written communication addressed to the Director, FBI, Attention: Investigative Automation Support|Section and should:

(1) Include in the title of the case: the field office and Bureau file numbers, if known, as well as the phrase "Request for Computer Assistance."

(2) Furnish any pertinent background data.

(3) Set forth the specific type of computer assistance being requested, along with an estimate of the volume of source material. A rough sketch of the desired output (computer printouts) should be enclosed showing what data fields are required and in what order or sequence they are needed. Totals required should be identified to include when needed (end of month, end of year, etc.) and where they should be printed.

(4) Set forth the approximate cost to accomplish the task manually. This should include the number of personnel required and the amount of time to complete the task.

(5) List any deadline data and the reason(s) for the deadline.

(6) Enclose typical samples (originals or legible copies) of the source material. (Note: Do not send all the source material until requested to do so by the|Investigative Automation Support|Section.)

(7) Indicate whether the source material will be used as evidence in court and whether any markings can be made on the material. It is often desirable to write on or stamp a number on the material to facilitate data entry processing.

(8) Advise how the material was obtained (Grand Jury subpoena, search warrant, etc.) and if there are any objections by the United States Attorney's office to the subcontracting of data entry aspect of this request.

(9) Indicate if it is anticipated that the requested computer printouts will be introduced into court and if there is a possibility that|Investigative Automation Support|Section personnel will be called upon to testify.

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 16 - 114

EFFECTIVE: 06/01/94

| 16-10.2 | Investigative Automation Support | Section Actions
Regarding Request

EFFECTIVE: 06/01/94

16-10.2.1 Approval of Request

The following factors are considered prior to approval of
a request for computer assistance:

- (1) Priority of the case - investigation
- (2) Deadline required
- (3) Computerization costs versus manual costs
- (4) Complexity and volume

(5) All online ISIS requests must be approved by the
Assistant Director and Deputy Assistant Director(s), Criminal
Investigative Division.

EFFECTIVE: 05/08/81

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 16 - 115

16-10.2.2 Completed Product

After a request has been approved, the results of the computer assistance will usually be furnished on printouts which will all be printed in upper case (capital) letters. These printouts can be prepared:

(1) In multiple copies where requested and necessary.

(2) On paper eight and one half inches in length and eleven inches in width or on paper eleven inches in length and from ten to sixteen inches in width.

EFFECTIVE: 05/08/81

16-11 WORD PROCESSING COORDINATION

Word Processing (WP) has been defined as the manipulation of textual material through the use of a keyboarding device capable of controlled storage, retrieval and automated typing. However, within the FBI implementation of the WP concept means production of typewritten documents and communications more efficiently through the use of systematic procedures, automated office equipment/communications devices and skilled personnel. Equipment used in the implementation of this concept include:

(1) Dictation/Transcription Equipment

(2) Standalone, nonvisual display and/or visual display text-editing machines with a printing device for each machine

(3) Shared-Logic text-editing systems comprised of keyboard visual display units which share a controller and printing device

(4) Shared Resource (distributed/clustered) text-editing systems comprised of both standalone and shared-logic capabilities and communications interface

EFFECTIVE: 05/08/81

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 16 - 116

16-11.1 Requests For Word Processing Equipment

All requests for WP equipment are considered according to WP equipment standards set forth in Federal Property Management Regulations (FPMRs), Federal Procurement Regulations (FPRs), and Department of Justice (DOJ) Orders. Processing of WP equipment requests is as follows:

(1) The Assistant Director of the Information Resources Division (IRD) has been assigned responsibility for reviewing the merits and approval/disapproval of all WP equipment requests.

(2) All requests for WP equipment are to be forwarded by appropriate communication, addressed to the Director, FBI, Attention: Information Resources Division.

EFFECTIVE: 06/01/94

16-11.1.1 Dictation/Transcription Equipment

When reviewing requests for dictation/transcription (D/T) equipment, the following equipment vs. manpower parameters will normally be used:

(1) 1 - Portable or desk-top dictation machine for every five headquarters (HQ) city Agents

(2) 1 - Desk-top transcriber for each employee assigned to a WP center, excluding supervisors

(3) 1 - Portable dictation machine for Investigative Assistants and/or Agents primarily assigned to "record check" duties

(4) 1 - Portable dictation machine for each Agent in resident agencies where no secretary is available and five or less Agents are assigned

(5) 1 - Portable dictation machine for every two Agents and a desk-top dictation machine for every five Agents assigned to resident agencies having a complement of five or more Agents

(6) 1 - Combination D/T machine for use of the Senior Resident Agent and the secretary/stenographer in those resident

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 16 - 117

agencies where secretarial/stenographic assistance is available

(7) Telephone dictation capability (if available in HQ city) for use by resident agencies in dictating expedite, nonsensitive airtels and teletypes

EFFECTIVE: 07/23/90

16-11.1.2 Text-Editing Equipment

When reviewing requests for text-editing equipment, the following criteria will normally be used:

(1) Combined Clerk-Stenographer, Secretary, Clerk-Typist and/or Clerk Dictation Machine Transcriber personnel allocation of the requesting field office/division

(2) The average hourly typing production rates determined during WP Studies at two representative field offices and FBIHQ for the typing personnel identified in (1), directly above.

(3) Economic justification of WP text-editing equipment, normally requires its utilization to a minimum of 80% of its available time (1,400 hours per year, 250 available days/year x 7-hour work shift = 1,750 hours x .80 = 1400 hours), and its utilization for the processing of appropriate WP applications.

(a) The studies indicate that an appropriate WP application is where 20% or more of all lines typed are repetitive in nature, i.e., that portion of a revision which is unchanged during a revision cycle.

(b) Special applications within a specific office will be considered on a case-by-case basis.

EFFECTIVE: 07/23/90

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 16 - 118

16-11.1.3 Equipment/Vendor Selection

All decisions as to equipment/vendor selection for WP equipment will be made at FBIHQ based on standards set forth in FPMRs, FPRs, DOJ Orders, and mandatory and desirable functional requirements. Basic selection criteria has been derived from Federal Supply Schedule contracts and WP equipment evaluations derived from the WP studies of two representative field offices in an effort to ensure procurement of appropriate equipment.

EFFECTIVE: 11/12/80

16-11.2 Allocation of Text-Editing Equipment

(1) In allocating text-editing equipment to field offices/divisions, primary consideration will be given to ensuring 80% utilization of the text-editing equipment during its available time (See 16-11.1.2). It is suggested that allocated equipment be assigned to areas where dedicated typing personnel can use any available piece of text-editing equipment.

(2) Results of previously mentioned field office WP studies have shown that Secretarial personnel type only 15% of the time. For this reason, secretaries are not good candidates for assigning text-editing equipment.

EFFECTIVE: 11/12/80

16-11.3 Word Processing (WP) Equipment Inventory Matters

(1) All WP equipment must be inventoried according to provisions set forth in the FBI's "Accountable Property Manual."

(2) Any problems arising with the WP equipment inventory should be referred to Information Resources Division (IRD). IRD will work with the Property Accounting Systems Unit in resolving WP equipment inventory problems.

Sensitive

PRINTED: 02/18/98

XXXXXX
XXXXXX
XXXXXXFEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

6

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 552Section 552a☐ (b)(1)☐ (b)(7)(A)☐ (d)(5)☒ (b)(2)☐ (b)(7)(B)☐ (j)(2)☐ (b)(3)☐ (b)(7)(C)☐ (k)(1)☐ (b)(7)(D)☐ (k)(2)☒ (b)(7)(E)☐ (k)(3)☐ (b)(7)(F)☐ (k)(4)☐ (b)(4)☐ (b)(8)☐ (k)(5)☐ (b)(5)☐ (b)(9)☐ (k)(6)☐ (b)(6)☐ (k)(7)

- ☐ Information pertained only to a third party with no reference to the subject of your request or the subject of your request is listed in the title only.
- ☐ Documents originated with another Government agency(ies). These documents were referred to that agency(ies) for review and direct response to you.

Pages contain information furnished by another Government agency(ies). You will be advised by the FBI as to the releasability of this information following our consultation with the other agency(ies).

Page(s) withheld inasmuch as a final release determination has not been made. You will be advised as to the disposition at a later date.

Pages were not considered for release as they are duplicative of _____

Page(s) withheld for the following reason(s): _____

- ☒ The following number is to be used for reference regarding these pages:

MIOG Pet Sec 16 p 119-124

XXXXXXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X for this page X
XXXXXXXXXXXXXXXXXXXX

XXXXXX
XXXXXX
XXXXXX

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 16 - 125

EFFECTIVE: 02/16/89

16-14 REVIEW OF LONG DISTANCE TELEPHONE TOLL CALL RECORDS
(INVESTIGATIVE TECHNIQUE)

For information concerning this matter see MIOG, Part II,
Section 10 (Investigative Techniques).

EFFECTIVE: 02/16/89

16-15 NATIONAL LAW ENFORCEMENT TELECOMMUNICATIONS SYSTEM, INC.
(NLETS) (See MIOG, Part II, 16-16 and MAOP, Part II,
7-5.2.)

(1) NLETS is the only national telecommunications network which provides Federal, state, and local law enforcement with the capability to exchange free-form criminal justice and criminal justice-related information interstate. It provides the capability to access most out-of-state vehicle registration and driver's license records automatically. Most field offices have access to NLETS via state or metropolitan area control terminals used to access the National Crime Information Center and/or state and local information systems.

(2) NLETS enhances the effectiveness of the FBI's investigative activities. In most instances NLETS makes it unnecessary for field offices to use the intra-FBI communications process to handle "one shot" leads such as a vehicle registration request. Without NLETS the requesting field office would have to prepare and transmit a teletype, airtel, or letter to the field office covering the territory of the source agency, such as the Department of Motor Vehicles (DMV) in another state. The receiving office would then open and assign a case, and the case Agent would have to cover the auxiliary lead and prepare and send written response to the requesting office. Use of NLETS for routine DMV and driver's license checks will produce a cost savings resulting from the reduction in paperwork. Additionally, the speed of direct communications will provide instantaneous results and an investigative time savings will also be realized.

(3) You should be aware that NLETS does not have any telecommunications security capability and care must be taken to limit

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 16 - 126

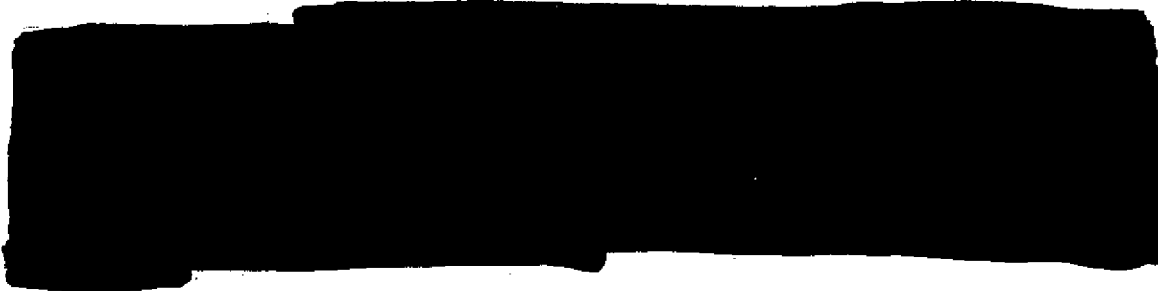
use of NLETS to the acquisition and dissemination of nonsensitive information. The following guidelines are set forth regarding the use of NLETS by the FBI:

(a) NLETS should be used to obtain nonsensitive record information from state and local law enforcement, license, and service agencies.

(b) NLETS may be used to transmit administrative messages (travel plans, weather advisories, etc.) between field offices and state and local law enforcement agencies.

(c) When appropriate, NLETS may be used by field offices to transmit APB-type general descriptive information to all law enforcement agencies in specific geographic areas.

(d) NLETS may not be used to transmit FBI investigative information extracted from the Central Records System to other Federal, state, or local law enforcement agencies or between FBI field offices. NLETS may be used to advise the requestor that the desired information will be provided by the specific field office, covering the requestor's territory and the requested information should be transmitted to that field office via SAMNET, facsimile, or registered mail.



EFFECTIVE: 08/18/94

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 16 - 127

16-16 NATIONAL CRIME INFORMATION CENTER (NCIC) (See MIOG, Part I, 79-1.2 and MAOP, Part II, 7-5.2.)

Those field offices needing assistance or making special requests should contact the Criminal Justice Information Services Division, Programs Support Section at FBIHQ. Programs Support Section at FBIHQ may be contacted via the National Law Enforcement Telecommunications System, Inc. (NLETS), using the identifier DCFBIWAT8. (See Section 16-15 above.)

EFFECTIVE: 08/18/94

16-16.1 Off-Line Search (See MAOP, Part II, 7-5.1.)

An off-line search (inquiry) is a special query of the NCIC computer for information which cannot be obtained through the use of an on-line inquiry. An off-line search of NCIC data may be conducted and/or coordinated only by the Criminal Justice Information Services Division, Programs Support Section at FBIHQ at the request of the case Agent or field supervisor. For more details, see the NCIC pamphlet, "NCIC Off-Line Search."

EFFECTIVE: 08/18/94

16-16.2 Canadian Police Information Centre (CPIC) System (See MAOP, Part II, 7-5.3.)

The CPIC System may be accessed through NLETS. Refer to your State Operating Manual for guidelines to access this database.

EFFECTIVE: 05/13/96

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 16 - 128

16-16.3 Missing Person Reports

(1) The signing of the Missing Children Act (MCA) on October 12, 1982, requires policy changes in the Bureau's handling of missing person reports received. The Act requires the Attorney General to "acquire, collect and preserve any information which would assist in the location of any missing person (including an unemancipated person as defined by the laws of the place of residence of such person) and provide confirmation as to any entry for such a person to the parent, legal guardian, or next of kin of that person (and the Attorney General may acquire, collect, classify, and preserve such information from such parent, legal guardian, or next of kin)." Therefore, a parent, legal guardian, or next of kin of a missing child has the legal right to inquire of the FBI whether data on the missing child has been entered in the NCIC Missing Person File. When a field office receives one of these requests, a determination should be made verifying that the requestor is the parent, legal guardian, or next of kin by means of any form of identification data. Thereafter, an NCIC Missing Person File inquiry should be made to determine the existence of a record.

(2) In the rare case where (1) a record has not been entered because the local authorities refused to enter, and (2) the parent, legal guardian, or next of kin requests the FBI to enter the record, follow the procedures below. (Use Forms FD-626 and FD-630. These forms should be placed in the 79-0 administrative control file after NCIC entry has been made by the field office. These forms are intended for field office use and should not be forwarded to FBIHQ.)

(a) Explain to the requestor that the FBI only enters data on individuals into the file in rare cases where the local police refuse to enter the data on the individual.

(b) Ascertain if there has been an unambiguous refusal by the local authorities to enter the record into NCIC and specifically who at the local department refused to make such entry.

(c) Inquire of the requestor if a missing person report is on file with a police agency and, if so, secure a copy of same. If possible, have the requestor bring such a copy with him/her.

(d) If at all feasible, insist that the parent, legal guardian, or next of kin come to the field office (including resident agencies, if applicable) to make the report. Verify the identity of the requestor.

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 16 - 129

(e) Explain to the requestor that the FBI does not have authority or jurisdiction to investigate missing person cases unless there has been a violation of Federal law falling within our jurisdiction, e.g., the Federal kidnaping statute.

(f) Advise the requestor of the extreme importance of notifying the FBI promptly when the child returns.

(g) Indicate to the requestor that his/her name and telephone number will be contained within the text of the message and that he/she may be called directly if the child is located.

(h) The field office will telephonically confirm the refusal of the local agency to enter the record and whether or not there are extenuating circumstances of which the FBI should be aware. Additionally, if the refusing police agency has a "time delay entry" rule, the FBI should proceed to enter the record and coordinate the removal of such record with the police agency when they enter their record.

(i) After good faith satisfaction of the above, the field office will enter the missing person record. If such extenuating circumstances exist, advise the parent, legal guardian, or next of kin that no entry is being made.

(3) After an NCIC entry is made, the following validation procedures should be followed:

(a) A written communication should be sent to the local authorities confirming that agency's stated refusal to enter the record, the FBI entry of the record, and the necessity of being immediately notified when the individual returns.

(b) A copy of the above communication should be sent to the parent, legal guardian, or next of kin reiterating the extreme importance and necessity for the FBI being promptly advised of the individual's return.

(c) Set a tickler to contact the parent, legal guardian, or next of kin on the third working day following the date of entry, again at the end of two weeks, four weeks, and then once a month until the individual has been located. If, after two consecutive attempts, the FBI cannot, despite reasonable efforts, locate a person or agency able to verify the currency of the record, the record should be removed from the NCIC File and the requesting parent, legal guardian, or next of kin who requested entry should be

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 16 - 130

notified by registered mail.

(4) The NCIC Operating Manual, Part 8, contains the necessary information to enter a missing person record. In addition to this information, the following should also be included in the Miscellaneous Field of the record: the parent's, legal guardian's, or next of kin's name, address, and telephone number. If the local or state law enforcement agency has a pending case, enter the agency's name and case number, if available, following the parent, legal guardian, or next of kin information. This information may have to be abbreviated since the Miscellaneous Field is limited to 121 characters. Any other pertinent information may follow if space is available.

(5) The Act does not confer upon the FBI any new investigative jurisdiction. A positive response to an inquiry should not be interpreted as constituting FBI authorization for detention of the individual described in the record. The FBI is not responsible for effectuating the return of the individual to the parent, legal guardian, or next of kin. Inquiring agencies should be informed clearly of these facts.

(6) Upon receipt of a hit confirmation request, the field office (being the originating agency (ORI) of the record) must within ten minutes furnish a substantive response, i.e., a positive or negative confirmation or notice of the specific amount of time necessary to confirm or reject.

(7) The field office must make a reasonable attempt to notify the investigating agency and/or the parent, legal guardian, or next of kin of the missing child of the inquiry on the missing person record. If unsuccessful, notify the agency which is seeking hit confirmation that all reasonable efforts have been exhausted and that the information in the record is the best available information at hand. If successful in contacting the parent, legal guardian, or next of kin, advise them of the individual's location and the inquiring agency's location. Advise them to immediately contact the inquiring agency. After contacting all parties concerned, immediately clear your record from the file.

(8) When the subject of a juvenile record becomes emancipated, the record is retained indefinitely in NCIC until action is taken to remove the record.

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 16 - 131

EFFECTIVE: 05/11/87

16-16.4 Unidentified Person File

The Missing Children Act of 1982 also resulted in the implementation of the NCIC Unidentified Person File. This file contains records for unidentified deceased persons (including victims of a catastrophe), body parts that have been recovered, and unidentified living persons who are unable to ascertain their identities (such as amnesia victims and small children or infants).

The Unidentified Person File operates in conjunction with the Missing Person File. Specifically, records from one file are searched with those in the other file. Personal identifiers can be entered in both files, which are used to compare an unidentified person record with missing person records and vice versa. For complete details on the Unidentified Person File, refer to the NCIC Operating Manual, Part 12.

EFFECTIVE: 07/28/87

16-16.5 Foreign Fugitives

The NCIC Foreign Fugitive File operates for the purpose of locating foreign fugitives. Records for fugitives wanted in Canada are entered by Royal Canadian Mounted Police Headquarters in Ottawa and include individuals wanted in Canada based on Canada-wide warrants. Records for fugitives wanted by other foreign countries are entered by the U.S. National Central Bureau (USNCB), the point of contact for the International Criminal Police Organization (INTERPOL), based on information received on the Red Notices (wanted notices) issued by INTERPOL member countries. All record entries are made in accordance with established entry criteria. Refer to Part 9 of the NCIC Operating Manual for details on inquiries and procedures on handling positive responses.

EFFECTIVE: 07/28/87

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 16 - 132

16-16.6 U.S. Secret Service (USSS) Protective File

This NCIC File lists records of individuals who may pose a threat to a USSS protectee. All records are entered and maintained by the USSS. Refer to Part 11 of the NCIC Operating Manual for details.

EFFECTIVE: 07/28/87

16-16.7 Bureau of Alcohol, Tobacco and Firearms (ATF) Violent Felon File (See MAOP, Part II, 7-2.10.)

The ATF Violent Felon File contains records on individuals who have had three or more previous convictions for a violent felony or serious drug offense. These persons, if found in possession of a firearm, are in violation of Title 18, USC, Section 924 (e)(1), which provides a fine of not more than \$25,000 and imprisonment of not less than 15 years with no suspension, parole, or probation. All records are entered and maintained by the ATF. Refer to NCIC Technical and Operational Updates 91-4 and 92-1 for details.

EFFECTIVE: 08/18/94

16-16.8 Deported Felon File (See MAOP, Part II, 7-2.10.)

The Deported Felon File contains records on criminal aliens who have been deported for drug trafficking, firearms trafficking, and serious violent crimes in the event they might reenter the United States without permission. These criminal aliens who have been deported and reenter the United States without permission are in violation of Title 8, USC, Section 1326, which carries a fine of up to \$250,000 and incarceration of up to 20 years. All records are entered and maintained by the Immigration and Naturalization Service. Refer to NCIC Technical and Operational Update 95-3 for details.

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 16 - 133

EFFECTIVE: 05/13/96

16-16.9 Violent Gang and Terrorist Organization File (VGTOF)
(See also MAOP, Part II, 7-5.8.)

The VGTOF is designed to provide identifying information about violent criminal gangs and members of those gangs and terrorist organizations and members of those organizations to law enforcement personnel. The information serves to warn law enforcement officers of the potential danger posed by violent individuals and promotes the exchange of information about these organizations and members to facilitate criminal investigations. Refer to NCIC Technical and Operational Updates 94-2 and 95-2 for details.

EFFECTIVE: 05/13/96

16-17

[REDACTED]

b2
b7E

[REDACTED]

[REDACTED]

[REDACTED]

Sensitive

PRINTED: 02/18/98

XXXXXX
XXXXXX
XXXXXXFEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET15

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 552Section 552a☐ (b)(1)☐ (b)(7)(A)☐ (d)(5)☒ (b)(2)☐ (b)(7)(B)☐ (j)(2)☐ (b)(3)☐ (b)(7)(C)☐ (k)(1)☐ (b)(7)(D)☐ (k)(2)☒ (b)(7)(E)☐ (k)(3)☐ (b)(7)(F)☐ (k)(4)☐ (b)(4)☐ (b)(8)☐ (k)(5)☐ (b)(5)☐ (b)(9)☐ (k)(6)☐ (b)(6)☐ (k)(7)

- ☐ Information pertained only to a third party with no reference to the subject of your request or the subject of your request is listed in the title only.
- ☐ Documents originated with another Government agency(ies). These documents were referred to that agency(ies) for review and direct response to you.

Pages contain information furnished by another Government agency(ies). You will be advised by the FBI as to the releasability of this information following our consultation with the other agency(ies).

Page(s) withheld inasmuch as a final release determination has not been made. You will be advised as to the disposition at a later date.

Pages were not considered for release as they are duplicative of _____

Page(s) withheld for the following reason(s): _____

- ☒ The following number is to be used for reference regarding these pages:

MIOG Pt II Sec 16 p134-148

XXXXXXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X for this page X
XXXXXXXXXXXXXXXXXXXX

XXXXXX
XXXXXX
XXXXXX

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 16 - 149

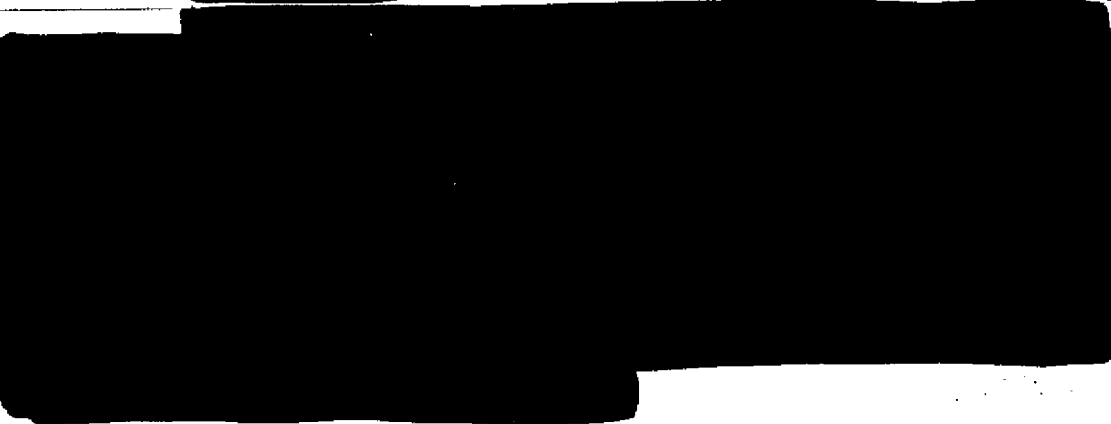
EFFECTIVE: 11/24/97

16-18 FBI MICROCOMPUTER POLICY

EFFECTIVE: 02/16/89

16-18.1

b2
b7E



EFFECTIVE: 07/14/95

16-18.2 Purpose and Objectives of Policy

(1) The purpose of this policy is to establish appropriate internal practices and procedures to ensure the proper management and use of microcomputers and the accuracy of microcomputer-processed information. A microcomputer, as defined for this policy, is any computer including the standard terminals, intelligent workstations, and all similar machines from any manufacturer that provides local processing for an end-user. Implementing control procedures unique to microcomputers should reduce the risk of illegal system access, data loss and stolen or unauthorized use of hardware and software.

(2) The objective of this policy is to ensure that the management and use of microcomputer resources in the FBI are in compliance with regulations relevant to automation and information

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 16 - 150

management.

EFFECTIVE: 03/23/92

16-18.3 Scope and Applicability

This policy applies to:

(1) All elements of the FBI which process, store, or produce information on any microcomputer, including word processors with local storage or memory,

(2) Microcomputers connected to FBI or public telecommunications networks, and

(3) Microcomputers used in standalone mode.

EFFECTIVE: 03/23/92

16-18.4 Responsibilities

(1) The Operations Management Section (OMS), Information Resources Division (IRD), shall:

(a) Provide hardware and software operational guidance and problem resolution;

(b) Maintain authorized software listings and act as an information clearinghouse for users;

(c) Maintain a library of applications for dissemination to Computer Specialists requesting assistance in a particular area;

(d) Communicate noteworthy developments and activities to users;

(e) Deleted

(f) Assist in the development, maintenance and dissemination of microcomputer principles, standards and guidelines;

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 16 - 151

(g) Deleted

(h) Provide guidance on applicable federal, departmental and FBI information resource management laws, policies, principles, standards and guidelines;

(i) Provide Computer Specialists guidance in determining the feasibility of using either a microcomputer application or a mainframe application for effective implementation of automated technology throughout the FBI;

(j) Coordinate procurement and delivery of hardware and software;

(k) Coordinate all routine microcomputer maintenance activities, including routine requests for maintenance and maintenance contracts for seized and forfeited microcomputers;

(l) Deleted

(m) Provide ADPT Service Support Center operations to handle all associated issues, problems and questions.

(2) The Assistant Directors (ADs) of each FBI Headquarters division and the Special Agents in Charge (SACs) of each field office must ensure effective, efficient and economical management and allocation of microcomputers as well as enforcement of microcomputer policy, principles, standards and guidelines prescribed by the Director.

(3) Each FBI division, through the Computer Specialist, shall:

(a) Systematically maintain a current on-site listing, in accordance with FBI inventory guidance, of its microcomputer hardware, software, and administrative or investigative data bases; (See MIOG, Part I, 190-2.3(3).)

(b) Provide hardware and software operation guidance and problem resolution to end-users;

(c) Communicate noteworthy developments and activities to end-users;

(d) Develop contingency plans (including emergency response, backup operations and recovery) that are consistent with IRD

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 16 - 152

ADPT facility contingency plans to ensure continued operation of essential functions within the division in the event that data processing support is interrupted;

(e) Maintain and disseminate to end-users microcomputer policy, principles, standards and guidelines provided by IRD;

(f) Perform preventive maintenance as necessary on Information Technology microcomputer equipment.

(4) End-users must ensure that:

(a) All microcomputer data files are accurate, complete and reliable;

(b) All microcomputer data files are secured consistent with central records system procedures;

(c) Planned backup and recovery procedures are executed; and,

(d) All other applicable rules, regulations, policies and procedures are followed.

(e) Perform preventive maintenance as necessary on Information Technology microcomputer equipment (cleaning).

(5) The Property Procurement and Management Section of the Finance Division shall submit annual inventory reports of microcomputer hardware to each Computer Specialist so that these inventories can be verified. (See MIOG, Part II, 16-18.9.)

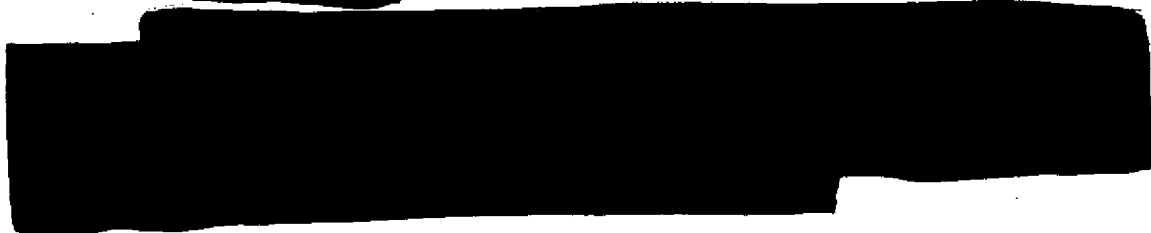
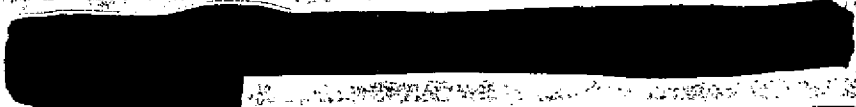
EFFECTIVE: 08/04/97

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 16 - 153

b2
b7E
16-18.5



EFFECTIVE: 09/16/93

| 16-18.5.1 | Deleted |

EFFECTIVE: 07/26/95

| 16-18.5.2 | Deleted |

EFFECTIVE: 07/26/95

| 16-18.5.3 | Deleted |

EFFECTIVE: 07/26/95

16-18.5.4 Deleted

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 16 - 154

EFFECTIVE: 03/23/92

16-18.5.5 Deleted

EFFECTIVE: 03/23/92

16-18.6 Information Management

EFFECTIVE: 03/23/92

16-18.6.1 Source of Data

Any information subject to the provisions of the Privacy Act that is processed by or stored in microcomputers must be traceable to documents serialized in Bureau files (the FBI's Central Records System) or in other established FBI systems of records.

EFFECTIVE: 03/23/92

16-18.6.2 Access Controls

Access to automated records is restricted to a need-to-know basis consistent with existing controls afforded counterpart manual records.

EFFECTIVE: 02/16/89

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 16 - 155

16-18.6.3 Retention/Destruction of Electronic Information

(1) At the conclusion of an investigation, the data need not be retained in electronic format. However, if paper output from the data base was required by the substantive supervisor or the prosecuting attorney, or was introduced as evidence in a courtroom, that output must be serialized in the FBI file and the data in electronic format must be retained.

(2) Electronic media to be retained must be stored as a serial, 1A or 1B exhibit. The media must be labeled with the following information in the "Content" and "Comments" sections of the Data Descriptor Label (SF-711):

(a) Description of the microcomputer being used (e.g., standard terminal, intelligent workstation, etc.);

(b) Identity of the operating system (e.g., CTOS, BTOS, MS-DOS, OS2, etc.) and its release number;

(c) Application and release used to create the original data base (e.g., RBase, Multiplan, Lotus 123, etc.); and

(d) Archived data base name and, where applicable, password.

EFFECTIVE: 02/16/89

16-18.7 Requests for Microcomputer Resources

Generally, FBI Headquarters will acquire microcomputers and related resources, including software, peripheral devices, initial training and maintenance contracts, through large-volume procurements as a cost containment measure. Priority of need will dictate microcomputer distribution to field offices by FBI Headquarters and the application of microcomputer resources within each field division. Microcomputers used as part of a "front" operation of undercover or special operations activities will be approved by either the Criminal Investigative Division or National Security Division with procurement assistance and funding provided by IRD.

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 16 - 156

EFFECTIVE: 07/14/95

| 16-18.7.1 | Deleted |

EFFECTIVE: 02/16/89

| 16-18.7.2 | Deleted |

EFFECTIVE: 02/16/89

| 16-18.7.3 | Deleted |

EFFECTIVE: 02/16/89

| 16-18.7.4 | Deleted |

EFFECTIVE: 02/16/89

| 16-18.8 | Security - See MIOG, Part II, Section 35. |

EFFECTIVE: 07/26/95

| 16-18.8.1 | Deleted |

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 16 - 157

EFFECTIVE: 07/26/95

| 16-18.8.2 | Deleted |

EFFECTIVE: 07/26/95

| 16-18.8.3 | Deleted |

EFFECTIVE: 07/26/95

| 16-18.8.4 | Deleted |

EFFECTIVE: 07/26/95

| 16-18.8.5 | Deleted |

EFFECTIVE: 07/26/95

| 16-18.8.6 | Deleted |

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 16 - 158

EFFECTIVE: 07/26/95

| 16-18.8.7 | Deleted |

EFFECTIVE: 07/26/95

| 16-18.8.8 | Deleted |

EFFECTIVE: 07/26/95

| 16-18.8.9 | Deleted |

EFFECTIVE: 07/26/95

| 16-18.8.10 | Deleted |

EFFECTIVE: 07/26/95

| 16-18.8.11 | Deleted |

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 16 - 159

EFFECTIVE: 07/26/95

| 16-18.8.12 | Deleted |

EFFECTIVE: 07/26/95

| 16-18.8.13 | Deleted |

EFFECTIVE: 07/26/95

16-18.9 Reporting Requirements (See MIOG, Part II, 16-18.4(5) and 35-9.4.7.)

(1) Computer Specialists (CS) in conjunction with the Supply Technician will maintain current inventories of hardware on the FBI's Property Management System. On an annual basis, the Property Procurement and Management Section of the Finance Division will submit an inventory of microcomputer hardware to each CS for verification. Any discrepancies in the report must be rectified immediately. Inventory information will include the following:

- (a) Hardware:
 - Division
 - Equipment type
 - Equipment profile (for example, Model Number)
 - Hard disk type
 - Floppy disk type
 - Monitor type, including TEMPEST/non-TEMPEST designation
 - Location (Squad/Unit)
 - Function (e.g., rotor, squad secretary)
 - Other

- (b) Deleted

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 16 - 160

- (2) Deleted
- (3) Deleted
- (4) Deleted
- (5) Deleted

EFFECTIVE: 09/22/97

16-18.10 Automation Training Staff

(1) The Automation Training Staff, from the Service Support & Implementation Unit, SSIU, provides instructor-based training in classroom settings on PC-based applications and investigative/administrative applications to field, FBIHQ and Legat personnel. The staff administers training through the use of interactive video (IVD), computer-based training (CBT), compact disc (CD-ROM) and/or video methods.

(2) The staff researches training techniques and new technologies of data communications and microcomputers. It provides assistance and support to automation personnel in problem resolution. The staff works with applications program managers, computer clients, project teams and appropriate division personnel in the development and delivery of training.

EFFECTIVE: 07/26/95

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 16 - 161

16-18.11 Computer Specialist Selection Process

(1) Computer Specialists conduct programming tasks to support the creation, maintenance, and analysis of information files and the communication of data in a fourth-generation distributed environment.

(2) Entrance salaries range from GS-5 through GS-13 at FBIHQ and range from GS-5 through GS-12 in a field office. Hiring may occur at FBIHQ or a field office. The basic salary is commensurate with the applicant's education and experience.

EFFECTIVE: 12/13/96

16-18.11.1 Computer Specialist Eligibility Requirements

- (1) Be a United States citizen.
- (2) Be a high school graduate or its equivalent and have additional education as set forth below.
- (3) Pass a rigorous background investigation including drug and polygraph tests.

EFFECTIVE: 12/13/96

16-18.11.2 Computer Specialist Qualifications

(1) GS-5: Must have a Bachelor's Degree or three years of general experience, one year of which is equivalent to at least the GS-4 in the federal government. General experience is that which provided basic knowledge of data processing functions and general management principles that enabled an understanding of the stages required to automate a work process. Experience may have been gained in positions such as a computer operator or assistant, computer sales representative, program analyst, or other position that required the use or adaptation of computer programs and systems.

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 16 - 162

(2) GS-7: Must have one full year of graduate level education of cumulative grade point average of 3.0 or higher or one year of specialized experience equivalent to at least the GS-5 in the federal government. Specialized experience is that which includes the performance of tasks such as:

(a) translating detailed logical steps developed by others into language codes;

(b) conducting user-requirements analysis and synthesizing the results into information flowcharts;

(c) troubleshooting, in particular during unscheduled halts;

(d) prioritizing processes for production efficiency; and

(e) organizing documentation for cost/benefit studies.

(3) GS-9: Must have two full years of progressively higher level graduate education or a Master's Degree or equivalent graduate degree or one year of specialized experience equivalent to at least the GS-7 in the federal government. Specialized experience is that which demonstrates knowledge of computer requirements and techniques in carrying out multitask project assignments typical of minor system modifications. Such assignments must demonstrate ability in analysis of:

(a) interfunctioning system components;

(b) planning the sequence of actions to complete the project; and

(c) leadership in at least a segment of the overall project.

(4) GS-11: Must have three years of progressively higher level graduate education or a Ph.D. or equivalent doctoral degree or one year of specialized experience equivalent to at least the GS-9 in the federal government. Specialized experience is that which demonstrates successful accomplishment of projects involving a range of requirements and techniques as well as those of computer specialty areas. In addition to those noted for the GS-9 level, assignments

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 16 - 163

must have been involved in:

(a) planning the sequence of actions to complete the project in coordination with outside organizational units; and

(b) the development of project controls and guidelines.

(5) GS-12 and above: Must have experience that demonstrates accomplishment of major project assignments that required a wide range of knowledge of requirements and techniques. Such assignments include those involving:

(a) the analysis of a number of alternative approaches; and

(b) advising management regarding major aspects of ADP system design such as what system interrelationships, operating modes, software, and/or equipment configuration will be required or affected during project builds or enhancements.

(6) If substituting education for experience, major study must be in any of these disciplines: Computer Science, Information Science, Management Information Systems, Mathematics, Statistics, Operations Research, or Engineering, or course work that required the development or adaptation of computer programs and systems and provided knowledge equivalent to a major in the computer field.

EFFECTIVE: 12/13/96

16-18.11.3 Computer Specialist Promotions

A career path for the Computer Specialists has been established at the GS-5 through GS-13 level at FBIHQ and GS-5 through GS-12 level in the field offices. In order to qualify for the next grade level the employee must meet the following requirements:

(1) specified technical experience;

(2) specified training;

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 16 - 164

- (3) specified performance rating;
- (4) maintain the appropriate level of working proficiency in specific applications;
- (5) have a favorable recommendation of immediate supervisor; and
- (6) approval from the Program Manager (PM) of the Computer Specialists Management Program (CSMP). The Personnel Division's Staffing Unit will not take action on a request for promotion without the approval of the PM.

EFFECTIVE: 12/13/96

16-18.11.4 Computer Specialist Career Board Selections

The PM of the CSMP must be notified of all career board selections. At the conclusion of the career board, the PM must receive all related documentation before approval will be granted.

EFFECTIVE: 12/13/96

16-18.11.5 Computer Specialist Reassignments

The PM must give approval before an employee is reassigned into or out of the CS position.

EFFECTIVE: 12/13/96

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 16 - 165

16-18.11.6 Computer Specialist Internal/External Postings

The PM is to be notified of all internal/external postings prior to occurrence.

EFFECTIVE: 12/13/96

16-19 DATA CIRCUIT TECHNICAL SUPPORT AND TEST EQUIPMENT
MAINTENANCE POLICY

EFFECTIVE: 05/26/89

16-19.1 Technical Support Policy

(1) The communications circuits supporting the Integrated Digital Communications System (IDCS) and Secure Automated Message Network (SAMNET) systems are designed to conserve line costs, while providing reliable service. Certain field offices (FOs) have been established as SAMNET nodes or IDCS hubs and are responsible for maintaining teletype and data circuits for many other FOs, by functioning normally as unattended relay points. Other FOs, although on a smaller scale, function as relay points for the IDCS by linking resident agencies (RAs) and/or off-sites to the major hubs within the network.

(2) The Telecommunications Manager or Supervisory Electronics Technician (SET) in each FO is responsible for providing prompt technical support for these systems.

(3) Offices providing communications support for other offices must have a qualified ET available for immediate circuit restoration assistance during normal work hours.

(4) During off-duty hours, weekends and holidays, a qualified ET must be on call and available to assist with circuit restoration. On-site response should be within one hour after notification or as soon as possible considering travel conditions at the specific office.

(5) Exceptions to the above may be granted by FBIHQ on a

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 16 - 166

case-by-case basis. Request for exceptions should be directed to FBIHQ, Attention: Operations Management Section, Room 6421.

EFFECTIVE: 04/28/94

16-19.2 Test Equipment Maintenance Policy

(1) CMs/SETs are responsible to ensure that all test equipment associated with data circuit maintenance, assigned to their office, is in proper working order.

(2) Any test equipment that develops operational problems or is subject to routine periodic maintenance/calibration must be scheduled for maintenance/calibration promptly.

EFFECTIVE: 05/26/89

16-19.3 Response to FBIHQ Communications

(1) FBIHQ aperiodically issues communications directing maintenance procedures or data equipment/data test equipment that require technical action and/or formal response.

(2) CMs/SETs must respond promptly to any FBIHQ inquiries, directives or surveys to ensure proper maintenance of both data equipment/data test equipment and maximum usage of maintenance/repair contracts. Formal response must be provided when requested.

EFFECTIVE: 05/26/89

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 17 - 1

SECTION 17. APPLICANT AND EMPLOYEE INVESTIGATIONS CONDUCTED
FOR OTHER GOVERNMENT AGENCIES - GENERAL INSTRUCTIONS

17-1 AUTHORITY

(1) Executive Order 10450, which was promulgated in 1953, makes appointment to positions in the Executive Branch subject to a background investigation. The Office of Personnel Management has the primary responsibility to investigate persons being employed in the competitive service and has permitted other Federal agencies with investigative resources to conduct background inquiries.

(2) Even prior to this Executive Order, however, the FBI had been conducting background investigations for other agencies as well as for itself. At present, various statutes, Executive Orders, Departmental Orders, and agreements between the Attorney General and other Federal entities provide a basis for the FBI's role in this area. If specific information is desired concerning the authority for the FBI to conduct any investigation, contact FBIHQ for detailed information.

EFFECTIVE: 12/10/91

17-2 CLASSIFICATIONS OF INVESTIGATIONS (See MIOG, Introduction, 2-2.2; Part I, 77-1.1 through 77-1.13, 77-4.3, 77-4.11, 140-3, 161-4, 161-5, 161-9; MAOP, Part II, 3-1.1, 3-1.2, 10-23; & Correspondence Guide-Field, 1-17.)

Requests for an FBI investigation are made in writing by another federal entity. These requests are assigned to a classification which, in general, corresponds to the source of the request. The following classifications are currently in use:

- Office
- (1) 73 - Background Investigation - Pardon Attorney's
 - (2) 77
 - (a) 77A - Background Investigation - Presidential Appointment with Senate

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 17 - 2

Confirmation - Nonreimbursable

- (b) 77B - Background Investigation -
U.S. Courts - 15 Year - Reimbursable
- (c) 77C - Background Investigation -
U.S. Courts - 10 Year - Reimbursable
- (d) Deleted
- (e) 77E - Background Investigation -
Department of Justice - Nonreimbursable
- (f) 77F - Background Investigation -
U.S. Attorney's Office (Staff) -
Reimbursable
- (g) Deleted
- (h) 77H - Background Investigation -
U.S. Attorney's Office (Attorney) -
Reimbursable
- (i) 77I - Background Investigation -
Department of Justice - Reimbursable
- (j) 77J - Background Reinvestigation -
Department of Justice - 10 Year -
Reimbursable
- (k) 77K - Background Reinvestigation - Department of
Justice - 7 Year - Reimbursable
- (l) 77L - Background Reinvestigation - Department of
Justice - 5 Year - Reimbursable
- (m) 77M - Background Reinvestigation - Department of
Justice - 3 Year - Reimbursable
- (3) 116A - Department of Energy - Applicant
116B - Department of Energy - Five-Year
Reinvestigation
116C - Nuclear Regulatory Commission - Applicant
116D - Nuclear Regulatory Commission - Five-Year
Reinvestigation

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 17 - 3

- (4) 140A - Office of Personnel Management - Referral
- 140B - Office of Personnel Management - Employees
- 140C - Office of Personnel Management - Other
- (5) 161A - Level I-Presidential Appointment
Level I-Presidential Appointment, Senate
Confirmation
- 161B - Level II-Presidential Appointment, Senate
Confirmation (Non-White House)
- 161C - Level III-Presidential Appointment
Level III-Presidential Appointment, Senate
Confirmation
- 161D - Level I-White House Staff
- 161E - Level II-White House Staff
Level II-White House Access
Level II-National Security Council
- 161F - Level II-White House Staff
(Five-Year Reinvestigation)
Level II-White House Access
(Five-Year Reinvestigation)
Level II-National Security Council (Five-Year
Reinvestigation)
- 161G - Level III-White House Staff
Level III-White House Access
- 161H - Level III-White House Staff (Five-Year
Reinvestigation)
Level III-White House Access
(Five-Year Reinvestigation)
- 161I - Level III-Congressional Committee
- 161J - Level III-Congressional Committee (Five-Year
Reinvestigation)
- 161K - Expanded Name Check
- 161L - Level II-Presidential Appointment
Level II-Presidential Appointment, Senate
Confirmation (White House)

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 17 - 4

- (6) 259A - Security Clearance Investigations - Classified Information Procedures Act (CIPA)
- 259B - Security Clearance Investigations - Foreign Intelligence Surveillance Act (FISA)
- 259C - Security Clearance Investigations - Joint Task Forces (JTF)
- 259D - Security Clearance Investigations - Others
- 259E - Security Clearance Investigations - Periodic Reinvestigations/Security Clearances
(See MIOG, Part I, 259-2, 259-3, 259-4, 259-6, 259-7, and 259-8.)

- (7) 260A - Industrial Security Program - Personnel Clearance
- 260E - Industrial Security Program - Personnel Clearance Reinvestigations (See MIOG, Part I, 260-1(2), 260-5.1, 260-5.2.)

Any questions involving 259 and 260 classifications should be directed to the Security Programs Manager (SPM), National Security Division.

EFFECTIVE: 01/03/97

17-2.1 TURK Classifications (See MIOG, Part I, 77-1.2, 77-1.3, 77-1.6, 77-1.8, 77-1.9, 77-1.10, 77-1.11, 77-1.12, 77-1.13, 77-4.3, 77-4.11; MAOP, Part II, 10-23.)

For TURK purposes, these classifications are separated into reimbursable and nonreimbursable investigations. Reimbursable matters are billed to other agencies at a predetermined rate per investigative request, and these funds provide the FBI with the resources with which to address these inquiries. Nonreimbursable matters are funded in the FBI's budget. Where it is possible to have both reimbursable and nonreimbursable requests in one classification, alpha designators have been applied. As a general rule, cases received from the Administrative Office of the U.S. Courts (77B and 77C), the Department of Energy (116A and 116B), Nuclear Regulatory Commission (116C and 116D), Department of Justice (77F, 77H, 77I, 77J, 77K, 77L and 77M), Office of Personnel Management (140B), and White House (161B) are reimbursable.

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 17 - 5

EFFECTIVE: 12/20/96

17-2.2 Applicability of this Section's Instructions

This Section provides instructions and guidance which are applicable to all of the above classifications. Specific requirements which are unique to individual classifications are set forth in Part I of this manual under the appropriate classification.

EFFECTIVE: 12/10/91

17-3 ADMINISTRATIVE PROCEDURES

EFFECTIVE: 12/10/91

17-3.1 Initiation of Investigation

Investigative requests are received from client agencies at FBIHQ and are initiated by teletype, electronic communication, or facsimile transmission depending upon the urgency associated with the request. Personal history data and release forms as received at FBIHQ are forwarded to the field if necessary. Files at FBIHQ will be reviewed, including records of the Criminal Justice Information Services Division, and pertinent information will be forwarded to the field for investigative purposes or for inclusion in the report.

EFFECTIVE: 04/08/96

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 17 - 6

17-3.2 Initial Interview of Applicant

An interview of applicant should be conducted at the inception of the investigation (see Part II, Section 17-5.6, of this manual, for additional instructions concerning this interview). The office covering current residence and/or employment will normally conduct the interview and should promptly set out leads for any additional investigation needed as a result of the interview. Where residence and employment are split between field divisions, FBIHQ will designate office to conduct interview in the opening communication. If a substantial delay is encountered in contacting the applicant or arranging for the interview, immediately notify FBIHQ so that an appropriate course of action can be considered.

EFFECTIVE: 02/12/92

17-3.3 Assignment of Cases

These matters must be searched, opened, and assigned immediately. Investigation is to commence immediately.

EFFECTIVE: 02/12/92

17-3.4 Indices Searches

(1) FBIHQ general and ELSUR indices are searched only against the candidate's name and the names of all close relatives. The name of the candidate and, in presidential appointment cases, the names of all close relatives (except deceased relatives) are also searched through the Criminal Law Enforcement Application (CLEA), Intelligence Information System (IIS), and National Crime Information Center (NCIC) records at FBIHQ. Circumstances may indicate necessity to also search general indices against the names of other persons, businesses or organizations with which the candidate has had contact or association (i.e., cohabitants, foreign nationals, etc.).

(2) Each field office must make a careful search, and advise FBIHQ of the results, of its general and any other specialized indices (except confidential and ELSUR), concerning the below-listed individuals/entities. (Confidential and ELSUR indices need not be searched):

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 17 - 7

- (a) Candidate - offices covering places of residence, employment, or education;
 - (b) Close relatives (see 17-6.9 for identification of persons who are considered close relatives) - residing in field office territory;
 - (c) Cohabitants - office covering current place of residence;
 - (d) Businesses or associations located in field office territory when candidate or appointee holds controlling interest or is an officer;
 - (e) Others - circumstances may indicate necessity to search names of other persons, businesses or organizations with which candidate has been identified.
- (3) Any variations or additional names developed during the investigation should be checked. The search should include all names used by relatives, such as maiden name of a spouse. Advise FBIHQ and interested offices of additional names developed including the identity of any close relatives whose names were not available at the inception of the investigation. It is not necessary to search names of relatives under 15 years of age.
- (4) FBIHQ should be advised of any information located which is identifiable with the candidate, listed relatives, cohabitants and business establishments. If the information is not available in files at FBIHQ, forward a copy of pertinent serials to FBIHQ.
- (5) Deleted

EFFECTIVE: 11/25/94

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 17 - 8

17-3.5 Deadlines (See MIOG, Part I, 73-10, 116-6(2), 161-5.)

(1) Each background investigation conducted by the FBI has a deadline known as a Bureau deadline or BUDED. The BUDED is the date the complete investigation must be received at FBIHQ (in the applicable FBIHQ unit). The BUDED is established by FBIHQ and cannot be changed without FBIHQ authority. The BUDED is to be set forth in each intra-Bureau communication in accordance with FBI policy, whether generated by FBIHQ or the field.

(2) BUDEDs are established principally to meet the needs of the client entity. In setting BUDEDs, FBIHQ will allocate as much time to the field to conduct these investigations as possible.

(3) BUDEDs are to be met unless the reason(s) for not doing so are beyond the control of the investigating office.

(a) If an investigating office is unable to meet the BUDED, it is to promptly advise FBIHQ (the applicable unit) telephonically, to include the reason(s) for delay and when receipt of the complete investigation at FBIHQ is anticipated.

(b) When an investigative office does not meet its BUDED, the reason(s) must clearly be set forth in the "Administrative" section of the cover page(s) of its investigative report.

EFFECTIVE: 11/18/96

17-3.6 Prior Applicant Investigation

Since investigations are frequently forwarded to field offices prior to a completion of a check of FBIHQ records, field office records may disclose a previous applicant-type investigation. If so, the following steps should be taken:

(1) If previous investigation was not conducted within the last six months, notify FBIHQ and other appropriate offices of investigation, and bring previous investigation thoroughly up to date and supplement it as necessary so that total scope will conform in all respects to current standards. Recontact persons previously interviewed who furnished derogatory information if such persons are

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 17 - 9

in a position to furnish current pertinent information and if such inquiry is practicable.

(2) If previous investigation was made within six months preceding receipt of new request, and if it was then complete, send an immediate teletype to FBIHQ and other appropriate offices advising of prior case. Then hold investigation in abeyance until further instructions are received from FBIHQ.

EFFECTIVE: 01/25/88

17-3.7 Leads for Other Offices

(1) Set out leads for other offices immediately as they become known during investigation. Use most expeditious means of communication commensurate with economy to meet deadline.

(2) Furnish FBIHQ with a copy of all communications setting out leads.

(3) If lead is being sent to office which has not received prior communications in case, the following information at least should be included:

(a) Name, aka, and any other title information, such as zone designations in title in 116 cases

(b) Character

(c) Bureau deadline

(d) Data necessary to identify applicant such as name, date of birth, Social Security number

(e) Specific lead

(f) Brief description of any derogatory information developed

(4) When a lead is set out for another office, the originating office should include pertinent data in its report so that the investigative record will clearly establish the source from which

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II,

PAGE 17 - 10

the additional information emanated.

EFFECTIVE: 01/25/88

||17-3.8| Receipt of Additional Information in Closed Cases

Individuals investigated under this program will probably be serving as Government employees for some time after the investigation is complete. In some instances involving presidential appointments, delays may occur between the time an investigation is conducted and the time in which the nomination and confirmation processes are complete. In either event, it is essential that FBIHQ be informed of any information which is developed by an office after that office has closed its investigation. When such information is received, the following steps should be taken:

(1) Recheck office indices concerning applicant for any additional information not previously reported.

(2) Furnish information to FBIHQ without delay in letterhead memorandum or supplemental report. If case warrants, such as a presidential appointment, use teletype.

(3) If it appears additional investigation will be involved in order to resolve allegation, advise FBIHQ by appropriate means (telephone or teletype) prior to initiating additional investigation and be guided by instructions from FBIHQ.

(4) If there is an indication the individual is no longer employed by the Government, take steps, including setting lead to another office, to verify this fact immediately at the inception of the investigation.

EFFECTIVE: 08/12/86

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 17 - 11

||17-3.9| Discontinuance of Investigation

(1) If information is received indicating applicant is no longer interested in Government employment, promptly notify FBIHQ and interested offices to hold investigation in abeyance. FBIHQ will contact the requesting agency to confirm this information and will advise the field regarding discontinuance. If instructed to discontinue, submit an RUC report to FBIHQ containing the results of investigation conducted to date.

(2) If significant derogatory information is received, promptly notify FBIHQ. Do not hold investigation in abeyance unless advised to do so by FBIHQ. In most instances, a client agency needs to have all results of investigation, both favorable and unfavorable, before it reaches an employment determination.

EFFECTIVE: 08/12/86

17-4 OBJECTIVES OF INVESTIGATION

The objective of these investigations is to conduct a thorough penetrating inquiry which will be useful in an assessment of an individual's suitability for Federal employment and/or for access to sensitive information. The principal areas which are addressed in accomplishing this objective are the following:

(1) Character - actions and statement which reveal a person's general attitude and possession of characteristics such as trustworthiness, reliability, and discretion or lack thereof.

(2) Associates - type of persons, businesses, groups, organizations or movements with which a person has been associated, with particular concern as to whether any of these associations have been of a disreputable or disloyal nature.

(3) Reputation - comments concerning the individual's general standing in the community.

(4) Loyalty - actions and statements revealing the person's attitude and allegiance toward the United States and its constituted form of government or indicating sympathies with any foreign government or ideology.

(5) Qualifications and ability - comments concerning an

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 17 - 12

individual's capacity or competence (native or acquired) to perform well in an occupation or field of employment. Inquiry in this area is not necessary in all cases (see instructions under specific classifications) but may be requested by FBIHQ in specific instances. When necessary, inquiries should encompass performance in all employment experiences and relate the positions held and the duties and responsibilities associated with those positions.

(6) Among concerns which are encompassed by the above objectives are the principal suitability and security standards for Federal employment, as contained in the Federal Personnel Manual, which are set out below:

(a) Suitability

1. delinquency or misconduct in prior employment
2. criminal, dishonest, infamous, or notoriously disgraceful conduct
3. intentional false statement or deception or fraud in examination or appointment
4. habitual use of intoxicating beverages to excess
5. abuse of narcotics, drugs or other controlled substances
6. reasonable doubt of loyalty to the United States
7. refusal to furnish testimony required by civil service rules
8. statutory disqualification (e.g. conviction of certain offenses).

(b) Security

1. any behavior, activities, or associations which tend to show that the individual is not reliable or trustworthy
2. any deliberate misrepresentations, falsifications, or omission of material facts

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 17 - 13

3. any criminal, infamous, dishonest, immoral, or notoriously disgraceful conduct, habitual use of intoxicants to excess, drug addiction, or sexual perversion

4. any illness, including any mental condition, of a nature which in the opinion of competent medical authority may cause significant defect in the judgment or reliability of the employee, with due regard to the transient or continuing effect of the illness and the medical findings in such case

5. any facts which furnish reason to believe that the individual may be subjected to coercion, influence, or pressure which may cause the person to act contrary to the best interests of the national security

6. commission of any act of sabotage, espionage, treason, terrorism or sedition, or attempts, threat, or preparation therefor, or conspiring with, or aiding or abetting, another to commit or attempt to commit any act of sabotage, espionage, treason, terrorism or sedition

7. establishing or continuing a sympathetic association with a saboteur, spy, traitor, seditionist, anarchist, terrorist or revolutionist, or with an espionage or other secret agent or representative of a foreign nation whose interests may be inimical to the interests of the United States, or with any person who advocates the use of force or violence to overthrow the Government of the United States or the alteration of the form of government of the United States by unconstitutional means

8. advocacy of use of force or violence to overthrow the Government of the United States, or of the alteration of the form of government of the United States by unconstitutional means

9. knowing membership, with specific intent of furthering the aims of, or adherence to and active participation in, any foreign or domestic organization, association, movement, group, or combination of persons (hereinafter referred to as organizations) which unlawfully advocates or practices the commission of acts of force or violence to prevent others from exercising their rights under the Constitution or laws of the United States or any State or subdivision thereof by unlawful means

10. intentional, unauthorized disclosure to any person of security information, or of other information, disclosure of

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 17 - 14

which is prohibited by law, or willful violation or disregard of security regulations

11. performing or attempting to perform duties, or otherwise acting, so as to serve the interests of another government in preference to the interests of the United States

12. refusal by the individual, upon the ground of constitutional privilege against self-incrimination, to testify before a congressional committee regarding charges of alleged disloyalty or other misconduct

EFFECTIVE: 08/12/86

17-5 GENERAL INSTRUCTIONS (See MIOG, Part I, 73-7, 77-1 and 77-2.)

Results are provided to other government agencies for examination and adjudication. Depending on the client being served, reports prepared in the field or memoranda summarizing investigative results prepared at FBIHQ are forwarded. If derogatory information is developed, that information is provided in its entirety along with summary memoranda sent to the White House. In situations where a presidential appointment requires Senate confirmation, reports or summary memoranda are made available for review by appropriate Senators and, in connection with matters handled for the Department of Justice, a limited number of staff personnel of the Senate Committee on the Judiciary.

(1) Investigation must be painstakingly exact, fair and unbiased.

(2) Interviews must be well planned, thorough and exhaustive and should include logical persons who are in a position to comment professionally about the applicant, such as business competitors, clients, and professional associates, and those who are in a position to furnish information as to their conduct during social and leisure activities, such as roommates and others with whom the applicant socializes on a regular basis.

(3) Purpose of interviews is to obtain information, not to dispense information. Care should be exercised to avoid any possibility of accusations of character assassination or rumor spreading.

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 17 - 15

(4) Do not convey impression person being investigated is under suspicion or that the investigation is of a criminal or subversive nature.

(5) Advise persons interviewed that investigation is of a personnel-type background inquiry and is being conducted because the individual is under consideration for government employment, for employment by a public international organization, or for access to classified or otherwise sensitive information in which the government has an interest.

(6) The general concerns (for example, trustworthiness, reliability, discretion, good conduct, and loyalty) addressed by the suitability and security standards cited in Section 17-4(6) should be covered during all interviews. If unfavorable comments are provided, obtain specific details including whether the information is based on direct knowledge or hearsay (see also Section 17-5.1). When indications of misconduct are received, the person being interviewed should be requested to provide sufficient details to permit an evaluation of the applicant's suitability for employment or access to sensitive information. Among factors which should be addressed are the nature and seriousness of the conduct, whether the conduct has been of a recurring nature, whether there has been any attempt at rehabilitation, and what the time frame of the conduct was (i.e., recent or in the past). Where unfavorable information is developed concerning a relative or associate, the degree of actual or potential influence such persons may exercise on the applicant should be determined. This would include some indications of the frequency and nature of contacts the applicant has with that individual.

(7) Each person interviewed who is knowledgeable of the applicant will be asked if the applicant has ever been known to abuse alcohol or prescription drugs or to use, possess, purchase, sell, or distribute illegal drugs, including marijuana. Obtain specific details regarding any such activity. Record results of ALL responses to questions concerning alcohol abuse, prescription drug abuse and illegal drug use in the details of the report.

(8) Each person interviewed who is knowledgeable of the applicant will be asked questions which will elicit information as to whether or not the applicant or candidate has a lifestyle or spending habits consistent with his or her means. The purpose of these questions is to determine if the candidate is financially responsible. The general nature of the questions asked and the responses provided by the interviewee must be recorded in report of interview.

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 17 - 16

Inconsistencies in spending versus means should be fully explored during the investigation and may require interview of the candidate and review of his or her financial records, if appropriate and with FBIHQ approval (see also Part II, Section 17-5.8 of this manual).

(9) Each person interviewed who is knowledgeable of the applicant will be asked if they are aware of anything in the applicant's background that could be used to influence, pressure, coerce, or compromise him/her in any way, or that could have an adverse impact on his/her character, judgment, stability, discretion, trustworthiness, or responsibility. The resulting FD-302/insert of all persons interviewed must also be sufficiently detailed to indicate this question was asked, clearly answered, and any identified activity or conduct was thoroughly addressed.

(10) Investigative personnel should be alert for any information disclosed during interviews of persons knowledgeable of the applicant or candidate which would indicate the candidate had applied for and was denied employment not indicated by the candidate during his or her initial interview or when required in response to questions on personnel security questionnaires.

(11) In connection with many federal positions, particularly those which can have an influence on policy and personnel decisions, the existence of bias or prejudice against any class of citizens or any religious, racial, or ethnic group, particularly the extent to which it manifests itself (for example, the degree to which judgment would be affected), is of interest and concern to employing agencies. FBIHQ will identify in opening communications those investigations wherein comments concerning possible bias or prejudice are needed. When this is done, ensure the results of interviews clearly indicate such inquiries were made. If an allegation of bias or prejudice is received concerning an individual not identified by FBIHQ as requiring this type of inquiry, conduct appropriate investigation to obtain comments to resolve the issue.

(12) Do not disclose identity of requesting agency or position involved when so instructed by FBIHQ.

(13) These investigations should not be regarded as routine. Each inquiry must receive careful analysis and diligent attention so that all pertinent and relevant information, either favorable or unfavorable, can be obtained.

(14) Details of reports should contain results of all investigative activity including, where necessary, an indication of

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 17 - 17

why certain investigative steps could not be accomplished or what steps with negative results were undertaken. Reports setting forth investigative results should be well organized and carefully prepared and proofread since the results are intended for dissemination to other agencies. Information in the report should generally follow the order of items as they are presented under 17-6. Where an intensive investigation has been conducted and a lengthy report is prepared, provide a table of contents. The synopsis of the report should succinctly present a summary of the detailed investigation and significant facts, particularly of a derogatory nature, should be clearly presented. Do not include comments such as "one individual would not recommend" or "arrest record set forth" without including some indication of the facts associated with those comments.

(15) Interviews should be conducted in person. Telephonic interviews are not permissible unless absolutely reasonable and necessary. The determination that a telephonic interview is appropriate under the circumstances should only be made by the SAC (see also Part II, Section 7-2.2 of this manual).

(16) Professional titles of persons interviewed must be accurate and complete; e.g., Major General John J. Jones, United States Army, Retired, should be set out rather than merely, General John J. Jones, United States Army.

(17) When reporting the results of a BI interview, it is very important to always obtain and include as much generic information about the interviewee as possible. (See also 17-5.4.) For example, the following information should always be obtained and reported:

The interviewee's relative length or period of association with the candidate, i.e., how long and/or when the interviewee has known (knew) the candidate.

The nature of the interviewee's association with the candidate, e.g., professional, personal, social.

The basis for the interviewee's knowing the information provided about the candidate, i.e., personal knowledge, hearsay, opinion.

To illustrate, the following example is being set forth:

John Allan Doe, President, ABC Bank, 1234 Main Street, Bigger City, Texas, telephone 404-596-4356; residence, 10001 Cowboy Road, Dallas, Texas, telephone 404-598-9854, advised that he was the candidate's

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 17 - 18

immediate superior at the ABC Bank for the last five years candidate was employed at ABC before the candidate resigned in 1990, and had known the candidate professionally for the twenty years prior to 1990. Doe has not seen or heard from the candidate since his 1990 retirement. Doe advised approximately three years ago, in 1993, he heard from ABC Vice-President of Consumer Financing, William Johnson, that candidate....

EFFECTIVE: 11/18/96

17-5.1 Derogatory Information

(1) Offices developing derogatory information must ensure that sufficient investigation is conducted in an attempt to verify or disprove the allegation. Expeditiously advise FBIHQ by telephone or teletype, as well as other offices which should be cognizant of the derogatory information in order that they may adequately conduct their part of the investigation. In 73, 77, 116, 140 and 161 matters, derogatory information is to be immediately telephonically conveyed to FBIHQ, to be followed within one work day by the facsimiling of interview(s) or insert(s) containing unfavorable information to FBIHQ. Teletypes are only to be sent in 73, 77, 116, 140 and 161 matters if other offices should be cognizant of the derogatory information in order to conduct adequately their part of the investigation.

(2) Whenever a person furnishes derogatory information, comments or conclusions, that person should be requested to provide specific facts, details or examples to support the statements being made. The report should clearly indicate whether or not the information is based on firsthand knowledge.

(3) Original sources of derogatory information should be identified and interviewed. It is not sufficient merely to receive such information indirectly or secondhand without an effort being made to determine its source and to resolve the matter fully. If for some reason it is not possible to interview original source, report should clearly show reason.

(4) If a question of identity is involved, report fully the information developed; initiate necessary investigation to resolve question of identity; and set out leads to interview original sources.

(5) In view of the possibility that information gathered

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 17 - 19

as a result of FBI investigation could become testimony at an administrative or judicial proceeding, set forth results on FD-302 as follows:

"JOHN Z. QUICK, Date of Birth (DOB) 1/1/44, 112 March Street, Seattle, Washington 90020, telephone (home) (206) 555-1234, (office) (206) 555-6789, was advised of the identity of the interviewing Agent as well as the fact that he was being contacted in connection with the background investigation of Ms. MARY DOE. Mr. QUICK provided the following information:"

(6) In the event that additional investigative information is to be submitted as an Insert to a report, the following format is to be used:

1

SE (file number)
ABC:def (Dictator's/typist's initials)

Seattle Division
At Seattle, Washington

Special Agent TOM PLAYFAIR conducted the following investigation on Monday, January 2, 1989:

JOHN Z. QUICK, Date of Birth (DOB) 1/1/44, 112 March Street, Seattle, Washington 90020, telephone (home) (206) 555-1234, (office) (206) 555-6789, was advised of the identity of the interviewing Agent as well as the fact that he was being contacted in connection with the background investigation of Ms. MARY DOE. Mr. QUICK provided the following information:

EFFECTIVE: 07/23/90

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 17 - 20

17-5.2 Data Obtained From File Searches

Information obtained from reviews of files on applicant, close relatives, references and associates should be used as lead material during the investigation. Pertinent information should also be organized for inclusion in the details of the report. Pertinent admissions, denials or explanation of associations with individuals or groups should be reported. Keep in mind this material will be disseminated to other Government agencies and, in some instances, to committees of the United States Senate. Any considerations affecting dissemination, such as material subject to Rule 6(e), opinion of the United States Attorney regarding release of information in pending investigations, protection of sensitive sources, and any restrictions on use of information regarding third parties, should be carefully examined. If necessary, consult with FBIHQ concerning the manner in which the information can be presented.

(1) Information on applicant - Office discovering derogatory information in its files on applicant should organize and report it unless data is contained in case in which another office is origin and that division has received copy of FBIHQ communication initiating investigation. In latter event, only office of origin in previous case should report data.

(2) Information on reference or other person to be interviewed - Office conducting interview has primary responsibility to report derogatory information. If this office has incomplete information but another office, such as office of origin, has complete information, office conducting interview must ensure that office having complete data reports it fully.

(3) If the only investigation required by an office is a file review, FBIHQ should be advised even if no record is located in office indices.

EFFECTIVE: 03/23/89

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 17 - 21

17-5.3 Association With Individuals or Groups

(1) While the First Amendment protects an individual's right of association, there are areas which are of legitimate interest to the Government in connection with employment consideration. In this category would be associations with individuals or groups which would deny other persons their rights under the Constitution, which advocate overthrow of legally constituted authority through violent means, or which engage in crimes against persons or property.

(2) Check names of such individuals or groups through office indices.

(3) Conduct inquiries to verify or disprove the alleged affiliation and provide characterizations of individual or group involved. Ascertain knowledge of or agreement with policies of group as well as dates of affiliation and extent of participation as member or officer. Contact logical informants familiar with group or allegations involved.

(4) If an individual is involved, ascertain the degree of association which exists and the extent to which applicant is aware of that individual's activities. The extent of influence which this person can exercise over the applicant should also be determined.

EFFECTIVE: 08/12/86

17-5.4 Freedom of Information Act/Privacy Act of 1974 (See Part I, 190-5(3), 190-7.3.)

(1) Pursuant to provisions of the Privacy Act of 1974 (Privacy Act), all persons interviewed during background investigations (BIs) must be advised by the interviewing employee of the purpose for which the information is sought (a background investigation), the uses to be made of the information (to determine a person's suitability for federal employment or access to national security information), the provisions which allow a BI candidate access to our records (i.e., the BI results, including an interviewee's comments), and the interviewee's right to request confidentiality.

(2) The Privacy Act permits a United States citizen or permanent resident alien to access records pertaining to him or her maintained in a system of records by an agency of the Executive Branch

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 17 - 22

of the federal government. Such an access request is processed under the provisions of the Freedom of Information Act and the Privacy Act (FOIPA).

The Privacy Act also permits the FBI to protect the identities of individuals interviewed during BIs who expressly request that their identity be held in confidence.

(3) When an individual has requested and been granted an express promise of confidentiality, it is absolutely imperative that this fact be clearly recorded along with the results of the interview.

Information collected by the FBI in these BIs will be disseminated to other government agencies and can also be made available to Senate committees when confirmation is involved. Therefore, when an individual interviewed during the course of a BI requests confidentiality under the Privacy Act, the level of confidentiality must be clearly set forth in the document recording the results of the interview (i.e., insert, FD-302). The three levels of confidentiality, an explanation of each, and the proper method to record them when reporting the results of interviews are set forth below:

(a) When interviewees request that their identities be protected from the candidate only, the following language is to be used:

"(Name, address, etc., of interviewee), who requested that (his/her) identity be protected only from the candidate, (name of candidate),...."

Under this level of confidentiality, the interviewee's identity could be included in documents provided to those agencies and/or certain members of congressional committees which have a need to access the candidate's BI. However, pursuant to an FOIPA request, the interviewee's identity and any information provided which could tend to identify the interviewee would be withheld from the requesting party.

(b) When interviewees request that their identities be protected outside the FBI (total anonymity is desired), the following language is to be used:

"(T-symbol, i.e., WMFO T-1), who requested that (T-symbol's, i.e., WMFO T-1's) identity be protected from anyone outside the FBI,...."

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 17 - 23

1. Under this level of confidentiality, the interviewee's identity would not be included in documents provided to those agencies and/or certain members of congressional committees having a need to access the candidate's BI. Here also, pursuant to an FOIPA request, the interviewee's identity and any information provided which could tend to identify the interviewee would be withheld from the requesting party.

2. When reporting the results of a BI interview of a person who has requested total confidentiality, it is important to include sufficient information intended to establish the credibility of the information provided and of the person providing the information. This information assists the client entity in assessing the reliability of the interviewee and/or how much weight to attach to the information provided by the interviewee.

FBIHQ recognizes that it is sometimes difficult to include specific information with regard to the interviewee due to issues involving confidentiality; therefore, it is very important to always obtain and include as much generic information about the interviewee as possible. (See also 17-5(17).) For example, the following information should always be obtained and reported:

The interviewee's relative length or period of association with the candidate, i.e., how long and/or when the interviewee has known (knew) the candidate.

The nature of the interviewee's association with the candidate, e.g., professional, personal, social.

The basis for the interviewee knowing the information provided about the candidate, i.e., personal knowledge, hearsay, opinion.

To illustrate, the following example is being set forth:

WMFO T-1 (hereinafter referred to as "T-1"), who requested that T-1's identity be protected from anyone outside the FBI, advised that T-1 has known the candidate well professionally for approximately the last twenty years, and socially the last ten years. T-1 advised that T-1 is aware that the candidate used cocaine and marijuana on a frequent basis over a five-year period between 1980 and 1985 because the candidate has discussed his drug use with T-1 and others in group settings on several occasions....

(c) When interviewees request that their identities

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 17 - 24

be protected until such time as required in a judicial proceeding or administrative hearing, the following language is to be used:

"(Name, address, etc., of interviewee), who requested that (his/her) identity be protected from the candidate until such time as it is required in a judicial proceeding or administrative hearing,...."

1. If interviewees request this level of confidentiality, it is recommended that they be asked if they would like to be advised prior to their identity being disclosed in such proceedings or hearings. If so, this is also to be set forth in the document recording the interview results.

2. Under this level of confidentiality, the interviewee's identity could be included in documents provided to those agencies and/or certain members of congressional committees having a need to access the candidate's background investigation. It would not be unnecessarily revealed in a judicial proceeding or administrative hearing to the candidate, until such time as it is required. Pursuant to an FOIPA request, the interviewee's identity and any information which could tend to identify the interviewee would be withheld from the requesting party unless it had been previously released to the requesting party in a judicial proceeding, administrative hearing, or was otherwise officially acknowledged.

(4) In addition to reporting the level of confidentiality requested by a BI interviewee, one of the following statements must appear in all background investigation communications reporting the results of interviews under the heading "Administrative":

(a) Use the following paragraph when one or more interviewees have been granted confidentiality: "All persons interviewed were furnished the appropriate provisions of the Privacy Act. Express promises of confidentiality, both limited and unlimited, have been granted to the following individuals:...."

(b) Use the following paragraph when no interviewees have been granted confidentiality: "All persons interviewed were furnished the appropriate provisions of the Privacy Act. Express promises of confidentiality have not been granted."

(5) Promises of confidentiality are not to be encouraged, but granted when it is the only means to secure information from the individual being interviewed. At what point in the interview process the person interviewed should be told of the Privacy Act and given the

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 17 - 25

opportunity to request confidentiality is left to the best judgment of the interviewing employee. However, the logical time is at the beginning of the interview to avoid the appearance of intentionally misleading or misinforming the person being interviewed.

EFFECTIVE: 06/03/96

17-5.5 Terminology

Stereotypical language should be avoided (e.g., "100 percent American," "liberal," "conservative"). When a general attribute is being attached to an individual (e.g., "abrasive"), provide specifics or details as to how the person relates that term to the applicant. Refrain from giving a negative cast to interviews by using statements, such as "unable to furnish any derogatory information," but instead report what information the interviewee is able to provide.

EFFECTIVE: 04/18/88

17-5.6 Interview of Applicant (See MIOG, Part I, 77-5 and Part II, 17-3.2.)

(1) Applicant must be interviewed at the inception of the investigation. The applicant must be advised that the purpose of the interview is to ensure that complete (current and accurate) information is available concerning the applicant. The interview is not to be confined to biographical data, but also is to be directed at developing any information known to the applicant that could have a bearing on the person's suitability for federal employment and/or eligibility for a security clearance or access to sensitive information. The results of the interview must be reported on an FD-302. Results must be incorporated into details of report and any necessary leads set forth for FBIHQ and appropriate offices. The narrative of the FD-302 must be sufficiently detailed to reflect that the applicant was advised of the interview's purpose and that each of the following points was completely and thoroughly addressed in the interview:

(a) Completeness and accuracy of the SF-86. The majority of the interview should not be spent reviewing the SF-86. In

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 17 - 26

most cases, it has been reviewed by FBIHQ personnel for completeness.

(b) Personal and business credit issues, including, but not limited to, repossessions, delinquent student loans, debts placed for collection and bankruptcy. (See Part II, 17-5.8.)

(c) Unpaid tax obligations. To the best of his/her knowledge, is the applicant current on all federal, state and local tax obligations. Has he/she ever made back payment of any such tax? This includes, but is not limited to, income taxes, medicare taxes, social security taxes, and unemployment taxes. If tax delinquencies or back payments are identified, determine type and amount (original and current) of tax owed/paid, tax year(s) covered, efforts and/or problems in paying the tax. Do not conduct any further investigation concerning federal tax delinquencies or back payments--FBIHQ will provide the information directly to the client agency which will consult directly with the IRS if necessary. For state and local tax delinquencies or back payments, immediately notify FBIHQ. If instructed to do so by FBIHQ, set forth appropriate leads to field offices to verify the information provided by the applicant.

(d) Civil suits as plaintiff or defendant, including divorces. Identify issues litigated.

(e) Any involvement in criminal matters as suspect or subject or any criminal charge, arrest and/or conviction.

(f) Any denials of employment and/or dismissals, particularly in the Federal sector. Include reasons.

(g) Any contact with representatives of foreign countries.

(h) Details of professional complaints or any nonjudicial disciplinary action, e.g., bar association grievances, better business complaints, student or military disciplinary proceedings, Equal Employment Opportunity complaints, etc.

(i) Business/investment circumstances that could or have involved conflict of interest allegations.

(j) Details of any psychological counseling with psychiatrists, psychologists, other qualified counselors or others.

(k) Any prescription drug or alcohol abuse, illegal drug use, to include marijuana and participation in drug/alcohol

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 17 - 27

counseling/rehabilitation programs, during applicant's entire adult life (since age 18). Identify all drugs used, when used, duration of usage, amount of drug used, place where drug was used (public or private setting), how the drug was obtained, whether or not applicant has provided drugs to anyone, if applicant has purchased or sold drugs, others having knowledge of applicant's drug use.

(1) Memberships in organizations whose policies restrict membership on the basis of sex, race, color, religion or national origin. Determine if, in fact, the membership of the organization includes minorities (Presidential appointees, U.S. Bankruptcy, Special Tribunal and U.S. Magistrate Judges only). If it is determined that a candidate has been a member of such an organization within the most recent five-year period, determine the candidate's role, for example, as a policy-making officer, in such an organization; determine if any steps have been taken by the candidate to alter official or covert restrictive admissions policies; and ascertain the candidate's personal viewpoint toward such policies. Any organizations that are determined to have potentially restrictive/discriminatory admissions policies shall be checked in field offices' indices for pertinent references.

(m) Any involvement in any organization which advocates the use of force to overthrow the U.S. Government, or any involvement in the commission of sabotage, espionage or assistance of others in terrorism.

(n) Concealment of any activity or conduct that could be used to influence, pressure, coerce, or compromise the applicant in any way, or that could have an adverse impact on his/her character, judgment, stability, discretion, trustworthiness, or responsibility.

(2) The report of interview need not reflect the specific questions asked of the applicant. A question and answer format is not desired as it tends to result in a "checklist" style of interview and failure to fully develop all information the applicant may possess regarding a specific area of inquiry.

(3) The FBI accepts investigative requests from other agencies with the understanding the referral agency has notified the applicant of the Privacy Act requirements described in Part I, 190-5(2) and (3) of this manual. This notification would cover an interview of the applicant by the FBI if confirmation is received from the applicant that the advice was furnished. The applicant can also be informed that the interview is being conducted as a result of a

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 17 - 28

request from the referral agency for the FBI to conduct a background investigation; that the purpose is to ensure the FBI has all the necessary information to conduct its investigation, the results of which will be disseminated by the FBI to the requesting agency as well as for other purposes consistent with the FBI's responsibilities; and that failure to provide the requested information could hinder the FBI's investigative efforts and cause delay in forwarding the completed results to the requesting agency for its use in making an employment or appointment determination.

(4) This interview is intended to obtain information to facilitate our investigative efforts. If an applicant provides information which could become a suitability or access issue, this should be fully explored with the applicant at the time of the interview. However, an applicant should not be contacted to resolve suitability or access issues which are developed during the investigation since resolution of such matters is primarily an adjudicative responsibility of the agency which requested the investigation. The FBI will conduct an interview to address such matters only when specifically requested or authorized by the employing agency.

EFFECTIVE: 05/27/94

17-5.7 Possible Testimony at Hearings

The possibility exists that an individual who furnishes derogatory information could be sought for testimony at a hearing if employment is being denied based on that information. Therefore, attempt to obtain a signed statement whenever such information is developed and obtain a statement concerning that person's availability to testify at a hearing.

EFFECTIVE: 01/18/91

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 17 - 29

17-5.8 Review of Financial Records

FBIHQ will accept an applicant's or candidate's financial data when provided by the agency requesting the investigation. When such data is provided, it will be reviewed at FBIHQ for any obvious leads and then forwarded to the field. Investigative personnel should compare the provided data with the results of credit checks and responses of financial questions asked of interviewees knowledgeable of the applicant or candidate. The candidate will not be specifically asked by the FBI to provide financial data unless it is necessary to resolve an issue. FBIHQ approval must be obtained before requesting such data from a candidate.

EFFECTIVE: 08/28/91

17-5.9 Status Inquiries

Occasionally, representatives of the FBI receive inquiries from Executive Branch agencies, Congressional committees or the applicants themselves requesting the status of a particular background investigation or to request that the matter be expedited. Some client agencies have requested that these inquiries be referred to them. The FBI must ensure that the desires of the client agency are followed in investigations being conducted at their request. Therefore, any requests received regarding the status of a background investigation should be referred to FBIHQ prior to a response to ensure that FBIHQ is in a position to promptly notify the client.

EFFECTIVE: 08/28/91

17-6 SCOPE OF FULL FIELD INVESTIGATIONS

(See MIOG, Part I, 73-8.4(1)(a), 77-3, 77-4.5, 77-4.7, 77-4.8, 77-4.9, 77-4.11, 77-6, 116-7, 260-2.5(2), 260-4.1(1)(b) and 260-4.2 (3)(a), Part II, 17-5(14).)

The scope of investigation may vary depending upon the position involved and whether or not there has been a previous background investigation concerning the individual. Some investigations are limited to the past 10 years of the applicant's life, exclusive of records checks. While the general scope of investigation is set forth hereinafter, the investigation should not be limited solely to the steps described herein. A thorough

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 17 - 30

examination of the applicant's personal history should be made along with consideration of the position involved. Investigative ingenuity should be exercised in an attempt to identify other leads which could reasonably be expected to produce relevant information concerning the applicant. The office should determine what resources available to it in the form of liaison contacts, informants, or assets which would be in a position to have knowledge of or provide comments concerning the applicant. For example, if the applicant is a bank official, contact should be made with the squad handling banking violations to identify any logical contacts which could be made to obtain comments about the applicant. In some instances, depending on the position involved and/or the applicant's background, specific guidance concerning contacts with informants or assets may be issued by FBIHQ. Variances in the scope of the investigation will be noted in the instructions set forth in the opening communication. It should be further noted that when issues of a pertinent or derogatory nature develop, investigation should be conducted to bring these issues to a logical conclusion, irrespective of the scope of the investigation.

EFFECTIVE: 05/27/94

17-6.1 Birth

[Verify applicant's date and place of birth at a bureau of vital statistics in all background investigations conducted for other Government agencies.]

EFFECTIVE: 08/28/91

17-6.2 Naturalization

(1) If applicant and/or spouse obtained citizenship through naturalization or derived citizenship through naturalization of parents, verify this through records of the Immigration and Naturalization Service (INS) or from court records. In view of time constraints, court records may prove to be more accessible for prompt review. In 116 matters in which Sensitive Compartmented Information access is required (which information will be provided to the field by FBIHQ) and in all 77 and 161 matters, the naturalization of close family members (parents, siblings, children and spouse) and current cohabitant(s) (residents of same household, living in spousal-type, or

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 17 - 31

roommate-type, relationships, but not domestic/other employees) also must be verified.

(2) If applicant and/or spouse are foreign nationals, verify immigration status through INS, usually at the INS District Office covering the current residence. In 116 matters in which Sensitive Compartmented Information access is required (which information will be provided by the field to FBIHQ) and in all 77 and 161 matters, the alien status of close family members (parents, siblings, children and spouse) and current cohabitant(s) (residents of same household, living in spousal-type, or roommate-type, relationships, but not domestic/other employees) also must be verified.

EFFECTIVE: 08/28/91

17-6.3 Education

(1) All college attendance and degrees obtained falling within the scope of the investigation should be verified. If applicant has not obtained a college degree during the period of time covered by the investigation, the highest college degree obtained must be verified, regardless of the time frame involved. Although detailed records of study need not be reported, dates of attendance and available class standing or grade point average (include scale used) are to be set forth. Also report information concerning academic honors or probation. Make inquiry as to the location of disciplinary records and review those records for any information concerning appointee. If school does not maintain any of the above information or has a policy against releasing such data, include an appropriate statement in the report.

(2) If education has occurred during recent years (last 3 years), professors, teachers, advisers or fellow students should be interviewed.

(3) If records or professors, etc., are not available, a clear statement should be set forth from a responsible official at the institution explaining the situation.

(4) When no college degree is indicated, high school graduation must be verified. Even if graduation from high school occurred prior to the period of time covered by the investigation, that information still must be confirmed. It will not

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 17 - 32

be sufficient to merely check attendance at business, commercial, or college institutions wherein no college degree has been obtained without also verifying high school graduation, unless it is clearly documented in those academic records that the applicant graduated from high school.

EFFECTIVE: 01/18/91

17-6.4 Marital Status

(1) Except in background investigations conducted for the Office of the Pardon Attorney, all divorces must be verified regardless of the scope of the investigation. For verification of divorces in investigations conducted for the Office of the Pardon Attorney, refer to MIOG, Part I, 73-8.4 (2)(g).

Divorce(s) should be verified through a review of appropriate records (e.g., court records). Identify which party was the plaintiff and the defendant as well as the grounds for, and date of, the divorce. All other pertinent information must be obtained, e.g., if the applicant has complied/is complying with all court-ordered obligations on a timely basis (e.g., child or spousal support or evidence of any violence, abuse or instability on the part of the applicant). If this information is not available through a review of appropriate records, efforts must be made to obtain it through an interview of applicant's attorney of record in the divorce proceeding or the attorney's representative. If this is unsuccessful, efforts must be made to obtain this information through the applicant's ex-spouse(s). If the aforementioned efforts fail, recontact the applicant in an effort to obtain/verify the necessary information.

(2) The results of each divorce verification, as reported, must clearly indicate whether or not the court imposed any financial obligations on the applicant. If so, identify each and address whether or not the applicant has complied/is complying with the obligations pursuant to the court's order in a timely manner. If no obligations were/have been imposed, so state.

(3) Except in background investigations conducted for the Office of the Pardon Attorney, all ex-spouses from divorces occurring within the scope of the investigation are to be interviewed. For interviews of ex-spouses in investigations conducted for the Office of the Pardon Attorney, refer to MIOG, Part I, 73-8.4 (2)(g). If the divorce occurred prior to the scope of the investigation, the

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 17 - 33

| ex-spouse does not have to be interviewed unless requested by FBIHQ or as otherwise deemed appropriate. |

(4) Current or separated spouse may be interviewed if considered necessary to resolve issues developed during investigation.

| (5) If any question about the applicant's current or previous marital status develops, attempt to verify through appropriate records. If not available, efforts are to be made to verify through other appropriate sources.

| (6) All unsuccessful efforts to obtain marital status or divorce information and/or resolve issues must be clearly reported. |

EFFECTIVE: 11/18/96

17-6.5 Employment

(1) All employments falling within the scope of the investigation should be verified. If not possible to verify appropriate employments, the reason for this should be included in the report. Any available files should be reviewed, specific dates of employment recorded, and the reason for termination determined.

(2) Supervisors, co-workers or other appropriate personnel should be interviewed. | Interviews of military personnel's supervisors, co-workers, etc., are limited to two years prior to the date of their last military service, if their military service was within five years prior to the date of their application. (See MIOG, Part I, 67-7.8(9) & (19) and Part II, 17-6.6.) | These should be in addition to any who may be listed as references or associates. Supervisors listed on the background data form should be interviewed. If not available, include a statement to that effect from a responsible individual.

(3) If applicant is or has been self-employed, interview clients, partners, employees and/or neighboring or competing business persons/professionals to verify self-employment and to ascertain applicant's reputation in the business/professional community. These interviews should address the security and suitability standards of Section 17-4. If business is incorporated, check the state Secretary of State's records, where doing business, for any grievances and review the articles of incorporation. If the business is a

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 17 - 34

partnership (excluding those professions regulated by licensing agencies), check the records of the County Clerk's Office (or the equivalent) for any grievances.

(4) If the employment record has been destroyed, or only limited data is available, report comment from appropriate person that this is the situation. Also determine whether applicant is known personally to that person or whether that person is able to provide the identity and/or location of others who might have known applicant.

(5) Periods of unemployment should be accounted for, and interviews of references, associates, neighbors, etc., may be useful in providing this knowledge.

EFFECTIVE: 11/28/95

17-6.6 Military Records

(1) These should be reviewed if applicant indicates any military service. National Guard records should be checked at the state National Guard headquarters. Review should include dates of service (active and reserve), awards received, rank attained, performance evaluations, disciplinary actions, clearances granted, and type of discharge received.

(2) If military records have been destroyed, verify service through other means such as Department of Veterans Affairs claims or physical observation of any military records in possession of applicant.

(3) If applicant is on active duty, or has been recently discharged, conduct interviews of supervisor and co-workers at current and/or recent assignments in the United States. Interviews are limited to supervisors and co-workers applicants have had within the two years prior to the date of their last military service, if their military service was within five years prior to the date of their application. (See MIOG, Part I, 67-7.8(9) & (19) & Part II, 17-6.5.) Interview commanding officer and review records at place of assignment.

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 17 - 35

EFFECTIVE: 11/28/95

17-6.7 Neighborhoods

(1) Neighbors at places of residence during the past five years should be interviewed. If applicant is unknown personally at the location, attempt to identify the owner of the property or the rental agency and verify from records.

(2) If derogatory information is developed, inquiries should be conducted in logical neighborhoods without regard to the five-year limitation.

(3) Do not waste efforts in endeavoring to conduct inquiries in neighborhoods, other than verification of residences, where applicant resided for very brief periods, such as one month in a trailer camp, unless investigative circumstances indicate a necessity for such inquiries.

(4) Favorable neighborhood inquiries may be summarized. The summary paragraph should indicate that favorable comments were made concerning applicant's character, associates, reputation, and loyalty, should include the length of time applicant resided there, and should advise if favorable recommendations for Government employment were made. Any derogatory information should be set forth in complete detail. For each person contacted set forth identity, address and number of years applicant has been known. If applicant is unknown at the location, report identity of persons contacted who provided that information.

(5) If unable to verify residence through above investigation, attempts should be made through references, associates and other individuals in a position to have this knowledge or through education or employment records to corroborate residence at that location.

EFFECTIVE: 12/10/91

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 17 - 36

17-6.8 References and Associates

- (1) Generally, all listed references and associates should be interviewed. However, if an individual cannot be contacted without an expenditure of unreasonable time and travel or an individual will be unavailable for a period of time which would unduly delay the investigation, interviews need not be conducted provided an adequate inquiry can be completed without that interview. The details of the report should advise that the individual is unavailable and should recount what efforts were made to contact that person.
- (2) If information is available which would preclude an interview, the individual should not be contacted. Explain on the cover pages of the report the reason why an interview is not appropriate.
- (3) Whenever derogatory information exists concerning a reference or associate, an appropriate characterization of that individual should be reported and the nature and extent of applicant's association with that person should be developed.
- (4) In recording results of interviews with references and associates, include information as to the nature of the relationship (e.g., social or professional basis) and the length of time of the association.
- (5) During interviews with persons knowledgeable about applicant (such as neighbors, co-workers, supervisors, listed references and listed associates), obtain identity of associates of applicant and ensure that persons other than those identified by applicant are interviewed.
- (6) Furnish name and identifying data concerning other individuals closely associated with applicant such as roommates and fiancé(s) to FBIHQ for a check of Criminal Justice Information Services Division records.

EFFECTIVE: 05/27/94

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 17 - 37

17-6.9 Relatives (See MIOG, Part II, 17-3.4(2)(b), 17-6.11.)

(1) Close relatives normally include spouse, children, parents, brothers and sisters. Other relatives who occupy the same residence as applicant or who were closely associated with the applicant's upbringing may also be included.

(2) Local law enforcement agency checks will not normally be necessary concerning close relatives since FBIHQ will check names of close relatives through Criminal Justice Information Services/Division records. However, if, through other investigation, an office develops information concerning criminal activity on the part of a relative, notify FBIHQ and include information in details of report.

(3) The identity of close relatives is ordinarily included in background data provided by the applicant, but offices should be alert for the identity of any close relatives not listed. If an additional relative is discovered, promptly notify FBIHQ and interested offices, along with necessary identifying data. Similarly, if it is determined data provided by applicant is in error, promptly advise FBIHQ and interested offices.

(4) If derogatory information exists or is developed concerning a close relative, the nature and extent of association with the applicant should be ascertained.

EFFECTIVE: 04/08/96

17-6.10 Credit Agency Checks

(1) Credit checks will be processed by contractor credit bureau personnel at FBIHQ, and will cover all places of an applicant's residence, education, and employment during the most recent seven-year period. If the credit check discloses any repossessions or court judgment, or if an account is listed as an uncollectible debt, skip, has been placed for collection, or significantly delinquent, a separate communication will be sent to the field from FBIHQ to ascertain from the firm listing the delinquency and/or through court records if the obligation remains outstanding or if it has been resolved.

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 17 - 38

(2) Where it is necessary to access records which are covered by the Right to Financial Privacy Act of 1978 (RFPA) (generally, banks, savings and loan associations, credit unions and credit card issuers), the applicant is to be furnished with a copy of Department of Justice (DOJ) letterhead memorandum captioned, "Statement of Customer Rights under the Right to Financial Privacy Act of 1978," which must be executed by the interviewing Agent. The applicant must execute Form DOJ-462 captioned, "Customer Consent and Authorization for Access to Financial Records." Copy of executed DOJ-462 should be furnished to each office where financial records are to be reviewed. For effective use of this customer consent and authorization form, ensure applicant identifies all financial institutions anticipated to require access. The purpose should also be stated broadly on the form. In addition, Form DOJ-461 captioned, "Certificate of Compliance with the Right to Financial Privacy Act of 1978," must be executed by a "supervisory official" and transmitted along with DOJ-462 to the financial institution before financial records may be obtained. The certification of compliance requirement is an absolute prerequisite to Government access to financial records under RFPA. See Part II, 23-6, of this manual, particularly concerning method of identifying material which is incorporated in reports.

EFFECTIVE: 08/28/91

17-6.11 Law Enforcement Agency Checks

(1) In all localities of residence, education, and employment, check the applicant's name against files of local law enforcement agencies. These checks are not to be limited to police departments but are to include records of sheriffs' office, or other duly constituted authorities which cover an area (i.e., Military Police if applicant resided on a military installation), and motor vehicle administrations or equivalent agencies. Where centralization of records on an areawide or statewide basis is in effect, those records are also to be reviewed. Some law enforcement agencies departmentalize their operations, making it necessary to check records of various squads and bureaus within the agency. Check of these records must be made.

(2) If a record is located, obtain in detail all necessary data which identifies applicant with the person to whom the record pertains. Avoid drawing conclusions by identifying the record as that of "the applicant." Instead, set forth the data from the

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 17 - 39

record which will identify the record with a particular individual. Ascertain not only disposition but check existing court docket, blotter, or case file for any additional data that might be available. Should it be necessary, interview arresting officer if available.

(3) Frequently arrests are made on charges which are generic and indefinite in nature. Examples of such vague charges are disorderly conduct, loitering, etc. In such instances, it is not sufficient merely to report that applicant was arrested on such a charge, but the exact nature of applicant's activities resulting in arrest must be ascertained. A charge of disorderly conduct might encompass activities ranging from sexual deviation to loitering. The exact nature of such a charge must be ascertained for inclusion in report.

(4) During the course of the background investigation, if it is disclosed through law enforcement entities that the applicant is the subject of a current criminal investigation, the field should hold the background investigation in abeyance and immediately notify FBIHQ.

EFFECTIVE: 08/28/91

17-6.12 Tax Matters

Check for tax liens (state and local) when there is questionable financial status concerning presidential appointments, Federal Judgeships, USAs, U.S. Marshals, Deputy Attorney General, Associate Attorney General, Assistant Attorneys General, Department heads, members of U.S. Parole Commission and U.S. Courts applicants, and others as directed by FBIHQ. Furnish questionable financial standing to auxiliary offices for appropriate checks. Where a check of IRS records is required, the interested agency will make necessary requests.

EFFECTIVE: 12/10/91

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 17 - 40

17-6.13 Agency Checks (See MIOG, Part I, 161-8.)

(1) When conducting background investigations (BGI) on personnel who will conduct all Office of Personnel Management (OPM) Department of Energy and Investigations (DCI), Central Intelligence Agency (CIA), and Selective Service System (SSS) checks. OPM checks are conducted in all appointments to positions (security investigations, DCI, etc.) include security clearance information contributed by the Department of Energy and Investigations (DISCO), is checked to indicate if individual has indicated prior or current service or civilian employment with any branch of the Armed Forces or if a disqualification being granted in individual's service record (and top Secret) based on actions taken by the Department of Energy and Investigations. Candidate's employment in United States Government, foreign

SSS is checked via a telephonic computerized system which maintains SSS registration information on male candidates who were born after 12/31/59. When appropriate, leads for various agency checks are set out by FBIHQ personnel to field office (Washington Metropolitan Field in most instances).

(2) If applicant is known to have been previously processed for clearance by Atomic Energy Commission, Department of Energy, or Nuclear Regulatory Commission, security files of appropriate area office or offices of Department of Energy or Nuclear Regulatory Commission which handled clearance procedures should be checked.

(3) In presidential appointment matters, the applicant's name should be checked at the U.S. Attorney's Office covering any area of residence, employment, or education for information that the applicant has been involved in any Federal litigation. The records of the U.S. Attorney's Office will be checked against the applicant's name during other investigations where the applicant is to be employed in a sensitive position, regardless of whether or not the candidate is to receive a presidential appointment, such as in all Level I and Level II 161 investigations and certain investigations for the Administrative Office of the U.S. Courts and the Department of Justice. FBIHQ will instruct the field in the opening communication as to which nonpresidential appointment cases require checks at the U.S. Attorney's Office.

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 17 - 41

(4) In addition to these checks, the applicant's background and information developed during the investigation should be examined for any other logical agencies where records could be compiled concerning an individual. If a person is engaged in a profession, state associations or licensing agencies should be checked to verify issuance of a license or certificate and to determine if any record of complaints or investigation exists concerning the applicant. Similarly, careful analysis should be undertaken to ensure logical checks of Federal, state and local governmental agencies, as well as private sources (e.g., Better Business Bureau), for information bearing on an individual's character and fitness for employment are thoroughly exhausted. When a licensing agency is checked, the following statement must appear: "The above-named agency is the licensing agency for (type of profession) in the state (state name)."

(5) If a check with an agency cannot be completed within the deadline, advise FBIHQ of this fact and complete other aspects of the investigation. The case can then be followed on tickler or placed in a pending inactive status and the results of the check can be forwarded to FBIHQ when received. FBIHQ, when all other investigative results are received, will forward the results to the client agency with a statement that the FBI's inquiry is complete and information from the other agency will be provided when it becomes available.

(6) If pertinent information is developed from a review of records of another agency, determine the identity of the original source and interview. If agency unwilling to or unable to identify the source, indicate reason and agency's evaluation in report. If person interviewed furnishes same information, it is not necessary to report this information was previously provided to the other agency. If interviewee contradicts information attributed to that person by another agency, quote information from other agency, discuss discrepancies with interviewee, and report interviewee's explanation for discrepancies. Do not reveal to interviewee that current interview is based on the other agency's information unless absolutely necessary, such as when contradictions need to be resolved. Identity of other agency should not be made known.

EFFECTIVE: 07/19/93

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 17 - 42

||17-6.14| Civil Suits

(1) Whenever information is developed indicating applicant is or has been a party to a civil suit, ensure that all appropriate court records are examined in order to identify any civil suit involving applicant. Report succinct summary of suit.

(2) It is recognized that in some instances a person who has occupied public office may be named in a number of suits by reason of the position held. When such a circumstance is encountered, point out in summary fashion that these suits were filed against applicant in connection with his/her role as a public official. Unless indications are received such suits pertain to improprieties personally committed by applicant, no further review would be necessary.

EFFECTIVE: 01/18/91

||17-6.15| Medical Records

If background furnished or investigation indicates person under investigation has been treated for serious physical or mental problem, verify through physician or institution records, obtaining medical release when needed, except in Special Inquiry matters where no investigation should be undertaken unless so instructed by FBIHQ.

EFFECTIVE: 01/18/91

17-7 FRAUD VIOLATIONS

Possible fraud against the Government (FAG) violations are sometimes detected during applicant-type investigations. They result from falsification or concealment in questionnaire or application executed and submitted to Government by applicant in apparent belief that true recitation of facts would prejudice opportunity for employment. For additional instructions, see section of this manual concerning Fraud Against the Government.

EFFECTIVE: 01/18/91

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 17 - 43

17-7.1 Applicable Statutes

- (1) Title 5, USC, Sections 3333 and 7311
- (2) Title 18, USC, Sections 1001 and 1918

EFFECTIVE: 01/18/91

17-7.2 Investigative Procedures

- (1) Cases involving serious falsifications or misrepresentations of material facts are to be presented to the USA; however, in order that employing agency can first be apprised of fact case is to be presented, advise FBIHQ by teletype of pertinent facts, including intent to present to USA. As soon as employing agency is notified by FBIHQ, field will be advised so case can be presented to USA as early as feasible to avoid unnecessary investigation in event he/she would not authorize prosecution.
- (2) Cases involving petty or immaterial offenses, such as an arrest for drunkenness or other minor misrepresentations, are brought to FBIHQ's attention by cover page(s) accompanying investigative report and are not presented to USA.
- (3) Investigate such possible fraud violations as part of the applicant-type investigation. Do not open separate case. When fraud matter is presented to USA, add "Fraud Against the Government" to character. Set forth in report opinion of USA, and ensure venue discussed.

EFFECTIVE: 01/18/91

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 18 - 1

SECTION 18. AGREEMENTS AND COORDINATION BETWEEN FBI, MILITARY
AND OTHER AGENCIES

18-1 THE AGREEMENTS

The following agreement was approved and entered into by the Departments of Justice (DOJ) and Defense (DOD) relative to the investigation and prosecution of crimes committed by individuals subject to the Uniform Code of Military Justice:

EFFECTIVE: 07/11/85

18-2 MEMORANDUM OF UNDERSTANDING BETWEEN DOJ AND DOD

"MEMORANDUM OF UNDERSTANDING BETWEEN THE DEPARTMENTS OF JUSTICE AND DEFENSE RELATING TO THE INVESTIGATION AND PROSECUTION OF CERTAIN CRIMES

"A. PURPOSE, SCOPE AND AUTHORITY

"This Memorandum of Understanding (MOU) establishes policy for the Department of Justice and Department of Defense with regard to the investigation and prosecution of criminal matters over which the two Departments have jurisdiction. This memorandum is not intended to confer any rights, benefits, privileges, or form of due process procedure upon individuals, associations, corporations or other persons or entities.

"This Memorandum applies to all components and personnel of the Department of Justice and the Department of Defense. The statutory bases for the Department of Defense and the Department of Justice investigation and prosecution responsibilities include, but are not limited to:

"1. Department of Justice: Titles 18, 21 and 28 of the United States Code; and

"2. Department of Defense: The Uniform Code of Military Justice, Title 10, United States Code, Sections 801-940; the Inspector General Act of 1978, Title 5, United States Code, Appendix I; and Title 5, United States Code, Section 301.

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 18 - 2

"B. POLICY

"The Department of Justice has primary responsibility for enforcement of federal laws in the United States District Courts. The Department of Defense has responsibility for the integrity of its programs, operations and installations and for the discipline of the Armed Forces. Prompt administrative actions and completion of investigations within the two (2) year statute of limitations under the Uniform Code of Military Justice require the Department of Defense to assume an important role in federal criminal investigations. To encourage joint and coordinated investigative efforts, in appropriate cases where the Department of Justice assumes investigative responsibility for a matter relating to the Department of Defense, it should share information and conduct the inquiry jointly with the interested Department of Defense investigative agency.

"It is neither feasible nor desirable to establish inflexible rules regarding the responsibilities of the Department of Defense and the Department of Justice as to each matter over which they may have concurrent interest. Informal arrangements and agreements within the spirit of this MOU are permissible with respect to specific crimes or investigations.

"C. INVESTIGATIVE AND PROSECUTIVE JURISDICTION

"1. CRIMES ARISING FROM THE DEPARTMENT OF DEFENSE OPERATIONS

"a. Corruption Involving the Department of Defense
Personnel

"The Department of Defense investigative agencies will refer to the FBI on receipt all significant allegations of bribery and conflict of interest involving military or civilian personnel of the Department of Defense. In all corruption matters the subject of a referral to the FBI, the Department of Defense shall obtain the concurrence of the Department of Justice prosecutor or the FBI before initiating any independent investigation preliminary to any action under the Uniform Code of Military Justice. If the Department of Defense is not satisfied with the initial determination, the matter will be reviewed by the Criminal Division of the Department of Justice.

"The FBI will notify the referring agency promptly regarding whether they accept the referred matters for investigation. The FBI will attempt to make such decision in one (1) working day of receipt

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 18 - 3

of such matters.

"b. Frauds Against the Department of Defense and Theft and Embezzlement of Government Property

"The Department of Justice and the Department of Defense have investigative responsibility for frauds against the Department of Defense and theft and embezzlement of government property from the Department of Defense. The Department of Defense will investigate frauds against the Department of Defense and theft of government property from the Department of Defense. Whenever a Department of Defense investigative agency identifies a matter which, if developed by investigation, would warrant federal prosecution, it will confer with the United States Attorney or the Criminal Division, the Department of Justice, and the FBI field office. At the time of this initial conference, criminal investigative responsibility will be determined by the Department of Justice in consultation with the Department of Defense.

"2. CRIMES COMMITTED ON MILITARY INSTALLATIONS

"a. Subject(s) can be Tried by Court-Martial or are Unknown

"Crimes (other than those covered by paragraph C.1.) committed on a military installation will be investigated by the Department of Defense investigative agency concerned and, when committed by a person subject to the Uniform Code of Military Justice, prosecuted by the Military Department concerned. The Department of Defense will provide immediate notice to the Department of Justice of significant cases in which an individual subject/victim is other than a military member or dependent thereof.

"b. One or More Subjects cannot be Tried by Court-Martial

"When a crime (other than those covered by paragraph C.1.) has occurred on a military installation and there is reasonable basis to believe that it has been committed by a person or persons, some or all of whom are not subject to the Uniform Code of Military Justice, the Department of Defense investigative agency will provide immediate notice of the matter to the appropriate Department of Justice investigative agency unless the Department of Justice has relieved the Department of Defense of the reporting requirement for that type or class of crime.

"3. CRIMES COMMITTED OUTSIDE MILITARY INSTALLATIONS BY PERSONS WHO CAN BE TRIED BY COURT-MARTIAL

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 18 - 4

"a. Offense is Normally Tried by Court-Martial

"Crimes (other than those covered by paragraph C.1.) committed outside a military installation by persons subject to the Uniform Code of Military Justice which, normally, are tried by court-martial will be investigated and prosecuted by the Department of Defense. The Department of Defense will provide immediate notice of significant cases to the appropriate Department of Justice investigative agency. The Department of Defense will provide immediate notice in all cases where one or more subjects is not under military jurisdiction unless the Department of Justice has relieved the Department of Defense of the reporting requirement for that type or class of crime.

"b. Crimes Relating to Scheduled Military Activities

"Crimes relating to scheduled military activities outside of a military installation, such as organized maneuvers in which persons subject to the Uniform Code of Military Justice are suspects, shall be treated as if committed on a military installation for purposes of the Memorandum. The FBI or other Department of Justice investigative agency may assume jurisdiction with the concurrence of the United States Attorney or the Criminal Division, Department of Justice.

"c. Offense is not Normally Tried by Court-Martial

"When there are reasonable grounds to believe that a Federal crime (other than those covered by paragraph C.1.) normally not tried by court-martial, has been committed outside a military installation by a person subject to the Uniform Code of Military Justice, the Department of Defense investigative agency will immediately refer the case to the appropriate Department of Justice investigative agency unless the Department of Justice has relieved the Department of Defense of the reporting requirement for that type or class of crime.

"D. REFERRALS AND INVESTIGATIVE ASSISTANCE

"1. REFERRALS

"Referrals, notices, reports, requests and the general transfer of information under this Memorandum normally should be between the FBI or other Department of Justice investigative agency and the appropriate Department of Defense investigative agency at the field level.

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 18 - 5

"If a Department of Justice investigative agency does not accept a referred matter and the referring Department of Defense investigative agency then, or subsequently, believes that evidence exists supporting prosecution before civilian courts, the Department of Defense agency may present the case to the United States Attorney or the Criminal Division, Department of Justice, for review.

"2. INVESTIGATIVE ASSISTANCE

"In cases where a Department of Defense or Department of Justice investigative agency has primary responsibility and it requires limited assistance to pursue outstanding leads, the investigative agency requiring assistance will promptly advise the appropriate investigative agency in the other Department and, to the extent authorized by law and regulations, the requested assistance should be provided without assuming responsibility for the investigation.

"E. PROSECUTION OF CASES

"1. With the concurrence of the Department of Defense, the Department of Justice will designate such Department of Defense attorneys as it deems desirable to be Special Assistant United States Attorneys for use where the effective prosecution of cases may be facilitated by the Department of Defense attorneys.

"2. The Department of Justice will institute civil actions expeditiously in United States District Courts whenever appropriate to recover monies lost as a result of crimes against the Department of Defense; the Department of Defense will provide appropriate assistance to facilitate such actions.

"3. The Department of Justice prosecutors will solicit the views of the Department of Defense prior to initiating action against an individual subject to the Uniform Code of Military Justice.

"4. The Department of Justice will solicit the views of the Department of Defense with regard to its Department of Defense-related cases and investigations in order to effectively coordinate the use of civil, criminal and administrative remedies.

"F. MISCELLANEOUS MATTERS

"1. THE DEPARTMENT OF DEFENSE ADMINISTRATIVE ACTIONS

"Nothing in this Memorandum limits the Department of Defense

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 18 - 6

investigations conducted in support of administrative actions to be taken by the Department of Defense. However, the Department of Defense investigative agencies will coordinate all such investigations with the appropriate Department of Justice prosecutive agency and obtain the concurrence of the Department of Justice prosecutor or the Department of Justice investigative agency prior to conducting any administrative investigation during the pendency of the criminal investigation or prosecution.

"2. SPECIAL UNIFORM CODE OF MILITARY JUSTICE FACTORS

"In situations where an individual subject to the Uniform Code of Military Justice is a suspect in any crime for which a Department of Justice investigative agency has assumed jurisdiction, if a Department of Defense investigative agency believes that the crime involves special factors relating to the administration and discipline of the Armed Forces that would justify its investigation, the Department of Defense investigative agency will advise the appropriate Department of Justice investigative agency or the Department of Justice prosecuting authorities of these factors. Investigation of such a crime may be undertaken by the appropriate Department of Defense investigative agency with the concurrence of the Department of Justice.

"3. ORGANIZED CRIME

"The Department of Defense investigative agencies will provide to the FBI all information collected during the normal course of agency operations pertaining to the element generally known as "organized crime" including both traditional (La Cosa Nostra) and nontraditional organizations whether or not the matter is considered prosecutable. The FBI should be notified of any investigation involving any element of organized crime and may assume jurisdiction of the same.

"4. DEPARTMENT OF JUSTICE NOTIFICATION TO DEPARTMENT OF DEFENSE INVESTIGATIVE AGENCIES

"a. The Department of Justice investigative agencies will promptly notify the appropriate Department of Defense investigative agency of the initiation of the Department of Defense related investigations which are predicated on other than a Department of Defense referral except in those rare instances where notification might endanger agents or adversely affect the investigation. The Department of Justice investigative agencies will also notify the Department of Defense of all allegations of the Department of Defense

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 18 - 7

related crimes where investigation is not initiated by the Department of Justice.

"b. Upon request, the Department of Justice investigative agencies will provide timely status reports on all investigations relating to the Department of Defense unless the circumstances indicate such reporting would be inappropriate.

"c. The Department of Justice investigative agencies will promptly furnish investigative results at the conclusion of an investigation and advise as to the nature of judicial action, if any, taken or contemplated.

"d. If judicial or administrative action is being considered by the Department of Defense, the Department of Justice will, upon written request, provide existing detailed investigative data and documents (less any Federal grand jury material, disclosure of which would be prohibited by Rule 6(e), Federal Rules of Criminal Procedure), as well as agent testimony for use in judicial or administrative proceedings, consistent with Department of Justice and other Federal regulations. The ultimate use of the information shall be subject to the concurrence of the Federal prosecutor during the pendency of any related investigation or prosecution.

"5. TECHNICAL ASSISTANCE

"a. The Department of Justice will provide to the Department of Defense all technical services normally available to Federal investigative agencies.

"b. The Department of Defense will provide assistance to the Department of Justice in matters not relating to the Department of Defense as permitted by law and implementing regulations.

"6. JOINT INVESTIGATIONS

"a. To the extent authorized by law, the Department of Justice investigative agencies and the Department of Defense investigative agencies may agree to enter into joint investigative endeavors, including undercover operations, in appropriate circumstances. However, all such investigations will be subject to Department of Justice guidelines.

"b. The Department of Defense, in the conduct of any investigation that might lead to prosecution in Federal District Court, will conduct the investigation consistent with any Department

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 18 - 8

of Justice guidelines. The Department of Justice shall provide copies of all relevant guidelines and their revisions.

"7. APPREHENSION OF SUSPECTS

"To the extent authorized by law, the Department of Justice and the Department of Defense will each promptly deliver or make available to the other suspects, accused individuals and witnesses where authority to investigate the crimes involved is lodged in the other Department. This MOU neither expands nor limits the authority of either Department to perform apprehensions, searches, seizures, or custodial interrogations.

"G. EXCEPTION

"This Memorandum shall not affect the investigative authority now fixed by the 1979 'Agreement Governing the Conduct of the Defense Department Counterintelligence Activities in Conjunction with the Federal Bureau of Investigation' and the 1983 Memorandum of Understanding between the Department of Defense, the Department of Justice and the FBI concerning 'Use of Federal Military Force in Domestic Terrorist Incidents.'

"Signed:

/s/ William French Smith
Attorney General
United States Department
of Justice

/s/ Caspar W. Weinberger
Secretary of Defense
United States Department
of Defense

Date: Aug 14, 1984

Date: August 22, 1984"

EFFECTIVE: 07/11/85

18-2.1 | Deleted |

EFFECTIVE: 07/11/85

18-2.1.1 | Deleted |

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 18 - 9

EFFECTIVE: 07/11/85

| 18-2.1.2 | Deleted |

EFFECTIVE: 07/11/85

| 18-2.1.3 | Deleted |

EFFECTIVE: 07/11/85

18-3 MEMORANDUM OF UNDERSTANDING ON MILITARY DESERTERS BETWEEN
THE FEDERAL BUREAU OF INVESTIGATION (FBI) AND THE
DEPARTMENT OF DEFENSE (DOD)

The following agreement between the FBI and DOD relative
to investigations concerning military deserters was approved and
entered into:

"MEMORANDUM OF UNDERSTANDING ON MILITARY DESERTERS BETWEEN
THE FEDERAL BUREAU OF INVESTIGATION (FBI) AND THE DEPARTMENT OF
DEFENSE (DOD)"

"Desertion is a most serious offense under the Uniform Code of Military
Justice. Vigorous efforts to apprehend deserters are essential in
order to return deserters to military control and to deter others from
deserting.

"It is, therefore, agreed that:

"(1) Each Military Department will continue to enter
information on each deserter into the National Crime Information
Center Computer. This information will be kept current by the
Military Departments and remain available to law enforcement officials
at the national, state, and local levels as long as the individual is
absent.

"(2) Responses to inquiries from any law enforcement
agency resulting from any other investigation of offense will disclose
that the subject of the inquiry is wanted by a Military Department.

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 18 - 10

"(3) The FBI Identification Division will continue to assist Military Departments in identifying persons through fingerprint comparison and will provide to the Military Departments wanted flash notice services for ordinary deserter cases and for offenses shown on the Attachment. These services will be initiated automatically upon the military's entry of a deserter's record in the Wanted Persons File of the National Crime Information Center.

"(4) The FBI will conduct investigations for the purpose of apprehending deserters in those cases where aggravating circumstances exist in addition to the desertion offense. Aggravating circumstances include those matters listed on the Attachment. In such cases, the Military Department Headquarters will provide the FBI Headquarters with written notice which will specify the serious offense, in addition to desertion, of which the absentee is suspected. Such notice indicates that appropriate judicial or administrative disposition is contemplated upon return to military control. Upon receipt of such notice, the FBI will initiate an active investigation. The FBI will be informed promptly of any change in the status of a military member who is subject of an FBI investigation.

"(5) It is possible other offenses may be committed which are not within the scope of the Attachment, yet because of their circumstances, are so aggravated that investigation and return to military control is warranted. Requests for FBI assistance in these few instances will be closely monitored by the Military Department Headquarters and that Headquarters will provide the FBI Headquarters with factual detail explaining the seriousness of the offense, in order to support an FBI investigation.

"(6) The DOD will undertake its own program to deter desertion and to apprehend deserters. The Military Departments will engage in desertion prevention programs and will cooperate with all law enforcement officials in the return of deserters to military control.

"(7) The FBI will conduct investigations to apprehend military personnel convicted of one of the attached articles who subsequently escape military confinement.

| Amendment

"(8) The FBI will conduct investigations to apprehend military personnel designated deserters by their respective Military Service during any national emergency involving armed conflict which

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 18 - 11

occurs subsequent to the date this amendment is signed.

March 19, 1979
Date

/s/ William H. Webster
For the FBI
Director

May 9, 1979
Date

/s/ Robert B. Pirie, Jr.
For the DOD
Assistant Secretary of
Defense (Manpower,
Reserve Affairs &
Logistics)

"General

"Desertion of officers.

"Desertion of those who have had access to certain classified defense information which if disclosed could, in the view of the Military Department concerned, jeopardize the security interests of the United States.

"Violations of the Uniform Code of Military Justice

- "Art. 82 Soliciting or advising another to desert or to mutiny, or to commit misbehavior before the enemy. Sedition.
- " 90 Striking, drawing or lifting up any weapon or offering any violence to his superior commissioned officer in the execution of his office.
- " 91 Striking or otherwise assaulting a warrant officer or a noncommissioned officer or petty officer while in the execution of his office.
- " 92 Disclosure of classified defense information.
- " 99 Misbehavior before the enemy.
- " 100 Subordinate compelling surrender.

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 18 - 12

- " 103 Looting and pillaging.
- " 104 Aiding the enemy.
- " 106 Spying.
- "Art. 116 Riot.
- " 118 Murder.
- " 119 Manslaughter.
- " 120 Rape.
- " 122 Robbery.
- " 124 Maiming.
- " 125 Sodomy by force and without consent, or with a child under the age of 16 years.
- " 126 Arson.
- " 127 Extortion.
- " 128 Assault upon a commissioned officer not in the execution of his office.
- " 134 Assault:
 - " Indecent.
 - " With intent to commit voluntary manslaughter, robbery, sodomy, arson or burglary.
 - " With intent to commit housebreaking.
 - " With intent to commit murder or rape.
 - " Firearm, discharging:
 - " Wrongfully and willfully, under circumstances as to endanger life.
 - " Homicide, negligent.

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 18 - 13

- " Indecent acts or liberties with a child under the age of 16 years.
- " 80 Attempting to commit any of the above.
- " 81 Conspiracy to commit any of the above."

EFFECTIVE: 06/08/79

18-4 MEMORANDUM OF UNDERSTANDING BETWEEN DOJ AND COAST GUARD

The following agreement was approved and entered into between the Departments of Justice and Transportation relative to the investigation and prosecution of crimes committed by members of the U.S. Coast Guard subject to the Uniform Code of Military Justice:

"MEMORANDUM OF UNDERSTANDING BETWEEN THE DEPARTMENTS OF JUSTICE AND TRANSPORTATION (COAST GUARD) RELATING TO THE INVESTIGATION AND PROSECUTION OF CRIMES OVER WHICH THE TWO DEPARTMENTS HAVE CONCURRENT JURISDICTION

"Whereas, certain crimes committed by Coast Guard personnel subject to the Uniform Code of Military Justice may be prosecuted by Coast Guard tribunals under that Code or by civilian authorities in the Federal Courts; and

"Whereas, it is recognized that although the administration and discipline of the Coast Guard requires that certain types of crimes committed by its personnel be investigated by that service and prosecuted before Coast Guard military tribunals other types of crimes committed by such military personnel should be investigated by civil authorities and prosecuted before civil tribunals; and

"Whereas, it is recognized that it is not feasible to impose inflexible rules to determine the respective responsibility of the civilian and Coast Guard military authorities as to each crime over which they may have concurrent jurisdiction and that informal arrangements and agreements may be necessary with respect to specific crimes or investigations; and

"Whereas, agreement between the Department of Justice and the Department of Transportation (Coast Guard) as to the general areas

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 18 - 14

in which they will investigate and prosecute crimes to which both civil and military jurisdiction attach will, nevertheless, tend to make the investigation and prosecution of crimes more expeditious and efficient and give appropriate effect to the policies of civil government and the requirements of the United States Coast Guard;

"It is hereby agreed and understood between the Department of Justice and the Department of Transportation (Coast Guard) as follows:

"1. Crimes committed on military installations (including aircraft and vessels). Except as hereinafter indicated, all crimes committed on a military installation by Coast Guard personnel subject to the Uniform Code of Military Justice shall be investigated and prosecuted by the Coast Guard if the Coast Guard makes a determination that there is a reasonable likelihood that only Coast Guard personnel subject to the Uniform Code of Military Justice are involved in such crime as principals or accessories, and, except in extraordinary cases, that there is no victim other than persons who are subject to the Uniform Code of Military Justice or who are bona fide dependents or members of a household of military or civilian personnel residing on the installation. Unless such a determination is made, the Coast Guard shall promptly advise the Federal Bureau of Investigation of any crime committed on a military installation if such crime is within the investigative authority of the Federal Bureau of Investigation. The Federal Bureau of Investigation shall investigate any serious crime of which it has been so advised for the purpose of prosecution in the civil courts unless the Department of Justice determines that investigation and prosecution may be conducted more efficiently and expeditiously by the Coast Guard. Even if the determination provided for in the first sentence of this paragraph is made by the Coast Guard, it shall promptly advise the Federal Bureau of Investigation of any crime committed on a military installation in which there is a victim who is not subject to the Uniform Code of Military Justice or a bona fide dependent or member of the household of military or civilian personnel residing on the installation and that the Coast Guard is investigating the crime because it has been determined to be extraordinary. The Coast Guard shall promptly advise the Federal Bureau of Investigation whenever the crime, except in minor offenses, involves fraud against the government, misappropriation, robbery, or theft of government property or funds, or is of a similar nature. All such crimes shall be investigated by the Coast Guard unless it receives prompt advice that the Department of Justice has determined that the crime should be investigated by the Federal Bureau of Investigation and that the Federal Bureau of Investigation will undertake the investigation for the purpose of prosecution in the

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 18 - 15

civil courts.

"2. Crimes committed outside of military installations. Except as hereinafter indicated, all crimes committed outside of military installations, which fall within the investigative jurisdiction of the Federal Bureau of Investigation and in which there is involved as a suspect an individual subject to the Uniform Code of Military Justice, shall be investigated by the Federal Bureau of Investigation for the purpose of prosecution in civil courts, unless the Department of Justice determines that investigation and prosecution may be conducted more efficiently and expeditiously by other authorities. All such crimes which come first to the attention of Coast Guard authorities shall be referred promptly by them to the Federal Bureau of Investigation as to particular types or classes of crime. However, whenever Coast Guard military personnel are engaged in scheduled military activities outside of military installations such as organized maneuvers or organized movement, the provisions of paragraph 1 above shall apply, unless persons not subject to the Uniform Code of Military Justice are involved as principals, accessories or victims.

"If, however, there is involved as a suspect or as an accused in any crime committed outside of a military installation and falling within the investigative authority of the Federal Bureau of Investigation an individual who is subject to the Uniform Code of Military Justice and if the Coast Guard authorities believe that the crime involves special factors relating to the administration and discipline of the Coast Guard which would justify investigation by them for the purpose of prosecution before a Coast Guard military tribunal, they shall promptly advise the Federal Bureau of Investigation of the crime and indicate their views on the matter. Investigation of such a crime may be undertaken by the Coast Guard military authorities if the Department of Justice agrees.

"3. Transfer of investigative authority. An investigative body of the Coast Guard which has initiated an investigation pursuant to paragraphs 1 and 2 hereof shall have exclusive investigative authority and may proceed therewith to prosecution. If, however, any Coast Guard investigative body comes to the view that effectuation of those paragraphs requires the transfer of investigative authority over a crime, investigation of which has already been initiated by that or by any other investigative body, it shall promptly advise the other interested investigative body of its views. By agreement between the Departments of Justice and Transportation (Coast Guard), investigative authority may then be transferred.

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 18 - 16

"4. Administrative action. Exercise of exclusive investigative authority by the Federal Bureau of Investigation pursuant to this agreement shall not preclude Coast Guard military authorities from making inquiries for the purpose of administrative action related to the crime being investigated. The Federal Bureau of Investigation will make the results of its investigations available to Coast Guard military authorities for use in connection with such action.

"Whenever possible, decisions with respect to the application in particular cases of the provisions of this Memorandum of Understanding will be made at the local level, that is, between the Special Agent in Charge of the local office of the Federal Bureau of Investigation and the local Coast Guard military commander.

"5. Surrender of suspects. To the extent of the legal authority conferred upon them, the Department of Justice and Coast Guard military authorities will each deliver to the other promptly suspects and accused individuals if authority to investigate the crimes in which such accused individuals and suspects are involved is lodged in the other by paragraphs 1 and 2 hereof.

"Nothing in this memorandum shall prevent the Coast Guard from prompt arrest and detention of any person subject to the Uniform Code of Military Justice whenever there is knowledge or reasonable basis to believe that such a person has committed an offense in violation of such code and detaining such person until he is delivered to the Federal Bureau of Investigation if such action is required pursuant to this memorandum.

"Approved:

/s/ Ramsey Clark

Ramsey Clark
Attorney General

Date: 9 October 1967

/s/ Alan S. Boyd

Alan S. Boyd
Secretary of Transportation

Date: 24 October 1967"

EFFECTIVE: 01/31/78

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 18 - 17

18-4.1 FBI Interpretation of Memorandum of Understanding

(1) This agreement is similar in all respects to the agreement between the Departments of Justice and Defense covering the investigation and prosecution of military personnel. (The agreement set forth above is the same as the agreement which previously existed between the Departments of Justice and Treasury. A new agreement was signed in October, 1967, because the Coast Guard was made a part of the Department of Transportation rather than the Treasury Department.) Instructions concerning the agreement between the Departments of Justice and Defense apply equally with reference to the Coast Guard Agreement.

(2) If any problems arise in your contacts with the various USAs or military officials relative to this agreement, FBIHQ must be immediately advised.

EFFECTIVE: 05/08/79

18-4.2

MEMORANDUM OF UNDERSTANDING BETWEEN THE DIRECTOR, FEDERAL BUREAU OF INVESTIGATION AND COMMANDANT, UNITED STATES COAST GUARD CONCERNING A POLICY OF MUTUAL ASSISTANCE IN SUPPORT OF COAST GUARD/FEDERAL BUREAU OF INVESTIGATION OPERATIONS TO COUNTERACT TERRORIST ACTIVITIES IN A MARITIME ENVIRONMENT

The following agreement was approved and entered into between the FBI and the United States Coast Guard relative to policy of mutual assistance and support of Coast Guard/FBI organizations to counteract terrorist activities in a maritime environment.

"In recognition of the U.S. Coast Guard's maritime law enforcement responsibility, and the operations of the Federal Bureau of Investigation in counteracting domestic terrorist activities, the following mutual assistance capabilities are identified. The Coast Guard maintains and operates a large number of strategically located floating units, aircraft, vehicles and shore stations. The Federal Bureau of Investigation maintains a large number of strategically located Special Weapons and Tactics teams (SWAT). Coast Guard personnel are trained to react to law enforcement activities in a maritime environment, while the FBI has personnel who are specifically trained to act as negotiators in dealing with terrorists' demands and SWAT teams to use in suppressing terrorists' actions during direct confrontation scenarios. The unique capabilities of the two forces in

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 18 - 18

a combined effort to counteract a terrorist takeover in the maritime environment is recognized.

"Close coordination and cooperation between forces of both Agencies is necessary to insure adequate response to potential terrorist activities involving such targets as offshore platforms, port and harbor facilities, liquefied natural gas (LNG) terminals and vessels, floating nuclear power plants, U.S. or foreign vessels within United States jurisdiction and any other target(s) which may require Coast Guard and FBI response.

"Accordingly, it is hereby understood and agreed upon that, subject to operational and budgetary constraints, the Agencies making this agreement will provide mutual support to each other in situations involving terrorist activities, threatened or real, and that each Agency will take necessary steps to establish local operating procedures to implement this agreement. It is further agreed that continued planning by the two concerned Agencies will include the development of a specific communications, command and control policy between Coast Guard Districts and FBI Regional offices.

"A basic objective of this agreement is to insure a coordinated effort to counteract terrorist activities in the maritime environment. Further, it is expected that this agreement will serve to eliminate delays in response time and insure continued development of procedures and contingency plans to counteract terrorist activities in the maritime environment.

/s/ John B. Hayes

/s/ William H. Webster

John B. Hayes
Commandant
United States Coast Guard

William H. Webster
Director
Federal Bureau of
Investigation

Date: April 17, 1979

Date: March 23, 1979"

EFFECTIVE: 05/08/79

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 18 - 19

18-4.3 FBI INTERPRETATION OF MEMORANDUM OF UNDERSTANDING

(1) While the U.S. Coast Guard has some law enforcement responsibilities on the high seas and in waters subject to the jurisdiction of the United States as provided by Title 14, USC, Sections 2 and 84, the FBI has taken the position, with the support of the Criminal Division, Department of Justice, that the FBI has primary investigative authority over certain crimes upon the high seas. Additionally, the United States Attorneys Manual indicates at Section 9-1.200, et seq that the FBI is the primary investigative agency for all the maritime crimes contained in Title 18 of the USC.

(2) It should be noted that the Memorandum of Understanding is meant to apply to a limited situation, e.g., terrorist attacks in a maritime environment. The Memorandum of Understanding basically contemplates cooperation between the U.S. Coast Guard and FBI Special Weapons and Tactics (SWAT) teams and hostage negotiators, and its application is limited to terrorist attacks. Cooperation in regard to investigation of other crimes on the high seas can be included, however, at a later time, if desirable.

(3) The Memorandum of Understanding also necessitates the development of standing lines of communication between FBI field offices and U.S. Coast Guard district offices. In view of the unique conditions existing in each area, such channels would be desirable to resolve local problems. However, FBI Headquarters will have supervisory authority over the actions of field divisions, in keeping with Bureau policy.

EFFECTIVE: 05/08/79

18-5 DOJ GUIDELINES FOR INVESTIGATIVE JURISDICTION OF FBI AND IRS

In order to eliminate, where possible, a duplication of investigative effort and to ensure a greater exchange of information between the FBI and IRS, the Department has drawn up a set of guidelines regarding investigative jurisdiction of Federal gambling violations; namely, the interstate transmission of wagering information, interstate transportation in aid of racketeering, and interstate transportation of wagering paraphernalia statutes. In the majority of cases that we investigate under these statutes, IRS, from the nature of the wagering tax laws, will have an interest also. The following guidelines are to be utilized by both agencies in such

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 18 - 20

instances. Each USA has been furnished a copy of these guidelines by the Department.

"Guidelines Regarding Investigative Jurisdiction of
Federal Gambling Violations

"In order to minimize any duplication in investigative effort between IRS and FBI field offices investigating potential violations of the wagering tax laws and the new anti-gambling legislation, the following guidelines appear appropriate.

"(1) The FBI and the IRS will continue to exchange current information regarding gambling operations which have come to the attention of each agency.

"(2) Upon the receipt of sufficient basic facts to indicate a potential violation of the anti-gambling statutes or wagering tax laws, the FBI and the IRS will notify each other prior to commencing an investigation involving such statutes within their respective jurisdictions. When the investigations involve a taxpayer who is a subject of interest to the Organized Crime and Racketeering Section of the Criminal Division the responsible Department of Justice attorney will also be notified.

"(3) If such notification reveals an apparent duplication of investigative effort, appropriate representatives of the FBI and the IRS in the field will meet to assign responsibility for the investigation to the agency whose investigation has the best potential for prosecution, depending upon the Federal statutes apparently involved and all the relevant investigative circumstances. Where it is deemed mutually desirable by the agencies, preliminary investigation might be appropriately conducted prior to any assignment of responsibility for the investigation to a single agency.

"(4) In the event that the agency representatives cannot agree as to the assignment of responsibility for a particular investigation, the matter should be resolved after discussion with the responsible United States Attorney or Department of Justice attorney.

"(5) Where statutory violations within the jurisdiction of the other agency become apparent in the middle or later stages of an investigation being conducted by either the IRS or the FBI, the agency conducting the investigation will immediately notify the other agency of the relevant facts. Responsibility for further investigation of the individual violations of law will be determined after discussion between representatives of the two agencies. If the agencies are

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 18 - 21

unable to agree as to the assignment of responsibility for further investigation, the matter should be resolved after discussion with the responsible United States Attorney or Department attorney. Depending on the circumstances, it may be preferable for such further investigation of all statutory violations to be conducted by a single agency. In such event it is expected that the other agency would cooperate and render such assistance as is deemed within its competence and capacity."

EFFECTIVE: 05/08/79

18-5.1 FBIHQ Instructions for IRS Guidelines

(1) FBIHQ will continue to make available to IRS current information of interest to that agency which is developed in the course of our investigations.

(2) With regard to item two of the guidelines as it pertains to notifying IRS when there is indication of a potential violation of wagering tax laws, such notification should be made after sufficient facts are developed to determine the logical procedures to follow and at a time when same would be more meaningful. With reference to investigations involving a taxpayer, referred to in the same item, this pertains to individuals whose names are included on a list of active gamblers maintained by Department's Criminal Division. Inasmuch as copies of all reports involving the three statutes named above are furnished the Department by FBIHQ, such should tend to serve notice to the Department that we are investigating an individual on that list. It is anticipated that when the Department receives our reports and checks its files it will thus be on notice that one of these individuals is currently being investigated.

(3) Items three and four of the guidelines are self-explanatory in that the USA should be consulted where there appears to be a duplication of investigative effort and such cannot be resolved by field representatives of both agencies. In connection with item five, regarding the assignment of investigation to a single agency, responsibility for an investigation should be definitely fixed in one agency insofar as an individual violation is concerned. In this way each agency would retain its own jurisdiction and the one whose case had the best potential for prosecution would continue its investigation. Furthermore, with regard to one agency proceeding with an investigation and the other rendering such assistance as is deemed within its competence and capacity, the agency proceeding with its

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 18 - 22

investigation should be furnished with all pertinent information of assistance by the other agency. This will preclude the necessity for any joint investigation and result in each agency handling its own violation completely.

(4) Each office should make every effort to avoid overlapping of jurisdiction which these guidelines are intended to minimize. It is recognized that at least preliminary investigation is necessary before any of these matters can be logically discussed by both agencies. It is the feeling of FBIHQ that the matter of jurisdiction in the majority of instances can be resolved on a field level by the two agencies and that the necessity for contacting the USA or Department attorney would be rare.

(5) FBIHQ should be kept advised of any matters in this regard that are discussed with the USA, and also should be advised of any investigative action withheld through agreement with IRS or on recommendation of the USA.

EFFECTIVE: 01/31/78

18-6 AGREEMENT BETWEEN FBI AND SECRET SERVICE

"AGREEMENT BETWEEN THE FEDERAL BUREAU OF INVESTIGATION AND THE UNITED STATES SECRET SERVICE CONCERNING PROTECTIVE RESPONSIBILITIES

"I. Purpose of Agreement

"The Federal Bureau of Investigation (FBI) originates, and receives from other sources, large numbers of reports on individuals and organizations. One purpose of this agreement is to define that portion of the information on file with, or received or originated by, the FBI, which the United States Secret Service (USSS) desires to receive in connection with its protective responsibilities.

"The USSS has statutory authority to protect, or to engage in certain activities to protect, the President and certain other persons. (Certain other persons, as used in this agreement, refers to those persons protected by the Secret Service under Title 18, U.S. Code, Section 3056.) The authority of the USSS to protect the President or certain other persons is construed to authorize it to investigate organizations or individuals and to interview individuals

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 18 - 23

who might constitute a threat to the President or certain other persons. The FBI has statutory authority to investigate assault, killing or kidnaping and attempts or conspiracies to kill or kidnap the President and other designated individuals.

"The FBI will make available to the USSS information it may request or information which by its nature reveals a definite or possible threat to the safety of the President and certain other persons.

"A second purpose of this agreement is to insure the most effective protection for the President and certain other persons by establishing a clear division of responsibility between the FBI and USSS. Such division will also avoid compromising investigations or sources and needless duplication of effort.

"II. General Responsibilities

"The USSS is charged by Title 18, U.S. Code, Section 3056, with the responsibility of protecting the person of the President of the United States, the members of his immediate family, the President-elect, the Vice President or other officer in the order of succession to the office of President, and the Vice President-elect; protecting the person of a former President and his wife during his lifetime and the person of a widow of a former President until her death or remarriage, and minor children of a former President until they reach 16 years of age, unless such protection is declined; protecting persons who are determined from time to time by the Secretary of the Treasury, after consultation with the Advisory Committee, as being major Presidential and Vice Presidential candidates who should receive such protection (unless the candidate has declined such protection); protecting the person of a visiting head of a foreign state or foreign government and, at the direction of the President, other distinguished foreign visitors to the United States and official representatives of the United States performing special missions abroad (unless such persons decline protection).

"The Executive Protective Service, under the control of the Director, USSS, is charged by Title 3, U.S. Code, Section 202, with protection of the Executive Mansion and grounds in the District of Columbia; any building in which Presidential offices are located; foreign diplomatic missions located in the metropolitan area of the District of Columbia; and foreign diplomatic missions located in such other areas in the United States, its territories and possessions, as the President, on a case-by-case basis, may direct.

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 18 - 24

"The FBI is charged under Title 18, U.S. Code, Section 1751, with investigative jurisdiction over the assault, killing or kidnaping, and attempts or conspiracies to assault, kill or kidnap the President of the United States and other designated individuals.

"The FBI has responsibility for Federal investigations of all violations of Title 18, U.S. Code, Sections 112, 970, 1116-1117 and 1201, relating to the Act for the Protection of Foreign Officials and Official Guests in the United States.'

"The FBI has investigative jurisdiction over violations of a wide range of the criminal statutes of the United States including primary jurisdiction over matters affecting the internal security of the United States.

"III. Exchange of Information and Coordination of Responsibilities

b7E
per
Secret
Service

[REDACTED]

refer

[REDACTED]

"The USSS agrees that it will conduct no investigation of individuals or groups identified or suspected of being threats to the internal security of the United States without notifying the FBI. However, when time for consultation is not available, and an

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 18 - 25

indication of immediate danger exists, the USSS may take such action as is necessary with respect to carrying out its protective responsibilities. Any information obtained by the USSS during such action will be furnished to the FBI as expeditiously as possible.

"The FBI will not conduct investigation of individuals or groups solely for the purpose of establishing whether they constitute a threat to the safety of the President and certain other persons unless there is an indication of a violation of Title 18, U.S. Code, Section 1751, or other statute over which the FBI has jurisdiction.

"It will be the responsibility of the FBI to advise the USSS when investigation is being initiated under Title 18, U.S. Code, Section 1751 and thereafter to furnish the USSS with copies of the FBI investigative reports as they are prepared. It will be the responsibility of the USSS to furnish the FBI any information in its possession or which may come to its attention which reasonably indicates that a violation of Title 18, U.S. Code, Section 1751, has been or is being committed.

"The USSS also agrees to furnish the FBI any information in its possession or which may come to its attention indicating a violation of any other statutes over which the FBI has investigative jurisdiction.

"The FBI, under its responsibility for investigation of violations of Title 18, U.S. Code, Sections 112, 970, 1116-1117, 1201 and 1751 will take cognizance of the protective responsibilities of the Treasury Department under Title 3, U.S. Code, Section 202 and Title 18, U.S. Code, Section 3056 and thus does not limit or interfere with the authority of the Secretary of the Treasury in the discharge of his statutory protective responsibilities. This is not to be construed as vesting concurrent investigative jurisdiction with the Treasury Department with respect to investigations of individuals or organizations engaged in activities affecting the national security including terrorism, treason, sabotage, espionage, counter-espionage, rebellion or insurrection, sedition, seditious conspiracy, neutrality matters, Foreign Agents Registration Act, or any other Statute or Executive Order relating to national security. Any investigations of such groups or individuals for any reasons other than in connection with protective responsibilities must be closely coordinated with and have the concurrence of the FBI in order to minimize interference with national security responsibilities of the FBI.

"IV. Information to be Furnished to the United States Secret Service by the Federal Bureau of Investigation

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 18 - 26

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

b7E
per
Secret
Service

"B. Types of information to be referred:

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 18 - 27

b7E
per
Secret
Service

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

"V. Provision of Federal Bureau of Investigation Personnel to Protect the President and Other Protected Persons

"The USSS may, in accordance with Title 18, U.S. Code, Section 3056 request FBI Agents be detailed to the USSS in order to augment the capacity of the USSS to perform its protective duties. Such requests should be addressed to the Director of the FBI.

"FBI Agents detailed to the USSS are under the direction and exclusive operational control of the Director of the USSS for the period of their assignment. The FBI agents so detailed may perform an armed or other protective function.

"VI. Implementation of Agreement

"In order to effect the best possible security of the President and certain other persons and places whose protection is the responsibility of the USSS, the FBI and the USSS will construe the terms of this agreement liberally and will take such steps as are necessary to insure the proper exchange and coordination of information.

"The agreement shall be reviewed annually by representatives of the FBI and the USSS, or at such other times as the FBI or the USSS may request, to insure that the agreement is both

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 18 - 28

practical and productive. Revisions may be made on the authority of the Director of the FBI and the Director of the USSS.

"This agreement supersedes all prior agreements between the FBI and the USSS.

July 16, 1973
Date

BY /s/ Clarence M. Kelley
Director
Federal Bureau of
Investigation

July 30, 1973
Date

BY /s/ James J. Rowley
Director
United States Secret
Service"

EFFECTIVE: 01/31/78

18-7 MEMORANDUM OF UNDERSTANDING BETWEEN FBI AND ERDA

"MEMORANDUM OF UNDERSTANDING BETWEEN THE ENERGY RESEARCH AND DEVELOPMENT ADMINISTRATION AND THE FEDERAL BUREAU OF INVESTIGATION FOR RESPONDING TO NUCLEAR THREAT INCIDENTS

"I. PURPOSE - In recognition of the responsibilities and functions of the Energy Research and Development Administration, hereinafter referred to as ERDA; and the Federal Bureau of Investigation, hereinafter referred to as the FBI, under the Atomic Energy Act of 1954, this Memorandum of Understanding sets forth the responsibilities of each agency with regard to nuclear threat incidents.

"II. IMPLEMENTATION - ERDA and the FBI will develop and exchange such additional instructions and operating procedures as are deemed necessary to the continued implementation of this Memorandum of Understanding.

"III. RESPONSIBILITIES

"A. FBI - The FBI is responsible for investigating all alleged or suspected criminal violations of the Atomic Energy Act as set forth in Section 221 b. of that Act. The mission of the FBI in a

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 18 - 29

nuclear threat incident is to take primary jurisdiction where a question of the violation of Federal law exists and, where appropriate, to coordinate the utilization of available resources in the interest of the public health and safety.

"It is therefore understood that the FBI shall:

"1. Assume jurisdiction over all field organizations associated with a nuclear threat incident.

"2. Establish and maintain contacts and coordinate nuclear threat incidents with other Federal and local law enforcement agencies, and military authorities, as appropriate.

"3. Ensure that all reasonable measures are provided for the security from physical violence of personnel and equipment to be utilized in search, deactivation, and cleanup operations related to a nuclear threat incident, and on the advice and recommendation and with the assistance of specially trained ERDA and/or DOD teams, ensure that all reasonable measures are provided for the safety of personnel from radiological hazard.

"4. Designate a liaison representative to accompany ERDA Nuclear Emergency Search Team (NEST) personnel to the scene of a threat incident for the purpose of coordinating with local FBI officials and law enforcement agencies.

"5. Promptly notify National Command Authority of any nuclear threat incident.

"6. Promptly notify ERDA Headquarters of any actual or alleged nuclear threat incident reports.

"7. Promptly provide ERDA with the exact wording of threat messages, copies of drawings, nuclear material samples, or other intelligence related to a threat for scientific analysis and credibility assessment.

"8. Promptly provide ERDA with all available information pertinent to an assessment of a threat perpetrator's technical capabilities to carry out a threat.

"9. At the scene of a nuclear threat incident, provide necessary support as may be needed by ERDA NEST personnel in carrying out assigned operations.

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 18 - 30

"10. Request assistance of DOD/Civil Explosive Ordnance Disposal (EOD) resources, as appropriate.

"B. ERDA - The mission of ERDA in a nuclear threat incident is to provide expert assistance to the FBI upon notification of the existence of such an incident.

"It is therefore understood that ERDA shall:

"1. Activate the ERDA Headquarters Emergency Action and Coordination Team (EACT), as appropriate, to coordinate with the FBI and direct ERDA's involvement in a nuclear threat incident.

"2. Provide scientific and technical support for threat assessment and search operations, device deactivation, relocation and storage of special nuclear material evidence, and/or in post-incident cleanup.

"Scientific and technical support shall include:

"a. Analysis of threat messages for technical content, nuclear design feasibility, and general credibility.

"b. Prediction as to the size of a potential nuclear burst as may occur from the successful detonation of a threatened nuclear device activation.

"c. Prediction of contamination zones and radioactivity levels.

"d. Recommendations for evacuation.

"e. Recommendations for special search techniques.

"f. Operations of special search techniques.

"g. Identification of isotopes.

"h. Recommendations for special EOD procedures and techniques.

"i. Identification of nuclear weapons and components.

"j. Identification of radioactive hazards during cleanup activities and bomb scene investigation.

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 18 - 31

"k. The provision of personnel who are expert in nuclear weapon design, health physics, special detectors, explosives, nuclear materials, arming and firing systems, radiography, transportation and storage of nuclear materials, and contamination prediction.

"3. Acquire, maintain, and make available any special equipment and capabilities required to provide the necessary scientific and technical support.

"4. Coordinate nuclear threat incident activities with the Nuclear Regulatory Commission (NRC), as appropriate. (Nuclear threat incidents involving facilities or material within the jurisdiction of the NRC are initially reported by NRC to the FBI.)

"5. Arrange for any special transportation of ERDA equipment and personnel, and/or nuclear evidence, as required during a nuclear threat incident.

"6. Notify and request assistance from the DOD and civilian agencies for post-incident cleanup activities as soon as appropriate.

"7. Have final authority in matters of (a) Restricted Data classification and (b) ERDA-originated National Security Information classification associated with source material, special nuclear material, radioactive byproducts, or nuclear weapons/components.

"8. Provide, upon request by the Justice Department, scientific and technical information and testimony for use in any legal action taken by the Department of Justice.

"C. JOINT

"The FBI and ERDA shall:

"1. Coordinate all proposed press releases related to nuclear threat incidents. Any media or public inquiries will be initially referred to the FBI; responses to such inquiries will be coordinated with ERDA.

"2. Where appropriate, identify individuals assigned to fulfill the positions and responsibilities outlined in Section IV. B., 1, and 2, and 3.

"3. Treat all threat incident information with adequate

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 18 - 32

security and confidentiality commensurate with National Security guidelines and the standards for the preservation of criminal evidence.

"4. Review, as appropriate, the events leading to and occurring during any nuclear threat incident alert for the purpose of improving upon future joint responses.

"5. Provide a mechanism for coordinated planning and the testing of nuclear threat incident management, equipment and personnel.

"IV. STANDARD PROCEDURES

"A. INITIAL NOTIFICATION

"1. Nuclear threat incidents could be reported to either the FBI or ERDA. Upon receipt of such a report the agency informed shall immediately notify the other agency about the situation and as to the exact information known.

"2. Both agencies shall notify, as appropriate, the various branches, offices or individuals within their jurisdictions about the situation and what actions might be required.

"B. POINTS OF CONTACT

"1. The FBI will designate a Special Agent to take command of field operations in a nuclear threat incident, and a Special Agent to act as a liaison officer with ERDA at the Headquarters level.

"2. The ERDA Headquarters EACT will command the ERDA Headquarters Operations Center and the Director, EACT, will direct an ERDA Field Manager of Operations to act as ERDA representative for field operations in a nuclear threat incident.

"3. The Director, EACT, will consult with the FBI and will assign NEST personnel to provide required support in a nuclear threat incident. An FBI liaison representative will be designated to accompany NEST personnel to the scene of a threat incident for local coordination purposes.

"4. Points of contact with other involved Federal agencies will be maintained by the Director, EACT, as appropriate.

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 18 - 33

"C. THREAT ASSESSMENT

"1. ERDA will provide scientific and technical support for determining the credibility of specific nuclear threats and the potential hazard associated with those threats.

"2. ERDA will endeavor to verify, with the cooperation of the NRC and/or DOD, whether any source material, special nuclear material, radioactive byproducts, or ERDA nuclear weapons/components are missing or unaccounted-for.

CLEANUP "D. SEARCH, DEVICE DEACTIVATION, AND POST-INCIDENT
SUPPORT

"1. ERDA will dispatch, upon request of the FBI, an ERDA NEST response group and any necessary specialized equipment to the scene of an incident.

"2. The ERDA NEST lead representative on-scene will:

"a. Direct the activities of the ERDA response group in support of the FBI Agent in Charge.

"b. Ensure coordinated ERDA support in all matters pertaining to search and identification operations and bomb scene examinations.

"c. Ensure coordinated ERDA support of the EOD services associated with any device deactivation operations.

"d. Ensure coordinated ERDA support with the DOD and other civilian agencies, as currently provided for under other agreements, for post-incident cleanup operations.

"e. Advise the on-scene Special Agent in Charge of any requirement for additional ERDA response capabilities and coordinate the provision of such additional capabilities as may be mutually agreed upon.

"3. The on-scene Special Agent in Charge will:

"a. Establish and maintain all local contacts with other law enforcement agencies.

"b. Direct the on-scene activities of the FBI and other law enforcement agencies.

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 18 - 34

"c. Establish a field command post.

"d. Provide for necessary escorts as may be required to facilitate rapid movement of ERDA and ERDA contractor personnel and equipment to the scene of a threat incident.

"e. Direct the recovery operation of lost or stolen special nuclear materials, radioactive byproducts, and nuclear weapons/components.

"E. MAJOR EMERGENCY DISASTER -- In the event of a major emergency/disaster, ERDA will assist in the response to post-incident cleanup requirements in coordination with the DOD, and various civilian agencies as currently provided for under other agreements. ERDA will request assistance from the DOD as provided for in the Joint DOD and ERDA Agreement in Response to Accidents and Incidents Involving Radioactive Materials and Nuclear Weapons.

"V. EMERGENCY ASSISTANCE EXPENSE - ERDA and the FBI will each fund for the costs incurred in providing the necessary assistance required to meet the responsibilities defined in this Memorandum of Understanding.

"This Memorandum of Understanding takes effect immediately.

/s/ Alfred D. Starbird
Assistant Administrator for National
Security
Energy Research and Development
Administration

6/11/76
Date

/s/ Clarence M. Kelley
Clarence M. Kelley
Director
Federal Bureau of Investigation"

6/8/76
Date

(NOTE: See Appendix next for definitions and abbreviations.)

APPENDIX

"DEFINITIONS AND ABBREVIATIONS

DOD - Department of Defense

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 18 - 35

EACT - ERDA Headquarters Emergency Action and Coordination Team composed of representatives of the Divisions of Military Application; Safeguards and Security; Operational Safety, and the Office of Public Affairs

EOD - Explosive Ordnance Disposal, U.S. Army

ERDA - Energy Research and Development Administration

FBI - Federal Bureau of Investigation

NEST - Nuclear Emergency Search Team

NRC - Nuclear Regulatory Commission

Nuclear Threat Incident - Any situation involving stolen, lost or unauthorized possession of source materials, radioactive byproducts, nuclear weapons/devices of U.S. and/or foreign manufacture, improvised nuclear explosives, radioactive dispersal devices or the threatened use of said items.

Source Material - The term "source material" means (1) uranium, thorium or any other material which is determined by the Administration pursuant to the provisions of Section 61 of the Atomic Energy Act to be source material; or (2) ores containing one or more of the foregoing materials, in such concentration as the Administration may by regulation determine from time to time.

Special Nuclear Material - The term "special nuclear material" means (1) plutonium, uranium enriched in the isotope 233 or in the isotope 235, and any other material which the Administration, pursuant to the provisions of Section 51 of the Atomic Energy Act determines to be special nuclear material, but does not include source material; or (2) any material artificially enriched by any of the foregoing, but does not include source material.

Radioactive Byproduct - The term "radioactive byproduct" means any

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 18 - 36

radio active material (except special nuclear material) yielded in or made radioactive by exposure to the radiation incident to the process of producing or utilizing special nuclear material.

Improvised Nuclear Explosive Device - Any non-conventional explosive device containing nuclear or radioactive material in combination with explosives."

EFFECTIVE: 01/31/78

18-8

"MEMORANDUM OF UNDERSTANDING BETWEEN THE FEDERAL BUREAU OF INVESTIGATION AND THE NUCLEAR REGULATORY COMMISSION REGARDING NUCLEAR THREAT INCIDENTS INVOLVING NRC LICENSED FACILITIES, MATERIALS, OR ACTIVITIES

"I. PURPOSE

"In recognition of the responsibilities and functions of the Federal Bureau of Investigation (FBI) and the Nuclear Regulatory Commission (NRC) under the Atomic Energy Act of 1954, as amended, this Memorandum of Understanding (MOU) delineates the responsibilities of each agency regarding nuclear threat incidents involving NRC-licensed facilities, materials, or activities. (This agreement does not affect the procedures and responsibilities set forth in the November 23, 1988, Memorandum of Understanding between the NRC and the Department of Justice (DOJ) regarding cooperation concerning NRC enforcement actions, criminal prosecution by DOJ, and the exchange of pertinent information.)

"Having closely related statutory responsibilities with regard to nuclear materials, facilities, and activities in the United States, the FBI and NRC must cooperate fully in carrying out their respective responsibilities in the interest of achieving:

"1. Effective communication and exchange of relevant information, and

"2. A timely, reliable, and effective response to a nuclear threat incident.

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 18 - 37

"II. DEFINITIONS

"For the purpose of this agreement, nuclear threat incidents are defined as threats, or acts of theft or sabotage in the U.S. nuclear industry, including the following:

"Theft or attempted theft of NRC-licensed special nuclear material.

"Sabotage or attempted sabotage of NRC-licensed nuclear facilities or NRC-licensed transportation activities.

"Attacks on NRC-licensed nuclear facilities or activities.

"Credible threats involving NRC licensed facilities, materials, or activities.

"III. RESPONSIBILITIES

"A. The FBI

"The FBI derives the authority to investigate criminal matters related to NRC licensed facilities, materials, or activities from the Atomic Energy Act of 1954, as amended; Title 18, Section 831 "Prohibited transactions involving nuclear materials," and other Federal statutes as may be applicable. The FBI has been designated as the lead agency for coordinating the Federal response to acts of terrorism within the United States by National Security Decision Directive (NSDD) Number 207 and the National System for Emergency Coordination (NSEC).

"It is therefore understood that the FBI shall:

"1. Provide to NRC, intelligence information concerning possible criminal acts relative to the security of nuclear facilities, materials, or activities.

"2. Notify NRC when allegations of a serious nature arise, or derogatory information is developed involving licensee personnel occupying positions considered critical to the safety and security of nuclear facilities or activities.

"3. Investigate ongoing nuclear-related threat situations; advise NRC regarding the credibility and danger of such threats.

"4. Establish liaison and develop contingency response plans

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 18 - 38

with pertinent local law enforcement agencies to ensure effective and coordinated law enforcement response operations.

"5. In accordance with the Omnibus Diplomatic Security and Anti-Terrorism Act of 1986, conduct identification and criminal history records checks on individuals with unescorted access to NRC licensed nuclear power plants or access to Unclassified Safeguards Information.

"6. Establish liaison with pertinent NRC Headquarters staff, NRC regional offices, and licensed facilities to ensure effective information exchange, threat evaluation, and contingency response planning.

"In the event of a nuclear threat incident the FBI shall:

"7. Coordinate the Federal response to a nuclear threat incident involving NRC-licensed facilities, materials, or activities. The FBI will rely on the NRC on matters concerning public health and safety, as they relate to the nuclear facility, material, or activity.

"8. Manage the law enforcement and intelligence aspects of the response to a nuclear threat incident involving NRC-licensed facilities, materials, or activities.

"9. Establish and maintain contacts and coordinate the incident response with other Federal and local law enforcement agencies and military authorities, as appropriate.

"10. Ensure that all reasonable measures are provided to ensure the physical safety and security of all NRC personnel and equipment to be used in support of the incident.

"11. Promptly provide NRC with all information applicable to an assessment of a perpetrator's operational capability to carry out a threat.

"12. At the scene of a nuclear threat incident, provide the necessary support, as may be needed by NRC personnel, in carrying out assigned operations and actions to protect the public from radiological hazards.

"13. Request Department of Defense (DOD)/Civil Explosive Ordnance Disposal (EOD) resources, as appropriate.

"B. The NRC

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 18 - 39

"NRC shall provide, to the extent compatible with its primary mission to protect the public's health and safety, as required by the Atomic Energy Act of 1954, as amended, the Energy Reorganization Act of 1974, and the Omnibus Diplomatic Security (Act) and Anti-Terrorism Act of 1986, scientific and technical support to the FBI upon notification of the existence of a nuclear threat incident.

"It is therefore understood that NRC shall:

"1. Review and correlate intelligence information on possible criminal acts received from the FBI; evaluate potential adversary capabilities and trends as a basis for rulemaking, evaluations, and systems design.

"2. When informed of an FBI investigation involving an NRC licensed nuclear facility or activity, will promptly provide to the FBI investigating office a list of all positions considered critical to the safety and security of that facility or activity.

"3. Establish liaison with FBI Headquarters staff and field office personnel to ensure effective information exchange, threat evaluation, and contingency response planning.

"4. Support joint operational readiness planning between licensees and associated local law enforcement agencies for prompt law enforcement response assistance when needed at licensed facilities or activities.

"5. Notify the FBI of threats involving NRC-licensed nuclear facilities, materials, or activities; assist the FBI in evaluating the nuclear aspects and the credibility of such threats, as appropriate.

"6. Disseminate, with the approval of the FBI, to the affected licensees, alert and warning information received from the FBI about specific nuclear-related threats.

"In the event of a nuclear threat incident, NRC shall:

"7. Plan for and manage the public health and safety aspects of the response to a nuclear threat incident involving NRC-licensed facilities, materials, or activities.

"8. Provide NRC field liaison and technical assistance to the FBI at the scene of an incident.

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 18 - 40

"9. Evaluate the radiological hazards of the particular incident and provide technical assessment of any potential or actual impact upon the public health and safety.

"10. Ensure that all reasonable measures are provided for the health and safety of all FBI personnel and equipment involved in the support of the incident.

"11. Provide for the health and safety of the public from radiological hazards.

"C. Joint

"The FBI and NRC shall:

"1. Coordinate all proposed press releases related to nuclear threat incidents involving NRC-licensed facilities, materials, or activities.

"2. Identify individuals assigned to fulfill the positions and responsibilities outlined in Section III of this agreement.

"3. Handle all threat incident information with adequate security and confidentiality commensurate with national security guidelines and the standards for the preservation of criminal evidence.

"4. Review and evaluate the events leading to and occurring during a nuclear threat incident for the purpose of improving upon future joint responses.

"5. Exercise and test nuclear threat incident management procedures, equipment, and personnel.

"IV. STANDARD PROCEDURES

"A. Initial Notification

"1. Nuclear threat incidents involving NRC-licensed facilities, materials, or activities may be reported to either the FBI, NRC, or others. Upon receipt of a reported threat, the agency informed shall immediately notify the other concerned agencies about the situation and exact information known.

"2. The FBI and NRC will notify appropriate individuals and

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 18 - 41

offices of any nuclear emergency in accordance with current procedures and agreements.

"B. Points of Contact

"1. The FBI Special Agent in Charge of the responding FBI field office will take command of the field operations in a nuclear threat incident involving NRC-licensed facilities, materials, or activities. At the Headquarters level, a Special Agent may be designated to act as a liaison officer with the NRC Executive Team (ET).

"2. The NRC Headquarters ET will convene and during the initial stage of the response will direct NRC activities. The Director may transfer authority for managing the NRC emergency response to the Director of Site Operations.

"3. The FBI and NRC field representatives will coordinate and cooperate with each other in carrying out their respective responsibilities. The FBI and NRC representatives will report on the situation and make recommendations to their respective agencies regarding the need for additional assistance at the scene.

"4. The FBI and NRC will maintain points of contact with the other Federal agencies involved in responding to a nuclear threat incident involving NRC-licensed facilities, materials, or activities.

"V. THREAT ASSESSMENT

"1. NRC will provide scientific and technical advice for determining the credibility of specific nuclear threats and potential hazards associated with those threats.

"2. NRC will endeavor to verify, with the cooperation of the Department of Energy and/or the Department of Defense, whether any source material, special nuclear material, or radioactive by-products, are missing or unaccounted for.

"VI. FUNDING RESPONSIBILITIES

"Interest parties will each fund for the cost incurred in providing the necessary assistance required to meet the responsibilities defined in this MOU.

"VII. TERMS OF AGREEMENT

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 18 - 42

"1. This Agreement will become effective immediately upon signature by all parties and shall continue in effect unless terminated by any party upon 120 days notice in writing to all other parties.

"2. Amendments or modifications to this Agreement may be made upon written notice by all parties to the Agreement.

"For the Federal Bureau of Investigation

/s/ William S. Sessions, date May 29, 1991
William S. Sessions
Director

"For the Nuclear Regulatory Commission

/s/ Kenneth M. Carr, date 13 March 1991
Kenneth M. Carr
Chairman"

EFFECTIVE: 08/28/91

18-9 "JOINT FEDERAL BUREAU OF INVESTIGATION, DEPARTMENT OF ENERGY AND DEPARTMENT OF DEFENSE AGREEMENT FOR RESPONSE TO IMPROVISED NUCLEAR DEVICE INCIDENTS

"I. PURPOSE AND SCOPE.

"To set forth and define specific areas of responsibility and procedures for responding to emergencies involving improvised nuclear devices (IND) within the United States, District of Columbia, Commonwealth of Puerto Rico, and U.S. possessions and territories, by representatives of the Federal Bureau of Investigation (FBI), Department of Energy (DOE), and the Department of Defense (DOD). These provisions amplify the current DOD/DOE Agreement of 1 March 1977, DOE/FBI Memorandum of Understanding of June 1976 dealing with response to accidents or incidents involving nuclear material, and the Attorney General's letter to the Secretary of Defense on assistance to Federal agencies in combatting terrorism, dated November 10, 1972.

"II. TERMS OF AGREEMENT.

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 18 - 43

"a. This agreement shall be effective upon signature by representatives of the Federal Bureau of Investigation, the Department of Energy, and the Department of Defense.

"b. Amendments, modifications, or termination of this agreement may be made by written agreement of all parties.

"III. POLICY.

"In the event of a Nuclear Threat Incident involving an Improvised Nuclear Device (IND), the Federal Bureau of Investigation is responsible, as set forth in Section 221.b. of the Atomic Energy Act, as amended, for investigating all alleged or suspected criminal violations of that Act. The FBI has primary jurisdiction where a question of the violation of Federal law exists and, where appropriate, will coordinate the utilization of available resources in the interest of public health and safety.

"The Department of Energy and the Department of Defense will provide assistance and support to the FBI as listed in Section V of this agreement.

"IV. IMPLEMENTATION.

"Each party will issue its own departmental instructions and detailed operating procedures implementing this agreement and will develop and exchange additional instructions and procedures as are deemed necessary to be continued implementation of this agreement.

"V. RESPONSIBILITIES.

"a. The Federal Bureau of Investigation will:

"1. Act as the Federal agency in charge at the scene of an IND incident and assume jurisdiction over all field organizations.

"2. Establish and maintain contacts and coordinate IND incident support requirements with other Federal and local law enforcement agencies.

"3. Provide security for personnel and equipment to be utilized in search, deactivation, and cleanup operations.

"4. Provide, at the incident scene, a representative to act as liaison with Federal and local authorities.

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 18 - 44

"5. Notify appropriate individuals and offices of any nuclear threat incident.

"6. Notify DOE Headquarters of support requirements and provide:

"(a) The exact wording of threat messages, copies of drawings, nuclear material samples, or other related intelligence for scientific analysis and credibility assessment.

"(b) All information pertinent to an assessment of a threat perpetrator's technical capabilities to carry out a threat.

"7. Notify the National Military Command Center (NMCC)/ Emergency Ordnance Disposal (EOD) of support requirements for either standby or deployment.

"8. Provide additional support as required by DOE and DOD/EOD personnel in carrying out assigned operations.

"b. The Department of Energy, upon notification by the FBI of an IND incident, will:

"1. Provide scientific and technical assistance and advice to the FBI and DOD in the areas of threat assessment and search operations, device deactivation, hazards assessment, containment, relocation and storage of special nuclear material evidence, and in post-incident cleanup.

"2. Analyze threat messages for technical content, nuclear design feasibility, and general credibility and provide such analyses to the FBI.

"3. Acquire, maintain, and make available any special equipment and capabilities required to provide the necessary scientific and technical support.

"4. Coordinate IND incident activities with the Nuclear Regulatory Commission (NRC), as appropriate. (IND incidents involving facilities or material within the jurisdiction of the NRC are initially reported by NRC to the FBI.)

"5. Arrange for any special transportation of DOE equipment, personnel, and/or nuclear material, as required.

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 18 - 45

"6. Notify the DOD and civilian agencies of, and request assistance for, post-incident cleanup activities as soon as appropriate.

"7. Have final authority concerning the classification of Restricted Data and DOE-originated National Security Information associated with source material, special nuclear material, radioactive by-products, or nuclear weapons/components.

"8. Provide, upon request by the FBI, scientific and technical information and testimony for use in any legal action undertaken by the Department of Justice.

"c. The Department of Defense, upon request by the FBI, will:

"1. Provide EOD technical and operational assistance to the FBI.

"2. Provide EOD technology, procedures and equipment for working point access, device deactivation, and nonnuclear device diagnostics.

"d. The FBI, DOE, and DOD will:

"1. Coordinate all proposed press releases related to IND incidents. Any media or public inquiries will be initially referred to the FBI; responses to such inquiries will be coordinated with DOE and DOD.

"2. Treat all IND incident information with adequate security and confidentiality commensurate with National Security classification guidelines and the standards for the preservation of criminal evidence.

"3. Review the IND incident for the purpose of improving upon future joint responses.

"4. Provide a mechanism for coordinated planning and for coordinated training and testing of IND incident management, equipment, and personnel.

"e. The DOE and DOD, in support of the FBI, will:

"1. Develop working point operating procedures

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 18 - 46

to be followed after location of an IND.

"2. Provide for:

"(a) IND EOD training material including inert nuclear and high-explosive devices and fuzing and firing systems.

"(b) Realistic training exercises that include participation by all parties (FBI, DOE, and DOD/EOD).

"(c) Training in EOD practices, procedures, and component identification safety precautions for IND.

"(d) Research and development in the areas of render safe and disposal technology including radiation dispersal containment concepts.

"VI. PROCEDURES.

"a. Initial Notification

"1. IND incidents could initially come to the attention of the FBI, DOE or the DOD. Upon receipt of such information, the agency informed shall immediately notify the nearest FBI office and provide all known information. The FBI will officially notify all agencies involved of the incident.

"2. All agencies shall notify the various branches, offices, or individuals concerned within their jurisdictions about the situation and specify what actions and/or resources might be required.

"b. Initial Preparation

"1. The FBI will designate a Special Agent to take command of field operations and Special Agents to act as liaison with DOE Headquarters, local police jurisdictions, and the National Military Command Center.

"2. DOE will consult with the FBI and will assign personnel to provide required support. An FBI liaison representative will be designated by competent authority to accompany DOE personnel to the scene of an IND incident for local coordination purposes.

"3. The NMCC will, upon the receipt of notification by the FBI of a credible IND incident, notify the applicable DOD

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 18 - 47

Operations Center which will utilize its established notification system in order to dispatch an EOD unit and other technical and operational support to the incident site. An FBI representative will be designated by competent authority as point of contact for EOD personnel at the scene of an IND incident for local coordination purposes.

"4. The DOD/EOD command post will be collocated in the incident site control center.

"c. Threat Assessment

"1. The FBI with DOE assistance, including DOD participation when appropriate, will provide a threat assessment.

"2. DOE will provide scientific and technical assistance for determining the credibility of specific nuclear threats and the potential hazards associated with those threats and report its assessments to the FBI.

"3. DOE will determine, in coordination with the NRC, if any source material, special nuclear material, or radioactive by-products are missing or unaccounted for and report results to the FBI. DOD and DOE will, when requested by the FBI, determine if any nuclear weapons or components are missing.

"4. The FBI will notify DOD through the NMCC of any credible threat and request DOE and DOD/EOD assistance.

"d. Search and Location

"1. DOE will have primary responsibility for the search and location of IND's.

"2. DOE will dispatch, upon request of the FBI, a DOE response group and necessary special equipment to the scene of an incident.

"3. The DOE response group will, by use of specialized equipment, attempt to determine the presence and location of an IND.

"4. DOE will relay all data relating to the IND including radiological readings, configurations, and location to the FBI and the DOD/EOD team.

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 18 - 48

"5. DOD/EOD personnel will identify the presence or suspected presence of booby-trapped devices in the area or structure in which the DOE response group is searching.

"6. The DOD/EOD team present will be responsible for the clearance of any booby-traps or other hazardous items encountered by the DOE team during the search.

"7. The FBI will have primary responsibility for security of, and access to, the location of an IND incident.

"e. Incident Site Reconnaissance and Clearance

"1. DOD/EOD, with DOE technical assistance, will have primary responsibility for incident site reconnaissance and clearance.

"2. DOD/EOD personnel will clear the area/structure of explosive devices.

"3. DOD will provide a qualified individual for safety and coordination of functions at the working point.

"f. Diagnostics and Measurements

"1. DOE, with DOD/EOD assistance, will have primary responsibility for diagnostics and measurements.

"2. DOE personnel will determine, through use of diagnostic and measurement equipment, details of the suspected device, including its structure and function.

"3. Data relative to the anticipated structure and function of the device will be provided by DOE to the FBI and DOD/EOD personnel.

"4. Provide a hazard assessment to the DOD and FBI as related to the incident.

"g. Dispersal Containment Preparations

"1. DOD with DOE and FBI support will have primary responsibility for dispersal containment preparations.

"2. DOD/EOD and DOE personnel will develop, with FBI support, any required containment apparatus for explosive and

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 18 - 49

| radiological matter.

| "h. Device Deactivation

| "1. DOD/EOD, with FBI and DOE support, will have the primary responsibility for device deactivation.

| "2. DOD/EOD and DOE personnel will develop suitable render safe procedures.

| "3. DOD/EOD personnel will perform the approved deactivation procedures. DOD/EOD, FBI, and DOE personnel will work in close cooperation to achieve the deactivation of the device.

| "i. Post Incident Operations

| "1. The FBI, with support of DOE, DOD and other Federal, state and local authorities will have primary responsibility for post-incident operations.

| "2. DOD/EOD and DOE personnel will work closely with, and in support of, the FBI in the preservation of evidence.

| "3. DOE and DOD will arrange for any special transportation of nuclear material in coordination with the FBI.

| "4. The FBI will request assistance from DOE, DOD, and appropriate civilian agencies for post-incident cleanup.

| "j. Major Emergency or Disaster.

| "In the event of a major emergency or disaster, DOE will assist in the response to post-incident cleanup requirements in coordination with the DOD and various civilian agencies as provided for under other agreements. DOE will have assistance from the DOD as provided for in the March 1, 1977, DOD and DOE Agreement in Response to Accidents-Incidents Involving Radioactive Material or Nuclear Weapons.

| "VII. Emergency Assistance Expense.

| "DOD, DOE, and the FBI will each fund for the costs which they incur in providing the equipment and services required to meet their responsibilities defined in this agreement. Any reimbursements which may subsequently be agreed upon by the undersigned in furtherance of this agreement will be in accordance with the Economy

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 18 - 50

Act, 31 U.S.C. 8. This agreement takes effect on the last date of signature shown below:

/s/ Duane C. Sewell, date 2/27/80

Duane C. Sewell, Assistant Secretary
for Defense Programs, DOE

/s/ David M. Mullaney, date 1/29/80

David M. Mullaney, Brig. Gen, USAF
Deputy Assistant to the Secretary
of Defense (Atomic Energy)

/s/ William H. Webster, date 2/21/80

William H. Webster, Director
Federal Bureau of Investigation

"Appendix A

"Definitions and Abbreviations

"Improvised Nuclear Device (IND) - Any nonconventional explosive device containing nuclear or radioactive material combined with explosives.

"Nuclear Threat Incident - Any situation involving stolen, lost, or unauthorized possession of source materials, special nuclear materials, radioactive by-products, nuclear weapons/devices of U.S. and/or foreign manufacture, improvised nuclear devices, radioactive dispersal devices, or the threatened use of said items.

"Explosive Ordnance Disposal (EOD) - The detection, identification, field evaluation, rendering-safe, recovery, and final disposal of Unexploded Explosive Ordnance (UXP).

"National Military Command Center (NMCC) - Centralized controlling and notification point to activate and coordinate DOD activities.

"Working Point - The area immediately surrounding the device.

"Special Nuclear Material - The term special nuclear material means (1) plutonium, uranium enriched in the isotope-233 or in the isotope-235, and any other material which DOE, pursuant to the provisions of section 51 of the Atomic Energy Act, as amended,

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 18 - 51

determines to be special nuclear material, but does not include source material or (2) any material artificially enriched by any of the foregoing, but does not include source material."

EFFECTIVE: 04/08/80

18-10

MEMORANDUM OF UNDERSTANDING BETWEEN THE DEPARTMENT OF
JUSTICE AND THE DEPARTMENT OF THE INTERIOR REGARDING
FEDERAL RESPONSE TO CIVIL DISORDER ON INDIAN RESERVATIONS

"The purpose of this agreement is to delineate the responsibilities of the various federal agencies for civil disorder control on Indian reservations in the United States and to identify basic command and control channels and general procedures for such operations. The policy contained herein shall apply to civil disorder situations arising on any Indian Reservation under federal law enforcement jurisdiction, either exclusive or concurrent.

"A current list of reservations and jurisdiction is attached to this agreement and will be updated from time to time as necessary by the Department of the Interior.

"For the purposes of this agreement, a civil disorder is defined as follows:

"The term 'civil disorder' means any public disturbance involving acts of violence by assemblages of three or more persons, which causes an immediate danger of or results in damage or injury to the property or person of any other individual." (18, USC, 12, Section 232(1))

"Nothing contained in this agreement shall be construed as in any manner limiting, modifying, or redefining the statutory and other investigative authority of the Federal Bureau of Investigation.

POLICY

"The Attorney General has been designated by the President as chief civilian officer for coordination of all federal government activities relating to civil disturbances, including acts of terrorism within the United States. However, it is the policy of the Attorney General that existing established law enforcement authority on Indian reservations will not be superseded or augmented by Department of Justice law enforcement resources and authority

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 18 - 52

unless absolutely necessary and then only at the request of the Secretary of the Interior or his designated representative.

"The primary responsibility for the law enforcement response to a civil disorder situation arising on an Indian reservation under Department of the Interior jurisdiction will rest exclusively with the Assistant Secretary - Indian Affairs or the Commissioner of Indian Affairs or his delegated representative.

"Where local resources are inadequate to deal with civil disorder, the Commander of specially trained Bureau of Indian Affairs law enforcement officers will act as the Commissioner's representative, will be responsible for restoring order. All Bureau of Indian Affairs law enforcement officers engaged in restoration of order on the reservation will operate under the command of the senior Special Operations Service Unit official on site.

"Whenever any civil disorder reaches a point beyond the control capabilities of local and Bureau of Indian Affairs resources, the Department of the Interior may elect to request assistance from the Department of Justice.

"Based upon a request for assistance by the Department of the Interior and an assessment of the civil disorder situation, the Attorney General or the Deputy Attorney General will determine what, if any, response is appropriate and shall so advise the Department of the Interior in a timely manner.

"If a decision is made to intervene, the Attorney General or Deputy Attorney General will order or request deployment of federal civilian or military forces. The selection of Department of Justice resources to be committed shall rest exclusively with the Attorney General or the Deputy Attorney General.

GENERAL PROCEDURES

"1. In the event of an actual or potential civil disorder on an Indian reservation under federal jurisdiction, the Bureau of Indian Affairs will take or direct appropriate law enforcement action and notify the nearest office of the Federal Bureau of Investigation.

"2. The Federal Bureau of Investigation (FBI) office notified will immediately report the incident to the FBIHQ in Washington. FBIHQ will immediately notify the Office of the Deputy Attorney General through the Department of Justice Emergency Programs Center.

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 18 - 53

"3. At this point civil disorder control responsibility rests solely with the Department of the Interior and any FBI special agents on site are responsible only for normally authorized investigative activity to the extent that such activity can be safely conducted and for keeping FBIHQ apprised of the disorder situation so that the Attorney General or Deputy Attorney General will be prepared to act quickly and effectively on any subsequent request for assistance.

"4. When the Department of the Interior determines that a civil disorder on an Indian reservation cannot be controlled or terminated by local or BIA resources and requests Department of Justice assistance, the Attorney General or the Deputy Attorney General will assess the situation and determine what response is appropriate. If a Department of Justice or other response is required, the selection of civil response resources to be employed shall rest exclusively with the Attorney General. If federal civilian resources are inadequate, military forces will be requested by the Department of Justice through established procedures.

"5. Upon arrival and deployment at the scene of a civil disorder, and at a time to be designated by the Attorney General or the Deputy Attorney General, the Attorney General's designee on site will assume operational control of the disorder situation and will be responsible for restoring order in accordance with established procedures and instructions.

"6. When the law enforcement resources designated by the Attorney General or the Deputy Attorney General assume control of a disorder situation the Secretary of the Interior will place his law enforcement resources at the site at the disposal of the Department of Justice designee.

"7. At a time to be mutually agreed upon by the Department of Justice and the Department of the Interior control of law enforcement activity at the scene of the civil disorder will be returned to the Department of the Interior.

"It is understood and agreed that a basic objective of this agreement is to ensure a coordinated and effective federal effort in response to incidents of civil disorder on Indian reservations. It is anticipated that this agreement will serve to eliminate delays in appropriate federal law enforcement action during periods of civil disorder and will clearly define basic law enforcement responsibilities, which will be further implemented through continuous development of contingency plans and procedures by the agencies involved.

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 18 - 54

FOR THE DEPARTMENT OF JUSTICE

FOR THE DEPARTMENT OF
THE INTERIOR

/s/ Charles B. Renfrew
CHARLES B. RENFREW
DEPUTY ATTORNEY GENERAL

/s/ Cecil D. Andrus

Dated: 1/20/81

Dated: 1/8/81"

"The following list of Indian Reservations was furnished by the
Department of the Interior, Bureau of Indian Affairs, Division of Law
Enforcement Services and represents those reservations as of 22
January 1981 that are included in the scope of this agreement.

Bureau of Indian Affairs
Division of Law Enforcement Services

BIA RESPONSIBILITY FOR LES BY STATE
AND RESERVATION/TRIBE

STATE

RESERVATION/TRIBE

1. Alaska (1)

2. Arizona (Incl. (18)
NM & Utah)

1. Annette Island

2. Navajo
3. Colorado River
4. Cocopah
5. Fort Mohave
6. Fort Yuma
7. Fort Apache
8. Kaibab
9. Hopi
10. Fort McDowell
11. Papago
12. Ak Chin (Maricopa)
13. Gila River
14. Salt River
15. San Carlos
16. Camp Verde
17. Havasupai
18. Hualapai
19. Yavapai-Prescott

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 18 - 55

- | | |
|---------------------|-------------------------------|
| 3. California (1) | 20. Tonto Payson |
| 4. Colorado (2) | 21. Hoopa/Yurok |
| 5. Florida (1) | 22. Southern Ute |
| 6. Idaho (4) | 23. Ute Mountain |
| | 24. Miccosukee |
| | 25. Fort Hall |
| | 26. Kootenai |
| | 27. Coeur D' Alene |
| | 28. Nez Perce |
| 7. Kansas (2) | 29. Kickapoo |
| | 30. Potawatomie |
| 8. Maine (3) | 31. Indian Township |
| | 32. Pleasant Point |
| | 33. Penobscot |
| 9. Michigan (5) | 34. Bay Mills |
| | 35. Hannahville |
| | 36. Keweenaw Bay |
| | 37. Saginaw-Isabella |
| | 38. Sault Ste. Marie |
| 10. Minnesota (2) | 39. Nett Lake |
| | 40. Red Lake |
| 11. Mississippi (1) | 41. Choctaw |
| 12. Montana (7) | 42. Blackfeet |
| | 43. Crow |
| | 44. Flathead |
| | 45. Fort Belknap |
| | 46. Fort Peck |
| | 47. Northern Cheyenne |
| | 48. Rocky Boys |
| 13. Nebraska (1) | 49. Omaha |
| 14. Nevada (26) | 50. Battle Mountain
Colony |
| | 51. Campbell Ranch |
| | 52. Carson Colony |

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 18 - 56

53. Duck Valley
Reservation
54. Duck Water
Reservation
55. Dresslerville
Colony
56. Elko Colony
57. Fallon Colony
58. Fort McDermitt
Reservation
59. Goshute Reservation
60. Las Vegas Colony
61. Lovelock Colony
62. Moapa Reservation
63. Odgers Ranch
64. Pyramid Lake
Reservation
65. Reno-Sparks Colony
66. Ruby Valley
Reservation
67. South Fork
Reservation
68. Summit Lake
Reservation
69. Walker River
Reservation
70. Washoe Pinenut
Allotments
71. Washoe Ranches
72. Winnemucca Colony
73. Woodfords Community
74. Yerington Colony
75. Yomba Reservation

15. New Mexico (22)

76. Jicarilla
77. Mescalero
78. Nambe Pueblo
79. Picuris Pueblo
80. Pojoaque Pueblo
81. San Ildefonso
Pueblo
82. San Juan Pueblo
83. Santa Clara Pueblo
84. Taos Pueblo
85. Tesuque Pueblo
86. Acoma Pueblo

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 18 - 57

- | | |
|------------------------|------------------------------|
| | 87. Cochiti Pueblo |
| | 88. Isleta Pueblo |
| | 89. Jemez Pueblo |
| | 90. Laguna Pueblo |
| | 91. Sandia Pueblo |
| | 92. San Felipe Pueblo |
| | 93. Santa Ana Pueblo |
| | 94. Santo Domingo Pueblo |
| | 95. Zia Pueblo |
| | 96. Zuni Pueblo |
| | 97. Ramah-Navajo |
| 16. North Carolina (1) | 98. Eastern Cherokee |
| 17. North Dakota (3) | 99. Fort Berthold |
| | 100. Fort Totten |
| | 101. Turtle Mountain |
| 18. Oklahoma (10) | 102. Absentee-Shawnee |
| | 103. Apache |
| | 104. Caddo |
| | 105. Cheyenne-Arapaho Tribe |
| | 106. Comanche |
| | 107. Delaware |
| | 108. Kiowa |
| | 109. Pawnee Tribe |
| | 110. Ponca Tribe |
| | 111. Wichita |
| 19. Oregon (3) | 112. Warm Springs |
| | 113. Burns Paiute Allotments |
| | 114. Umatilla |
| 20. South Dakota (9) | 115. Cheyenne River |
| | 116. Crow Creek |
| | 117. Flandreau |
| | 118. Lower Brule |
| | 119. Pine Ridge |
| | 120. Rosebud |
| | 121. Sisseton |
| | 122. Yankton |
| | 123. Standing Rock (Inc. ND) |

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 18 - 58

21. Utah (2)

22. Washington (25)

23. Wisconsin (1)

24. Wyoming (1)

124. Skull Valley
125. Uintah and Ouray

126. Chehalis
127. Colville
128. Hoh
129. Kalispel
130. Lower Elwah
131. Lummi
132. Makah
133. Muckleshoot
134. Nisqually
135. Nooksack
136. Ozette
137. Port Gamble
138. Puyallup
139. Quileute
140. Quinault
141. Sauk-Suiattle
142. Shalwater
143. Skokomish
144. Spokane
145. Squaxon Island
146. Suquamish (Port
Madison)
147. Swinomish
148. Tulalip
149. Upper Skagit
150. Yakima

151. Menominee

152. Wind River

TOTALS: 24 States - 152 Reservations"

EFFECTIVE: 03/09/81

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 18 - 59

18-11 MEMORANDUM OF UNDERSTANDING AND COORDINATION BETWEEN THE
FEDERAL AVIATION ADMINISTRATION AND THE FEDERAL BUREAU OF
INVESTIGATION

"I. INTRODUCTION

"The enactment of Public Law 93-366, on August 5, 1974, affects the responsibility of the Federal Aviation Administration for the direction of law enforcement activity in aircraft hijacking situations. New Section 316(c), entitled "Overall Federal Responsibility," states:

"1. Except as otherwise specifically provided by law, no power, function, or duty of the Administrator of the Federal Aviation Administration under this section shall be assigned or transferred to any other Federal department or agency.

"2. Notwithstanding any other provision of law, the Administrator of the Federal Aviation Administration shall have exclusive responsibility for the direction of any law enforcement activity affecting the safety of persons aboard aircraft in flight involved in the commission of an offense under Section 902(i) or 902(n) of this act. Other Federal departments and agencies shall, upon request by the Administrator, provide such assistance as may be necessary to carry out the purposes of this paragraph.

"3. For the purposes of this subsection, an aircraft is considered in flight from the moment when all external doors are closed following embarkation until the moment when one such door is opened for disembarkation.

"In view of these and other changes in the scope of federal responsibility, the Memorandum of Understanding, dated September 25, 1970, between the Attorney General and the Secretary of Transportation is no longer sufficient and is hereby superseded. In its place, the following statements of authority and responsibilities are agreed upon.

"II. DESIGNATION OF AUTHORITY

"A. When the aircraft is in flight.

"1. When a aircraft is in flight, that is from the moment

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 18 - 60

when all external doors are closed following embarkation, until the moment when one such door is opened for disembarkation, the pilot in command of the aircraft shall have normal operational control of the flight.

"2. The Administrator of the Federal Aviation Administration has exclusive responsibility for direction of any law enforcement activity involving an offense under (902(i) and 902(n) of the Federal Aviation Act of 1958, as amended.

3. As appropriate, in each case involving such an offense, the designated official of the Federal Aviation Administration shall request the assistance of the designated official of the Federal Bureau of Investigation.

"4. After fully considering the expressed wishes of the pilot in command, the responsible official of the airline operating the aircraft and the designated official of the Federal Bureau of Investigation, the designated official of the Federal Aviation Administration shall determine if law enforcement action is appropriate. In those instances in which the designated official of the Federal Aviation Administration determines that law enforcement action is appropriate, he shall request the designated official of the Federal Bureau of Investigation to advise as to the appropriate methods to be used and, after approval of the designated official of the Federal Aviation Administration, take the law enforcement action that is required.

"5. Whenever such a request is made, the designated official of the Federal Bureau of Investigation shall provide such law enforcement assistance as is necessary.

"6. The designated official of the Federal Bureau of Investigation and the designated official of the Federal Aviation Administration shall maintain continuing coordination between their respective offices during the course of such law enforcement activity.

"B. When the aircraft is not in flight.

"1. When an aircraft is not in flight, that is prior to the moment when all external doors are closed after

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 18 - 61

embarkation and after the moment when one such door is opened for disembarkation, the designated official of the Federal Bureau of Investigation shall make the decision to take law enforcement action with respect to a hijacking. The designated official of the Federal Bureau of Investigation shall give full consideration to the expressed wishes of the pilot in command, the responsible official of the airlines operating the aircraft, and the designated official of the Federal Aviation Administration prior to initiating action.

"C. The decision of the designated official of the Federal Aviation Administration shall prevail in those instances where a question arises as to whether an aircraft is in flight or is not in flight.

"III. INFORMATION AND COOPERATION

"A. The Federal Aviation Administration shall take all possible steps to establish a comprehensive information and intelligence communications network. To achieve this objective, the fullest cooperation of the commercial airlines and their pilots will be solicited.

"B. The Federal Aviation Administration and the Federal Bureau of Investigation agree to cooperate fully with each other in order that each agency may discharge its responsibilities hereunder. This shall include the full exchange of information and intelligence.

"IV. DELEGATION OF AUTHORITY AND DESIGNATION OF OFFICIAL OF THE FEDERAL AVIATION ADMINISTRATION AND THE FEDERAL BUREAU OF INVESTIGATION

"A. Until the Federal Aviation Administrator is otherwise notified in writing by the Director of the Federal Bureau of Investigation, JAMES B. ADAMS, Assistant to the Director, Deputy Associate Director, or the official acting in his capacity, will act on behalf of the Federal Bureau of Investigation and will coordinate with the Federal Aviation Administration and its designated responsible officials.

"B. Until the Director of the Federal Bureau of Investigation is otherwise notified in writing by the Federal Aviation Administrator, RICHARD F. LALLY, Director, Civil Aviation Security Service, or the official acting in his capacity, will act on behalf of the Federal Aviation Administration and will coordinate with the

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 18 - 62

Federal Bureau of Investigation and its designated responsible officials.

"Dated at Washington, D.C. this ____26th____ day of February, 1975.

/s/ Alexander P. Butterfield
Administrator
Federal Aviation
Administration

/s/ Clarence M. Kelley
Director,
Federal Bureau of
Investigation"

EFFECTIVE: 01/08/82

18-12 MEMORANDUM OF UNDERSTANDING BETWEEN THE FEDERAL BUREAU OF
INVESTIGATION AND OFFICE OF INSPECTOR GENERAL RESOLUTION
TRUST CORPORATION

"This memorandum constitutes an agreement voluntarily entered into between the Office of the Inspector General (OIG) of the Resolution Trust Corporation (RTC), and the Federal Bureau of Investigation (FBI).

"A. PURPOSE

"The purpose of this memorandum is to delineate the investigative responsibilities of the FBI and the OIG-RTC to ensure the most effective and efficient utilization of the limited resources which are available, and to ensure the timely exchange of information regarding allegations of criminal conduct involving RTC employees, programs, and functions.

"B. APPLICABLE AUTHORITY

"The Inspector General Act of 1978 ("IG ACT"), Public Law 95-452 (5

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 18 - 63

USC App.), created OIGs with the statutory authority to conduct investigations relating to fraud, waste, and abuse within their respective agencies' programs and operations. The Financial Institution Reform, Recovery, and Enforcement Act of 1989 (P. L. 101-73) (FIRREA) amended the IG Act to add an Inspector General for the RTC.

"The FBI derives its criminal investigative jurisdiction from Titles 18 and 28 of the United States Code (USC), the Code of Federal Regulations and through the Attorney General of the United States.

"Section 535 of Title 28, USC, specifically sets forth the FBI's jurisdiction to investigate violations of Title 18 involving Government officers and employees. Further, this statute also imposes upon every department and agency head of the Executive Branch of the Government a duty to report expeditiously to the Attorney General any information, allegations, or complaints relating to possible violations of Title 18 involving officers or employees of the Government unless the responsibility to perform the investigation of that violation is, by law, specifically assigned otherwise.

"C. BACKGROUND

"The Attorney General has formulated a written policy statement for the Department of Justice (DOJ) regarding its relationship and coordination with the statutory Inspectors General. The policy states in part, that the Attorney General is the chief law enforcement officer of the United States. Further, that whenever there is reason to believe that a Federal crime has occurred, the DOJ should be advised. This reporting normally will be to the United States Attorney (USA) in the district where the crime occurred or is occurring.

"In order to comply with the Attorney General's reporting requirement, the FBI and the OIG-RTC agree to present all allegations of a violation of Federal criminal statutes to the USA's Office in the district where the crime occurred or is occurring. The presentation to the USA will occur within 30 days of receipt of the information indicating a criminal violation, for the purpose of obtaining a preliminary prosecutive opinion.

"The FBI and the OIG-RTC further agree to advise each other of the initiation of any criminal investigation involving RTC employees, programs or functions and/or individuals and contractors acting for or on behalf of the RTC. The notification shall be in writing and will occur within 30 days of the initiation of a criminal investigation.

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 18 - 64

The notification shall include the predication for initiating the investigation, any facts developed, any evidence obtained, and the initial prosecutive opinion rendered by the USA's Office.

"The FBI and the OIG-RTC further agree to advise each other of the final results of those criminal investigations involving RTC employees, programs or functions. The notifications of the initiation of investigation and the final results of an investigation shall be made both to the field office covering the territory where the criminal activity took place and to the headquarters of both the FBI and the OIG-RTC.

"The reciprocal notifications will allow each agency to be informed of investigations being conducted by the other agency, thereby facilitating coordination of investigative efforts and avoiding duplication of effort. In addition, each agency may request to join an investigation being conducted by the other agency. The investigating agency may, however, decide to conduct the investigation unilaterally.

"The above reciprocal notifications shall not apply to those investigations where disclosure might endanger the safety of FBI, OIG-RTC, or other personnel, or otherwise have a potentially adverse impact upon the investigation.

"The FBI and the OIG-RTC agree to obtain the approval of one another prior to disseminating the other agency's documents to a third agency.

"D. RESPONSIBILITIES OF THE OIG-RTC

"1. The OIG will promptly advise the FBI upon the initiation of all criminal investigations undertaken by the OIG-RTC involving employees, programs, and functions of RTC and/or individuals and contractors acting for or on behalf of RTC. The OIG-RTC will provide the FBI with a list of regional OIG-RTC offices and ensure that any changes to the list of offices are provided to the FBI on a timely basis.

"2. The OIG will refer to the FBI, for investigation, all allegations of bribery or attempted bribery involving RTC employees and other individuals and/or contractors acting for or on behalf of RTC, upon receipt.

"3. The OIG will refer to the FBI for investigation all information pertaining to "organized crime," including both traditional La Cosa Nostra (LCN) matters and nontraditional criminal

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 18 - 65

enterprises identified in the FBI's National Organized Crime Strategy, upon receipt.

"4. The OIG will refer to the FBI, for investigation, all allegations of bank fraud and embezzlement which may have occurred prior to the date of "conservatorship."

"5. The OIG will investigate all noncriminal administrative and civil matters arising from and pertaining to RTC programs, functions, and personnel. Certain civil investigations arising from criminal cases investigated by the FBI may, however, be handled by the FBI. The OIG may institute whatever action is deemed appropriate in those instances where the FBI notifies the OIG that it is not going to initiate an investigation or that the USA has declined to prosecute a particular matter.

"E. RESPONSIBILITIES OF THE FBI

"1. The FBI will promptly advise the OIG-RTC upon the initiation of criminal investigations undertaken by the FBI involving employees, programs, and functions of RTC and/or individuals and contractors acting for or on behalf of RTC except in those situations articulated above. The FBI will also advise the OIG-RTC of the results of completed investigations as set forth above. The FBI will provide the OIG a list of all FBI field offices and ensure that changes to the list of field offices are provided to the OIG-RTC on a timely basis.

"2. The FBI will assume investigative responsibility for all allegations of bribery or attempted bribery involving RTC employees and other individuals and/or contractors working for or on behalf of RTC.

"3. The FBI will assume investigative responsibility for all allegations of criminal activity involving "organized crime" including traditional LCN matters and nontraditional criminal enterprises identified in the FBI's National Organized Crime Strategy. The FBI will promptly furnish the OIG-RTC a copy of the FBI's National Organized Crime Strategy and will promptly advise the OIG-RTC of any changes to the FBI's National Organized Crime Strategy.

"4. The FBI will assume investigative responsibility for all allegations of bank fraud and embezzlement which may have occurred prior to the date of "conservatorship."

"5. The FBI will advise the OIG whether or not it will

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 18 - 66

investigate a matter referred by the OIG within 45-60 days of the receipt of the information, except in matters of bribery and/or RTC employee involvement. In these latter situations, telephonic notifications should be made to the appropriate OIG-RTC Regional Inspector General for Investigation within 30 days.

"F. JOINT ENDEAVORS BY THE FBI AND THE OIG

"The OIG and FBI may agree to enter into joint investigative efforts, including undercover operations (UCO), in appropriate circumstances. Separate written agreements will be prepared for each joint undercover investigation, setting forth the respective responsibilities of each agency. All UCOS will conform to pertinent Attorney General and FBI guidelines. Control of joint UCOS will be the responsibility of the FBI.

"While differing circumstances will result in varied arrangements from project to project, certain conditions will remain constant. Participating personnel will be supervised by their respective agencies. Only one evidentiary document or report of interview will be prepared. Any contact with the news media, such as press releases, will be coordinated and agreed to in advance.

"G. REVISIONS/TERMINATION OF THIS AGREEMENT

"Both parties agree to consider any proposed changes to this agreement which would improve the working relationship between the FBI and the OIG-RTC. This agreement may be terminated at any time, by either party, by deliverance of a written notice to terminate.

"H. EFFECTIVE DATE

"This agreement becomes effective when approved and signed by both parties.

William M. Baker
ASSISTANT DIRECTOR
CRIMINAL INVESTIGATIVE DIVISION
FEDERAL BUREAU OF INVESTIGATION

John J. Adair
INSPECTOR GENERAL
RESOLUTION TRUST CORPORATION

10/21/91
DATE

October 30, 1991
DATE

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 18 - 67

EFFECTIVE: 04/30/93

18-13 MEMORANDUM OF UNDERSTANDING BETWEEN THE FEDERAL BUREAU OF INVESTIGATION, THE UNITED STATES MARSHALS SERVICE, AND THE FEDERAL BUREAU OF PRISONS ON VIOLATIONS OF THE FEDERAL ESCAPE AND RESCUE STATUTES

"I. PURPOSE: This Memorandum of Understanding (MOU) between the Federal Bureau of Investigation, hereinafter referred to as the FBI, the United States Marshals Service, hereinafter referred to as the USMS, and the Federal Bureau of Prisons, hereinafter referred to as the BOP, sets forth the responsibilities of each agency with regard to the apprehensions and investigations under the Federal Escape and Rescue Statutes (Title 18, United States Code (USC), Sections 751 through 757).

"II. GOALS: It is mutually agreed that a MOU should be established on the Federal Escape and Rescue Statute to ensure an effective and efficient federal response to escape incidents and to clarify Section D of the 1988 Attorney General 'Policy on Fugitive Apprehension in Federal Bureau of Investigation and Drug Enforcement Administration Cases.'

"It is mutually agreed that each participant in this MOU will coordinate, as appropriate, and fully share information and the fruits of their respective investigations to assist each in fulfilling its own mission and responsibilities concerning violations of the Federal Escape and Rescue Statute.

"III. IMPLEMENTATION: The FBI, the USMS, and the BOP will develop and exchange such additional instructions and operating procedures as are deemed necessary to the continued implementation of this MOU with the goal of a coordinated, efficient, and effective interagency response to escape violations.

"In accordance with the terms of this MOU, in those locations in which a federal correctional institution is situated, a single operational plan will be prepared by the three agencies which will address those issues unique to that location regarding resources, manpower, notification, etc. It will be prepared by and for the benefit of the affected personnel in each location who will be directly involved in any situation covered by this MOU. This operational plan will in no way circumvent or oppose the letter and

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 18 - 68

spirit of this MOU.

"IV. RESPONSIBILITIES:

"Federal Bureau of Investigation:

"A. The FBI will have apprehension responsibility and investigative jurisdiction for all violations of the Federal Escape and Rescue Statute (Title 18, USC, Sections 751-757), involving subjects of FBI investigations, up to and including the time of sentencing. The FBI will coordinate this apprehension and investigative responsibility with the USMS and the BOP, as appropriate.

"B. The FBI will maintain investigative responsibility for all violations encompassing conspiracies to violate the Federal Escape and Rescue Statute or the conspiracy statutes (Title 18, USC, Sections 371-373) covering escape/attempted escape as they concern federal penal institutions and detention centers.

"IT IS THEREFORE UNDERSTOOD THAT THE FBI SHALL:

"1. Assume apprehension responsibility for an escaped federal prisoner, from any facility, at any stage up to and including sentencing, who is the subject of an FBI substantive investigation, and/or the subject or member of an organization which is the subject of an existing FBI National Security, FBI Organized Crime, or FBI Terrorism investigation.

"2. Maintain investigative jurisdiction over all conspiracy, rescue, facilitation, incitement, or aid to escape or attempt to escape, where the escape or attempt occurs within/from a federal penal institution/detention center.

"3. The FBI will be immediately notified by the BOP and/or the USMS whenever an escape occurs from a federal facility and circumstances arise indicating a conspiracy to escape/attempted escape; the introduction of a firearm/contraband into a federal facility; corrupt and/or collusion of correctional facility personnel; acts of riot or mutiny; or acts of violence, death or serious bodily injury. Coordination will be implemented and maintained with the USMS, who will exercise apprehension responsibility for non-FBI subjects, and the BOP, as appropriate. Joint FBI and USMS/BOP investigation will be viewed as the optimum objective.

"4. The FBI will assume investigative responsibility

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 18 - 69

for conspiracy, rescue, facilitation, incitement, or aid to escape or attempt to escape, in violation of the Federal Escape and Rescue Statute (Title 18, USC, Sections 751-757) when the escape occurs within/from a nonfederal institution and involves riot, hostage taking or loss of life. Coordination will be implemented and maintained with the USMS and BOP. Joint FBI and USMS investigation will be viewed as the optimum objective.

"5. Facilitate USMS participation in, and joint investigation of, escape and conspiracy to escape cases where the FBI has investigative jurisdiction and the USMS has prisoner, transport, or court security responsibilities.

"6. Establish and maintain investigative liaison with the USMS, the BOP and other federal and local law enforcement agencies as appropriate.

"7. Establish and maintain coordination with the USMS when an escaped federal prisoner becomes the subject of an Unlawful Flight to Avoid Prosecution (UFAP) request to the FBI. The FBI will not seek a UFAP warrant against any fugitive sought by the USMS pursuant to the Federal Escape and Rescue Statute and will notify the requesting state or local authority of the USMS's interest.

"United States Marshals Service:

"A. Pursuant to 28 C.F.R 0.111(q), which delegates to the USMS the power and authority vested in the Attorney General to conduct and investigate fugitive matters, domestic and foreign, involving escaped federal prisoners, the USMS will maintain investigative jurisdiction for all violations of the Federal Escape and Rescue Statute (Title 18, USC, Sections 751-757).

"IT IS THEREFORE UNDERSTOOD THAT THE USMS SHALL:

"1. The USMS and the FBI agree that the FBI will have investigative and apprehension responsibility with regard to violations of the Federal Escape and Rescue Statute involving subjects of FBI investigations, up to and including the time of sentencing, or persons who are the subject of or were members of an organization which is the subject of an existing FBI National Security, Organized Crime or Terrorism investigation.

"2. If the USMS's investigation reveals a possible escape conspiracy or systemic corruption on the part of federal personnel, concerning a federal penal institution or an FBI subject,

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 18 - 70

that information will be shared with the FBI for their investigation of the conspiracy or irregularities matter.

"3. The USMS will have investigative and apprehension responsibility for all violations of the Federal Escape and Rescue Statute within/from state, county or city (contract) facilities in all cases other than presentenced FBI prisoners. In the event of a violation of the Escape and Rescue Statute within/from a state, county or city (contract) facility, the facility will immediately notify the USMS. The USMS will then notify the FBI if the escape or attempted escape involved a presentenced FBI prisoner or if the incident involves riotous behavior, hostage taking or loss of life.

"4. Inasmuch as the USMS and the FBI agree that a full sharing of information and the fruits of investigations benefit each agency in fulfilling its missions and responsibilities, the USMS and FBI will coordinate and bring to bear the two agencies' combined expertise and investigative resources upon escaped federal prisoners and their conspirators.

"Bureau of Prisons:

"A. The BOP will have investigative responsibility for all escape issues until the agency (FBI or USMS), having been notified in accordance with provisions set forth in this agreement, has arrived on site and is prepared to assume the investigative role.

"B. In that the BOP will ordinarily be the agency which will first discover indications of an escape conspiracy or actual escape event, the BOP recognizes the obligation to take initial steps to manage the crime scene appropriately and to make immediate notifications to the agency assuming the lead investigative role.

"IT IS THEREFORE UNDERSTOOD THAT THE BOP SHALL:

"1. Take immediate steps to preserve the crime scene, as well as any related audit trails, record systems, and other forms of evidence as appropriate. Upon on-site arrival of representatives of the agency assuming jurisdiction, the BOP will assume a joint-jurisdiction supporting role, and provide full access to the crime scene and all related evidence and records systems. In the event the designated agency cannot immediately respond, a mutual agreement will be sought regarding the full processing and release of the crime scene by BOP investigative staff.

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 18 - 71

"2. In the event of an actual escape, or suspected escape, the BOP will activate stationary escape posts, roving patrols, and special response units as necessary to establish an extended perimeter around the BOP facility as may be dictated by local terrain, potential routes of egress, and the proximity of population centers. Active immediate apprehension activities in the surrounding area shall continue until such time as the BOP Warden or CEO concludes that the fugitive(s) is(are) no longer in the immediate area of the BOP facility, and/or the responding agency has sufficient resources actually in place to assume the immediate apprehension role. The BOP will provide the responding agency with appropriate information regarding the nature and location of BOP immediate apprehension activities.

"3. In those cases where an escape conspiracy is identified by BOP staff, prompt notification shall be made to the FBI, and a joint-investigative plan shall be developed, with the FBI assuming lead role as appropriate. BOP investigative staff shall provide full access to evidence, record systems, and audit trails as appropriate to facilitate the investigative process.

"4. In all escape investigations that involve inmate telephone monitoring tapes, investigative access shall be provided in strict accordance with procedures established by the Department of Justice, Office of Enforcement Operations, as implemented by BOP policy.

"V. PROTOCOL: It is agreed that the contents of this MOU will be provided to all agencies involved in this agreement, as well as the Executive Office of the United States Attorney, so as to fully coordinate notification procedures, points of contact to facilitate liaison, crime-scene management procedures, and development of the criminal investigation.

"VI. STANDARD PROCEDURES:

"A. Initial Notification

"1. The BOP will immediately notify the FBI in the event of any incident involving a violation of the Federal Escape and Rescue Statute.

"2. The FBI will immediately notify the USMS of any escape from a federal facility, pursuant to the USMS' apprehension responsibilities as stated in this MOU. The FBI will coordinate, as appropriate, with the USMS and BOP pursuant to this MOU.

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 18 - 72

"3. The USMS will immediately advise the nearest FBI office of escape incidents involving nonfederal penal institutions where the escapee is an FBI subject or aggravated circumstances exist as described in USMS paragraph 3.

"B. Point of Contact

"1. The USMS, FBI, and the BOP shall each designate a point of contact to facilitate liaison and implementation of this MOU.

"2. Points of contact will be established with other involved federal agencies where appropriate.

VII. TERMS OF AGREEMENT:

"This MOU will take effect immediately upon signature of all parties.

"For the Federal Bureau of Investigation:

/s/ LOUIS J. FREEH
LOUIS J. FREEH
Director

June 24, 1994
Date

"For the United States Marshals Service:

/s/ EDUARDO GONZALEZ
EDUARDO GONZALEZ
Director

6/24/94
Date

"For the Federal Bureau of Prisons:

/s/ KATHLEEN M. HAWK
KATHLEEN M. HAWK
Director

6/24/94
Date

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 18 - 73

EFFECTIVE: 09/30/94

18-14 MEMORANDUM OF UNDERSTANDING BETWEEN THE UNITED STATES
DEPARTMENT OF THE INTERIOR BUREAU OF INDIAN AFFAIRS AND
THE UNITED STATES DEPARTMENT OF JUSTICE FEDERAL BUREAU OF
INVESTIGATION

"I. PURPOSE

"This Memorandum of Understanding (MOU) is made by and between the United States Department of the Interior (DOI) and the Department of Justice (DOJ) pursuant to the Indian Law Enforcement Reform Act (Act), 25 U.S.C. 2801 et seq. The purpose of this MOU is to establish guidelines regarding the respective jurisdictions of the Bureau of Indian Affairs (BIA) and the Federal Bureau of Investigation (FBI) in certain investigative matters, and to provide for the effective and efficient administration of criminal investigative service in Indian country.

"II. BUREAU OF INDIAN AFFAIRS JURISDICTION

"The Act establishes a Branch of Criminal Investigations within the Division of Law Enforcement (DLE) of the BIA, which shall be responsible for providing, or for assisting in the provision of, law enforcement services in Indian country. The responsibilities of the DLE shall include, inter alia, the enforcement of federal law and, with the consent of the Indian Tribe, Tribal law; and in cooperation with appropriate federal and Tribal law enforcement agencies, the investigation and presentation for prosecution of cases involving violations of 18 U.S.C. 1152 and 1153 within Indian country (and other federal offenses for which the parties have jurisdiction). In addition, the Act authorizes the Secretary of the Interior to develop interagency agreements with the Attorney General and provides for the promulgation of prosecutorial jurisdictional guidelines by United States Attorneys (USA).

"III. FEDERAL BUREAU OF INVESTIGATION JURISDICTION

"The FBI derives its investigative jurisdiction in Indian country from 28 U.S.C. 533, pursuant to which the FBI was given investigative responsibility by the Attorney General. Except as provided in 18 U.S.C. 1162 (a) and (c), the jurisdiction of the FBI

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 18 - 74

includes, but is not limited to, certain major crimes committed by Indians against the persons or property of Indians and non-Indians, all offenses committed by Indians against the persons or property of non-Indians and all offenses committed by non-Indians against the persons or property of Indians. See 18 U.S.C. 1152 and 1153.

"IV. GENERAL PROVISIONS

"1) Each USA whose criminal jurisdiction includes Indian country shall develop local written guidelines outlining responsibilities of the BIA, the FBI, and Tribal Criminal Investigators, if applicable. Local USA guidelines shall cover 18 U.S.C. 1152 and 1153 offenses and other federal offenses within the investigative jurisdiction of the parties to this MOU.

"2) Any other agreements that the DOI, DOJ and Indian Tribes may enter into with or without reimbursement of personnel or facilities of another federal, Tribal, state, or other government agency to aid in the enforcement of criminal laws of the United States shall be in accord with this MOU and applicable federal laws and regulations.

"3) The Secretary will ensure that law enforcement personnel of the BIA receive adequate training, with particular attention to report writing, interviewing techniques and witness statements, search and seizure techniques and preservation of evidence and the crime scene. Successful completion of the basic Criminal Investigator course provided by the Department of the Treasury at the Federal Law Enforcement Training Center or its equivalent shall constitute the minimum standard of acceptable training. The BIA may consult with the FBI and other training sources with respect to such additional specialized training as may be desirable. United States Attorneys may also require, and participate in, training at the field level.

"4) Any contracts awarded under the Indian Self-Determination Act to perform the function of the BIA, Branch of Criminal Investigations, must comply with all standards applicable to the Branch of Criminal Investigations, including the following:

"a) Local USA guidelines must be followed.

"b) Criminal Investigators must be certified Peace Officers and must have satisfactorily completed the basic Criminal Investigator course provided by the Department of the Treasury at the Federal Law Enforcement Training Center, or an equivalent course

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 18 - 75

approved by the Commissioner of Indian Affairs. Criminal Investigators will receive a minimum of 40 hours in-service training annually to keep abreast of developments in the field of criminal investigations.

"c) Compensation for Criminal Investigators must be comparable to that of BIA Criminal Investigators.

"d) Criminal Investigators must be United States citizens.

"e) Criminal Investigators must possess a high school diploma or its equivalent.

"f) No Criminal Investigator shall have been convicted of a felony offense or crime involving moral turpitude.

"g) Criminal Investigators must have documentation of semiannual weapons qualifications.

"h) Criminal Investigators must be free from physical, emotional, or mental conditions which might adversely affect their performance as law enforcement officers.

"i) Criminal Investigators must be certified by Tribal officials as having passed a comprehensive background investigation, including unannounced drug testing. Such examinations must be documented and available for inspection by the BIA.

"j) Appropriate procedures shall be devised to provide adequate supervision of Criminal Investigators by qualified supervisory personnel to ensure that investigative tasks are properly completed.

"k) When a Tribe is awarded a contract under the Indian Self-Determination Act, 25 U.S.C. 450 (a), there must be a "phase-in" period of not less than 180 days so as to ensure an orderly transition from one law enforcement agency to another. When a Tribe retrocedes its contract for the Criminal Investigator function, there must be a one-year time period from the date of request for retrocession, or a date mutually agreed upon by the BIA and the Tribe, for the BIA to prepare for reassuming the Criminal Investigation responsibility. All case files, evidence, and related material and documents associated with active and closed investigations must be turned over to the receiving criminal investigative agency, whether it be the BIA or a Tribe.

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 18 - 76

"l) Appropriate procedures shall be established with respect to the storage, transportation and destruction of, and access to, case files, evidence, and related documents and other material, with particular attention directed to the confidentiality requirements of 18 U.S.C. 3509(d) and Rule 6(e) of the Federal Rules of Criminal Procedure. Criminal Investigators shall follow these procedures at all times. Access to such material will be for official use only.

"m) Before any Tribe contracts for the Criminal Investigator function, the BIA and the Tribe must ensure that there is sufficient funding to cover the costs of a Criminal Investigator program including salary, equipment, travel, training, and other related expenses arising during both the investigation stage and the litigation stage of any case or matter covered by the contract.

"n) Tribal contractors must agree, and the BIA shall ensure, that there is an audit and evaluation of the overall contracted Criminal Investigator program at least every two years. Continuation of the contract shall be contingent upon successful completion of each audit and evaluation.

"o) Criminal Investigators are prohibited from striking, walking off the job, feigning illness, or otherwise taking any job action that would adversely affect their responsibility and obligation to provide law enforcement services in their capacity as Criminal Investigators.

"5) Any individual who is a holder of a BIA Deputy Special Officer Commission and performing duties as a Criminal Investigator must comply with the standards applicable to Criminal Investigators set forth in the preceding paragraph.

"6) When either the FBI or the BIA receives information indicating a violation of law falling within the investigative jurisdiction of the other agency, the agency receiving the information will notify the other agency. If either the FBI or the BIA declines to investigate a matter within the jurisdiction of both agencies, the other agency will be notified. The FBI and the BIA will attempt to resolve jurisdictional disputes at the field level. In the event the dispute cannot be resolved, it will be reviewed by each agency's respective headquarters for resolution.

"7) With respect to the use of sensitive investigative techniques, such as the nonconsensual interception of wire, oral or electronic communications and undercover operations involving any

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 18 - 77

sensitive circumstance (as defined in the Attorney General's Guidelines for FBI Undercover Operations), and the investigation of organized crime matters, the FBI shall be the agency primarily responsible. Undercover operations involving sensitive circumstances shall be conducted in accordance with the Attorney General's Guidelines for FBI Undercover Operations. This paragraph is not intended to prohibit the BIA from conducting consensual eavesdropping or undercover operations not involving a sensitive circumstance or utilizing other nonsensitive investigative techniques after proper training and when authorized by the appropriate United States Attorney.

"8) Nothing in this MOU is intended to change any existing cooperative relationships and responsibilities between the BIA and the FBI, and nothing in this MOU shall invalidate or diminish any law enforcement authority or responsibility of either agency.

"9) Consistent with the availability of resources, the FBI will offer specialized training to the BIA.

"10) Consistent with limitations regarding confidentiality, the requirements of the Privacy Act and any other applicable laws, and respective policies and procedures, the BIA and the FBI will cooperate on investigative matters of mutual interest, exchange intelligence, and investigative reports, as appropriate.

"11) To the extent possible and in consideration of limited resources, the FBI will continue to assist the BIA in its investigative matters by providing investigative support services through the Identification Division, Training Division, Criminal Investigative Division and Laboratory Division.

"This document constitutes the full and complete agreement between the BIA and the FBI. Modifications to this MOU will have no force and effect unless and until such modifications are reduced to writing and signed by an authorized representative of the parties thereto. This MOU will, at regular intervals, be subjected to a thorough review to determine if changes are appropriate.

"The provisions set forth in this MOU are solely for the purpose of internal guidance of components of the Department of the Interior and the Department of Justice. This MOU does not, is not intended to, shall not be construed to, and may not be relied upon to, create any substantive or procedural rights enforceable at law by any party in any matter, civil or criminal. This MOU does not, is not intended to, and shall not be construed to, exclude, supplant or limit otherwise

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 18 - 78

lawful activities of the Department of the Interior or the Department of Justice.

"By subscription of their signatures below, the parties acknowledge that they have read, understand, and will abide by the foregoing statements.

" BRUCE BABBITT
Secretary

September 3, 1993
Date

United States Department of the Interior

" JANET RENO
Attorney General

November 22, 1993
Date

United States Department of Justice"

EFFECTIVE: 11/07/94

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 20 - 1

SECTION 20. WHITE COLLAR CRIME

20-1 DEFINITION

(1) White-Collar Crimes are defined as those illegal acts characterized by deceit, concealment, violation of trust, and not dependent upon the application or threat of physical force or violence. They are committed to obtain money, property, or services; or to avoid the payment or loss of money, property, or services; or to secure personal or business advantage.

(2) By focusing on the nature of the act, rather than the nature of the violator, the classification of the crime will more clearly emerge. The modus operandi and objectives are crucial to correct categorization of these acts.

(3) The White-Collar Crime is usually of a more complex or sophisticated nature.

(4) The White-Collar criminal can come from all walks of life. The classic image of such a person being of top management and/or the pillar of the community is not sufficiently large to embrace all such criminals. Conversely, a person of the classic image is capable, and indeed has, committed crimes of the most base nature.

(5) The crime may be committed by individuals acting independently or by those who are part of a well-planned conspiracy. Clearly a person clothed in the aura of respectability acting in concert with a hardened criminal in a conspiracy which would involve the violation of his/her trust, would attach to that crime the significance and character of the "White-Collar Crime."

EFFECTIVE: 01/21/86

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 20 - 2

20-2 POLICY

(1) Since "White-Collar Crime" is a generic term and cannot be defined in terms of statutory elements as are specific crimes within FBI jurisdiction, the definition of White-Collar Crimes has been established as a working definition solely for Bureau use.

(2) Many crimes which have been investigated by the FBI for years can, quite properly, be classified as White-Collar Crimes. So too, many local and state violations are considered White-Collar Crimes. Care should be taken not to evaluate local crimes under the Bureau definition since the Bureau in no way intends to impose its definition of White-Collar Crimes upon state and local jurisdictions.

(3) The policy covering the specific classifications of the statutes under investigation will prevail in all White-Collar Crime matters and no statement within this Section should be construed as changing or modifying the policy in any of the substantive investigative matters handled by the Bureau.

(4) All investigations characterized as White-Collar Crimes should be given a high priority of investigative attention with the assignment of sufficient personnel to ensure the Bureau's investigative responsibilities are promptly met.

(5) Since many of the classifications within the Bureau's investigative jurisdiction fall within the general category of accounting type, those Special Agent Accountants and Special Agents with accounting backgrounds should be utilized where this specific expertise is needed.

EFFECTIVE: 11/20/90

20-3

FBI WHITE-COLLAR CRIME PROGRAM (WCCP) (See MIOG, Part I, 46-1.14, 58-10, 139-9, 206-6, 207-2, 255-9, 257-11, 258-8, 264-9, 272-6.2, 275-1; MAOP, Part II, 3-1.1, 3-1.2, 3-3.2(3), 3-4.5(5), 10-23; Correspondence Guide - Field, 1-17.)

(1) The Criminal Investigative Division at FBIHQ administers the WCCP in the White-Collar Crimes Section.

(2) The White-Collar Crimes Section is comprised of five subprograms: Governmental Fraud; Public Corruption; Financial

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 20 - 3

Institution Fraud; Economic Crimes; and Other WCC Matters.

(3) The classifications comprising the WCCP are grouped
as follows:

(a) Governmental Fraud Matters

- 17 Department of Veterans Affairs Matters
- 46 Fraud Against the Government
- 60 Antitrust
- 62 Lands Division Matter
- Miscellaneous - Civil Suits
- 83 Claims Court
- 86 Small Business Administration Matters
- 93 Ascertaining Financial Ability
- 120 Federal Tort Claims Act
- 131 Admiralty Matter
- 147 Housing and Urban Development Matters
- 187 Privacy Act of 1974 - Criminal
- 206 Department of Defense Matters
- 206 Department of Agriculture Matters
- 206 Department of Commerce Matters
- 206 Department of Interior Matters
- 207 Environmental Protection Agency Matters
- 207 National Aeronautics and Space
Administration Matters
- 207 Department of Transportation Matters
- 207 Department of Energy Matters
- 208 General Services Administration Matters
- 209 Health|Care Fraud|
- 210 Department of Labor Matters
- 213 Department of Education Matters
- 249 Environmental Crimes

(b) Public Corruption Matters

- 51 Jury Panel Investigations
- 56 Election Law Violations
- 58 Corruption of Federal Public Officials
- 62 Administrative Inquiries
- 139 Interception of Communications - Public
Officials or Government Agencies
- 139 Interception of Communications - All Others
- 194 Corruption of State and Local Public
Officials
- 205 Foreign Corrupt Practices

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 20 - 4

211 Ethics in Government Matters

(c) Deleted

(d) Financial Institution Fraud

- 29 Financial Institution Fraud
- 275 Adoptive Forfeiture Matter - White Collar Crime

(e) Economic Crimes

- 27 Patent Matters
- 28 Copyright Matters
- 36 Mail Fraud
- 49 Bankruptcy Fraud Matters
- 87 Securities Trafficking and Check Matters
- 139 Interception of Communications/Signal Theft
- 181 Consumer Credit
- 186 Real Estate Settlement Procedures
- 196 Fraud by Wire
- 255 Counterfeiting of State and Corporate Securities
- 257 Trademark Counterfeiting Act
- 258 Credit and/or Debit Card Fraud
- 264 Computer Fraud and Abuse
- 272B Money Laundering - White-Collar Crime Program

(f) Other Matters

- 69 Contempt of Court
- 72 Obstruction of Justice
- 74 Perjury
- 75 Bondsmen and Sureties
- 137 WCC Informants
- 232 Training Received - White-Collar Crime

EFFECTIVE: 11/12/93

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 20 - 5

20-4 PRIORITY AMONG OTHER FBI PROGRAMS

| See MIOG, | Introduction, Section 2. |

EFFECTIVE: 09/27/93

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 21 - 1

SECTION 21. FUGITIVE - GENERAL

21-1 FUGITIVE DEFINITION

A "fugitive" is the subject of a Bureau investigation for whom a Federal arrest warrant has been issued and whose whereabouts is unknown; or an individual whose whereabouts is unknown and whom the Bureau, by directive or agreement, has the responsibility for apprehending. A subject otherwise meeting these criteria who is outside the United States is considered a fugitive regardless whether he/she is in custody or not until such time as he/she is returned to United States control in the United States.

EFFECTIVE: 07/23/90

21-2 "A," "B," "C," AND "D" FUGITIVE PRIORITIES (See MIOG, Part I, 88-7.2; MAOP, Part II, Section 10.)

(1) To reflect investigative importance in the fugitive area, all fugitives will be designated either an "A," "B," "C," or "D" priority.

(2) An "A" fugitive is a subject wanted for crimes of violence against the person, such as murder, manslaughter, forcible rape, robbery, aggravated assault and felony residential burglary; one convicted of such a crime within the past five years or one who has been incarcerated after conviction for a crime of violence and escapes from custody or supervision (parole, probation) prior to completion of their sentence or term of supervision.

(3) A "B" fugitive is a subject wanted for a crime involving the loss or destruction of property valued in excess of \$25,000, one being sought for criminal charges involving in excess of two ounces of heroin or cocaine, 1,000 pounds of marijuana or 10,000 dosage units of clandestinely manufactured dangerous or hallucinogenic drugs, or a subject convicted of the above crimes within the past five years or one who has been incarcerated after conviction for such offenses and escapes from custody or supervision (parole, probation) prior to completion of their sentence or term of supervision.

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 21 - 2

(4) "C." All others, except UFAP-Parental|Kidnapping| fugitives, who will be designated "D" fugitives.

(5) All communications, regardless of the fugitive classification, should carry the appropriate priority letter in parentheses in the title after the word, fugitive, which will identify the subject's priority ranking. For example:

JOHN DOE - FUGITIVE (A)
UFAP-MURDER
OO: Albany

JOHN DOE - FUGITIVE (C)
FAG
OO: Albany

(6) If a situation arises where a fugitive of a lower priority becomes wanted for an offense of a higher priority, the case should be promptly elevated to the newer appropriate priority letter ranking.

(7) The above priorities are by no means absolute in terms of significance of importance. Therefore, priority "C" may contain some relatively high-impact cases.

EFFECTIVE: 10/18/95

21-3 OBJECTIVES OF THE BUREAU'S FUGITIVE|SUBPROGRAM|

(1) To effect the swift location and apprehension of all FBI fugitives, particularly those wanted in connection with crimes of violence, substantial property loss or destruction, illicit drug trafficking and parental kidnaping.

(2) During liaison contact with law enforcement authorities and in managing resources available for fugitive investigations, "A," "B," and "D" priority fugitives should be emphasized so that manpower is concentrated there and not on those fugitive matters of lesser impact.

(3) All requests for assistance in the fugitive area over which we have jurisdiction must, of course, be honored regardless of their priority.

(4) Each office, in keeping with these objectives, should concentrate on the apprehension of "A" and "B" priority fugitives regardless of the Bureau classification, and "D" priority fugitives

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 21 - 3

(UFAP-Parental Kidnaping).

EFFECTIVE: 07/23/90

21-4 DETERMINING THE FUGITIVE'S FBI NUMBER AS A MEANS OF
POSITIVE IDENTIFICATION (See MIOG, Part II, 14-15.4; MAOP,
Part II, 7-2.2.2.)

(1) All offices should ensure that a check of the Interstate Identification Index (III) is made in an effort to determine the fugitive's FBI number prior to entering the fugitive in the NCIC Wanted Person File (WPF) without an FBI number. When the subject's fugitive airtel, FD-65, is submitted to FBIHQ at the outset of the fugitive investigation, his/her FBI number should be included thereon if known.

(2) If the field office is unable to identify an identification record identical with the fugitive through the III inquiry, an electronic communication should be forwarded to the Criminal Justice Information Services (CJIS) Division, West Virginia Operations (Attention: Module D-2 Answer Hits to Wants (AHTW)), enclosing any available fingerprints of the fugitive so that a technical fingerprint search can be conducted and a positive stop based upon fingerprints can be placed. A fingerprint-based stop means that incoming applicant/criminal fingerprint cards in alias names will hit against the stop thereby triggering appropriate field office notification(s). (See MIOG, Part II, 21-21(4).)

(3) "Maybe Ident" stops (a stop in an identification record possibly identical with the fugitive) will not be placed in identification records for FBI fugitives entered in the NCIC WPF without an FBI number. For fugitives entered in the NCIC WPF without an FBI number, a "Name Stop" only will be placed in the CJIS Division's Criminal File. If, while placing the "Name Stop," the CJIS Division discovers a manual record(s) (criminal identification record not available through III) possibly identical with the fugitive, a copy(s) of the criminal record(s) or a laminated copy(s) of the civil fingerprint card(s) will be forwarded to the field office. It will be the field office's responsibility to determine if the record or fingerprint card is identical with the fugitive. If an identification determination is made, the FBI number of the fugitive should be modified into his/her NCIC WPF entry or the copy of the civil print should be returned to the CJIS Division so a positive stop based upon fingerprints can be established in place of the existing "Name Stop."

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 21 - 4

(See MIOG, Part II, 21-23(22).)

EFFECTIVE: 05/13/96

21-5 POTENTIAL FUGITIVE IDENTITY PROBLEMS

EFFECTIVE: 05/26/89

21-5.1 Stolen or Lost Identification

(1) If it is known that a fugitive is using the stolen or lost identification of another individual, and said name is being carried as an alias of the subject in NCIC, the following action should be taken to prevent this individual from being detained erroneously as the subject.

(2) 

EFFECTIVE: 05/26/89

21-5.2 Look Alikes

(1) Where an individual has been reported to an office as being identical with a fugitive and investigation determines he/she is not identical but he/she so strongly resembles the fugitive in appearance that there is a likelihood he/she will be reported again as being identical with the fugitive, the office of origin and FBIHQ should be advised.

(2) Upon receipt of this information, the office of origin should modify the subject's NCIC record under the miscellaneous field to reflect that they are not identical.

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 21 - 5

EFFECTIVE: 05/26/89

21-6 FUGITIVES TRAVELING TOGETHER

When it is known that two or more subjects are traveling or operating together, their respective NCIC records should be cross-referenced under the miscellaneous field to reflect this fact. In addition, FBIHQ should be notified of this fact and the Criminal Justice Information Services Division, West Virginia Operations (Attention: Module D-2 AHTW), requested to cross-reference the fugitive stops in their respective fingerprint identification records.

EFFECTIVE: 05/13/96

21-7 CIRCUMSTANCES WHICH REQUIRE FBIHQ NOTIFICATION

In a fugitive investigation FBIHQ should be promptly notified if the following circumstances exist:

- (1) If there is any publicity or anticipated publicity regarding the fugitive investigation.
- (2) If the fugitive is prominent locally.
- (3) If good judgment dictates that FBIHQ should be notified of events.

EFFECTIVE: 03/20/86

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 21 - 6

21-8

DETERMINING THE OFFICE OF ORIGIN WHEN MORE THAN ONE OFFICE
PROCESS OUTSTANDING ON A FUGITIVE

(1) If an office, other than the existing office of origin, knowingly obtains additional process on a subject while in fugitive status, it should enter him/her in NCIC and bring this situation to the attention of FBIHQ and the existing office of origin in the following manner. Attach an administrative page to the fugitive airtel (FD-65) setting forth the details and request that FBIHQ determine and advise which office should assume origin in the investigation.

(2) There will be instances where an office, other than the existing office of origin, unknowingly obtains additional process on a subject while in fugitive status. This situation usually occurs when the subject has committed offenses under different identities. When subsequent investigation by the field determines that these individuals are in fact identical, FBIHQ should be promptly advised of the full details by airtel and requested to determine and advise which office should assume origin in the investigations.

EFFECTIVE: 03/20/86

21-9

COMMUNICATIONS REQUESTING APPREHENSION

The field office requesting investigation of an auxiliary office for the apprehension of a fugitive should include the following information in its communication if not previously furnished so that the investigation and apprehension may be handled intelligently and effectively:

- (1) Photograph and complete description of the subject.
- (2) Sufficient details of the offense charged to conduct a hearing before the U.S. Magistrate.
- (3) Amount of bond fixed by the court or recommended by the USA.
- (4) Date and place where prosecuting USA desires the bond made returnable.
- (5) Full name of the complainant (individual who signs complaint before U.S. Magistrate).

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 21 - 7

- (6) Full name of U.S. Magistrate or district court judge issuing the warrant.
- (7) Full name of USA who filed information or indictment.
- (8) Details of local offense in unlawful flight cases to handle any press inquiries.
- (9) Caution statement if appropriate.

EFFECTIVE: 03/20/86

21-10 FUGITIVE DEADLINES

(1) The following deadlines pertain to all fugitives regardless of the classification.

(2) Priority "A" and "D" Fugitives

(a) Fugitive leads in headquarters cities or in headquarters cities of resident agencies are to be covered and reported within a total of 15 calendar days.

(b) An additional 7 calendar days are permitted for areas outside these cities.

(3) Priority "B" and "C" Fugitives

(a) Fugitive leads in headquarters cities or in headquarters cities of resident agencies are to be covered and reported within a total of 30 calendar days.

(b) An additional 7 calendar days are permitted for areas outside these cities.

(4) If good judgment indicates a fugitive lead is without immediate productive possibilities and economy can be effected by extending the deadline period, the above deadlines may be exempted.

(5) It is recognized that certain factors will dictate that more preferred attention be given to case than the above deadlines command. For example, a relatively low priority "C" fugitive might be wanted for questioning as a principal subject in a

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 21 - 8

major investigation. In such situations, the necessity for preferred attention should be set out regardless of the priority letter designation.

EFFECTIVE: 05/29/84

21-11 CAUTION STATEMENTS

(1) The use of caution statements as a special warning should be restricted to factual information aimed at alerting apprehending officers to exercise additional caution in arresting and controlling a subject.

(2) They must be included in all appropriate communications in underlined capital letters and in the subject's NCIC record.

(3) There are five basic caution statements:

(a) Armed and dangerous.

(b) Suicidal tendencies.

(c) Escape risk.

(d) A physical or mental condition or illness which may require immediate or professional care.

(e) "Warning: Known or Suspected HIV (Human Immunodeficiency Virus) Infected Person" (This warning should only be used in internal communications when also accompanied by the "Armed and Dangerous" warning or when other information is developed that the possibility of violence during an arrest is imminent.)

(4) The basis of the caution statement must be included in the caution statement in all initial communications to other field offices and FBIHQ. Subsequent communications to these offices need only set forth the caution statement, and its basis need not be restated.

(5) The caution statement should be set forth immediately after the case caption of the FD-517 and at the end of the narrative in prosecutive reports. In both investigative and nonprosecutive summary reports, the caution statement should be included immediately

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 21 - 9

after the case caption of the first cover page, at the end of the synopsis in every instance and at the end of the details of the first report. In the case of other communications, such as letters, airtels, and LHMs, it should be placed immediately after the case caption and at the end of the communication. If desired, an appropriate stamp may be used for this purpose. In teletypes, the caution statement should be included as the first line of the text.

(6) Notification when information first developed.

(a) In wanted flyer, identification order, or check circular cases, the developing office should immediately notify FBIHQ, office of origin, known auxiliary offices, and the office of prosecution (when other than the office of origin) by teletype. The office of origin should in turn furnish this information by teletype to all other auxiliary offices, by regular mail to all other offices and modify subject's NCIC record.

(b) In all other cases, the developing office should immediately notify FBIHQ, office of origin, known auxiliary offices, and the office of prosecution (when other than the office of origin) by teletype or airtel as the circumstances dictate. The office of origin should in turn furnish this information to all other auxiliary offices by teletype or airtel and modify the subject's NCIC record.

(7) When requesting the assistance or cooperation of local law enforcement officers or other agencies in apprehending the subject, fully apprise them of any caution statement.

(8) Form FD-65, the fugitive airtel, has a "Caution" block which must be checked when information exists indicating the need for enhanced caution by law enforcement personnel apprehending or controlling the fugitive. The "Caution" block will have checkboxes for appropriate warning statements. The basis for the caution statement must be stated as the first information reported in the "Miscellaneous" block of the FD-65. This information will be included in the NCIC record pertaining to the fugitive.

EFFECTIVE: 10/11/94

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 21 - 10

21-12 APPREHENSION OF BUREAU FUGITIVES

| (1) Bureau policy relating to arrest (use of force, forcible entry, etc.) is contained in Section 3, Legal Handbook for Special Agents. Also, see 21-13.4, infra, regarding entry to arrest.

| (2) When a Bureau fugitive is apprehended or located in custody, the apprehending office should immediately notify FBIHQ, office of origin, office of prosecution (when other than the office of origin), and all known auxiliary offices by routine teletype. The word, "FUGITIVE," should be carried in the title of all communications notifying FBIHQ and interested offices of the apprehension or location of a Bureau fugitive.

| (3) Good judgment must be exercised and where a more urgent communication is obviously justifiable, notification by telephone or immediate or priority teletype should be utilized.

| (4) When one of the Ten Most Wanted Fugitives is apprehended or located in custody or fugitive's apprehension appears imminent, FBIHQ must be immediately advised by telephone and confirmed by teletype.

| (5) Upon notification, the office of origin should review its case file and notify any other auxiliary office where investigation is pending of the apprehension or location by routine teletype.

| (6) If investigation is being conducted by a known Legat office, the apprehending office should request FBIHQ in its apprehension teletype to advise the particular Legat office to discontinue.

| (7) If the apprehending office has not requested FBIHQ to notify any or all Legat offices conducting investigation to discontinue, the office of origin should promptly submit a routine teletype to FBIHQ requesting same.

| (8) If the office of origin's case Agent is not readily available, it is the responsibility of the appropriate office of origin's supervisor to ensure that all auxiliary offices are advised to discontinue investigation and FBIHQ is requested to advise appropriate Legat offices to discontinue.

| (9) If the subject is a Ten Most Wanted Fugitive or the subject of an identification order, check circular, or wanted flyer,

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 21 - 11

FBIHQ will notify all offices and Legats by appropriate communication of his/her apprehension.

EFFECTIVE: 10/10/83

21-13 HARBORING STATUTES

EFFECTIVE: 10/10/83

21-13.1 Title 18, USC, Section 3. Accessory After the Fact

"Whoever, knowing that an offense against the United States has been committed, receives, relieves, comforts or assists the offender in order to hinder or prevent his apprehension, trial or punishment, is an accessory after the fact.

"Except as otherwise expressly provided by any Act of Congress, an accessory after the fact shall be imprisoned not more than one-half the maximum term of imprisonment or fined not more than one-half the maximum fine prescribed for the punishment of the principal, or both; or if the principal is punishable by death, the accessory shall be imprisoned not more than ten years."

EFFECTIVE: 10/10/83

21-13.2 Title 18, USC, Section 1071. Concealing Person from Arrest

"Whoever harbors or conceals any person for whose arrest a warrant or process has been issued under the provisions of any law of the United States, so as to prevent his discovery and arrest, after notice or knowledge of the fact that a warrant or process has been issued for the apprehension of such person, shall be fined not more than \$1,000 or imprisoned not more than one year, or both; except that if the warrant or process issued on a charge of felony, or after conviction of such person of any offense, the punishment shall be a fine of not more than \$5,000, or imprisonment for not more than five years, or both."

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 21 - 12

EFFECTIVE: 10/10/83

21-13.3 Elements

(1) Accessory after the fact

(a) A person who knows that an offense against the United States has been committed.

(b) Receives, relieves, comforts, or assists the offender.

(c) The act of receiving, relieving, comforting, or assisting the offender is committed in order to prevent the offender's apprehension, trial, or punishment.

(2) Concealing person from arrest

(a) A person harbors or conceals an individual.

(b) There is a warrant of arrest or other process outstanding for the individual harbored or concealed which was issued under the provisions of some Federal law.

(c) The person harboring or concealing the offender knows of the warrant or process.

(d) The act of harboring or concealing is done to prevent discovery and arrest of the offender.

EFFECTIVE: 01/21/86

21-13.4 Policy

(1) Since harboring is a substantive crime separate and distinct from the offense for which the fugitive is sought, Agents are justified in arresting a harborer where there is probable cause to believe such a violation is being or has been committed. Where possible, authorization of the U.S. Attorney should be obtained and an arrest warrant issued prior to the arrest of one accused of harboring. Entry to the harborer's own premises to execute the arrest warrant requires probable cause to believe the harborer is within, but does

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 21 - 13

not additionally necessitate a search warrant before entry to the premises.

(2) Where there is probable cause to believe a fugitive is located within the premises of a harbinger, entry to such premises to arrest the fugitive is contemplated, the premises are not the principal residence of the fugitive, and there are no exigent circumstances or consent justifying an immediate warrantless entry, a search warrant must be obtained naming the fugitive as the object of the search. (See Section 3-7, Legal Handbook for Special Agents.) The search warrant will support the complete and thorough search of the premises for the fugitive.

(3) An arrest of either the harbinger or a fugitive, with or without warrant, will justify a cursory search of the premises where Agents have a reasonable suspicion that confederates, accomplices, or others, lurking therein, may jeopardize their safety. (See Section 5-3.9, Legal Handbook for Special Agents.)

EFFECTIVE: 01/21/86

21-13.5 Venue

Prosecution shall be in the district in which the offense was committed.

EFFECTIVE: 01/21/86

21-13.6 Classification

The same as the substantive violation.

EFFECTIVE: 01/21/86

21-13.7 Character

Substantive offense - HARBORING

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 21 - 14

EFFECTIVE: 01/21/86

21-14 LOCATING, CLEARING, AND CANCELLING SUBJECT'S NCIC RECORD

(1) If the fugitive is apprehended or located in the territory of the office having the subject's record on file in NCIC they should immediately (within 24 hours) "clear" the Bureau's NCIC record and place a "located" on any other NCIC record positively identifiable with the fugitive. This is to be done via the terminal located in the office. The substantive case file is to show the "clear" and any "located" action taken in NCIC.

(2) If the subject is apprehended or located in the territory of an office other than the office having the subject's record on file in NCIC, the following procedures must be followed by said office and the office having the record on file in NCIC:

(a) The office apprehending or locating the fugitive must immediately (within 24 hours) change the status of the subject's Bureau NCIC record to show "located." Any other NCIC record positively identifiable with the fugitive must also be promptly changed to a "located" status. This is to be done through the office terminal. The substantive case file is to show that the "located" action was taken.

(b) The office having the subject's record on file in NCIC, upon receipt of notification via NCIC computer that a "located" message has been placed in the fugitive's Bureau NCIC record by another FBI office or military authorities in a deserter case, should immediately (within 24 hours) "clear" the subject's NCIC record through the terminal located in the office. The substantive case file is to show that the "clear" action was taken.

(c) The office having the subject's record on file in NCIC, upon receipt of notification via NCIC computer that a "located" message has been placed in the fugitive's Bureau NCIC record by an agency other than another FBI office or military authorities in a deserter case, should instruct the office covering the area of the "locating" agency to promptly verify both the identity and the apprehension of the fugitive. Following this verification immediately (within 24 hours) "clear" the subject's NCIC record through the terminal in the office. The substantive case file is to show that the NCIC record has been properly "cleared."

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 21 - 15

(3) If the federal process, or local process in the case of an unlawful flight fugitive, is dismissed prior to the fugitive's apprehension, the office having the Bureau's entry on file in NCIC must immediately (within 24 hours) "cancel" said entry. The substantive case file must reflect that this has been done.

(4) Refer to the Manual of Administrative Operations and Procedures, Part II, Section 7 for additional NCIC procedures in this area.

EFFECTIVE: 02/14/97

21-15 LETTERS OF APPRECIATION

(1) If a local, state, or Federal law enforcement official apprehends or assists in the apprehension of a Bureau fugitive, a letter of appreciation from the Director will be forwarded to the official by FBIHQ upon appropriate recommendation of the SAC.

(2) The recommendation, which may be set forth in the apprehension teletype, a separate communication, or by Form FD-468, must include the following:

(a) Official name, rank, and address of the officer causing the apprehension.

(b) Official name, rank, and address of the person in charge of the agency involved.

(c) Results of office indices checks against these individuals.

(d) Sufficient details to enable FBIHQ to afford the matter appropriate attention.

EFFECTIVE: 11/08/82

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 21 - 16

21-16 VERIFYING FEDERAL AND LOCAL PROCESS

(1) For those fugitives for whom Federal arrest process is outstanding, the office of prosecution shall verify once a year that the process is still outstanding and contact the USA to determine whether USA still desires to prosecute the fugitive if apprehended.

(2) For those fugitives wanted under the Unlawful Flight Statute, the underlying local process and intention of local authorities to extradite for prosecution or reconfinement must be verified once a year.

(3) When subsequently verifying Federal and/or local process for those fugitives after the case has been placed in a pending inactive unassigned status, because they are Mexican citizens who have fled to Mexico where they are not subject to extradition and deportation, it should be made a matter of record in the case file and need not be reported to FBIHQ.

EFFECTIVE: 11/08/82

21-17 DISMISSAL OF FEDERAL OR LOCAL PROCESS PRIOR TO
APPREHENSION

(1) If the federal process, or local process in the case of an unlawful flight subject, is dismissed prior to a fugitive's apprehension, the office of origin or office of prosecution, when other than the office of origin, should immediately notify FBIHQ and all auxiliary offices by routine teletype to discontinue. The word, "FUGITIVE," should be carried in the title of this teletype.

(2) This notification will enable FBIHQ to promptly remove the fugitive stop in the Criminal Justice Information Services Division and delete the subject from its fugitive index.

EFFECTIVE: 12/02/94

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 21 - 17

21-18 PENDING INACTIVE STATUS WHEN ALL LOGICAL INVESTIGATION HAS
BEEN CONDUCTED

(1) In fugitive cases, when all logical investigation has been conducted and the subject is still in fugitive status, FBIHQ can be requested on a UACB basis to allow the office of origin to place the case in a pending inactive status for six months for "A," "B," and "D" priority fugitives and for one year for "C" priority fugitives. "D" priority cases can also be placed in pending inactive status for six months when it has been determined that the parent who kidnaped the child is residing in a foreign country and, for whatever reason, the local authorities will not or are unable to have the subject extradited back to the United States.

(2) Prior to submitting such a request, conduct an in-depth file review in an effort to develop logical leads which may have been overlooked or bear recoverage due to the passage of time.

(3) Following this review, if your request is still desired, prepare a comprehensive summary report setting forth the full scope of investigation conducted for review by FBIHQ.

(4) The administrative section of the cover page should contain a statement that UACB this case is being placed in a pending inactive status for six months or one year (depending on the fugitive priority), since all logical investigation has been thoroughly conducted, after which time the case will be made pending and appropriate leads will be set out in an effort to locate and apprehend the subject.

EFFECTIVE: 10/18/88

21-19 LOCATING AND RELOCATING FUGITIVES OUTSIDE THE UNITED
STATES

EFFECTIVE: 10/18/88

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 21 - 18

21-19.1 Requesting Investigative Assistance Abroad - Extradition
Deportation

(1) In most instances, requests for fugitive investigations abroad will be handled by Legal Attaches (Legats) (see Part II, 23-4.5, of this manual), and in those areas not covered by a Legal Attache, through liaison with Interpol (see Part I, Section 163-10, of this manual), the U.S. Department of State, [REDACTED]

b3
b7c
CIA

(2) When submitting requests for fugitive investigations to our Legats through FBIHQ, include in the cover airtel, when LHM used, and set forth in the administrative section of a teletype, letter or airtel, where no LHM is used, the results of a recent contact with the USA or a local prosecutor if the fugitive matter is unlawful flight (UFAP) in nature. Set out a statement, if such is the case, that the USA (state authorities, if UFAP matter) will initiate the necessary action for subject's extradition if the fugitive is successfully located and informal deportation is not a possibility.

(3) Further, specifically include, where possible, the USA's (local prosecutor's, if UFAP matter) assessment of the seriousness of the case, the likelihood of conviction and whether subject can be expected to be released on bond or remanded to custody upon subject's return to this country.

(4) Legal Attaches will attempt to arrange informal deportations for FBI fugitives whenever possible. The U.S. Marshals Service (USMS) funds and handles transportation in informal deportations in the same manner that they handle extradition situations. All Legal Attaches, upon locating an FBI fugitive abroad, who would be available for informal deportation, are to notify FBIHQ by teletype, furnishing the identity and telephone number, if possible, of the local official in the particular country and/or embassy representative with whom the matter should be coordinated. FBIHQ will then notify the office of origin (OO) and the Office of International Affairs, Department of Justice (DOJ), who will then coordinate with the Enforcement Operations Division, USMS Headquarters, to request appropriate funding and transportation assistance. If the fugitive is the subject of an Unlawful Flight warrant, the Legal Attache will provide an estimate of expenses and, through FBIHQ, request OO to ensure that the interested State authorities are willing to assume the cost of the informal deportation, which would be subsequently billed to them by the U.S. Marshal. If the State authorities agree, OO is to advise the Legal Attache, through FBIHQ, and notify the Marshal holding the Federal

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 21 - 19

warrant that a request for deportation transportation will be made of their headquarters by FBIHQ through DOJ.

EFFECTIVE: 10/18/88

21-19.2 Mexican Citizen in Mexico

FBI fugitives who are Mexican citizens and who flee to Mexico are not subject to extradition or deportation. The office of origin should submit an appropriate communication to the proper border office or to FBIHQ for transmission to Legat, Mexico City, requesting that the fugitive be located. Once the fugitive is initially located in Mexico, no further action should be taken to relocate him/her in Mexico in the future by either Legat, Mexico City, or a border office and the case should be placed in a pending inactive unassigned status by the office of origin with the fugitive stops outstanding. If information is received that a fugitive has returned to the United States, the case should be reopened and investigation conducted to effect his/her apprehension. For those fugitives for whom Federal arrest process is outstanding, the office of prosecution shall verify once a year that the process is still outstanding and contact USA to determine whether USA still desires to prosecute the fugitive if apprehended. For those fugitives wanted under the Unlawful Flight Statute, the underlying local process and intention of local authorities to extradite for prosecution or reconfinement must also be verified once a year.

EFFECTIVE: 10/24/85

21-19.3 Fugitives Outside the United States Other Than Mexican Citizens in Mexico

The office of origin should submit an appropriate communication to the proper border office or to FBIHQ for transmission to the appropriate Legat or agency, if the country in question is not covered by our Legats, requesting that the fugitive be located. Once the fugitive is initially located in the foreign country and if his/her deportation or extradition cannot be legally accomplished or will not be instituted, the case should be placed in a pending inactive status by the office of origin, with stops outstanding, upon completion of all other necessary investigation. If information is received that a fugitive has returned to the United States, the case

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 21 - 20

should be reopened and investigation conducted to effect his/her apprehension. For those fugitives wanted under the Unlawful Flight Statute, the underlying local process and intention of local authorities to extradite for prosecution or reconfinement, if apprehended within the United States, must be verified once a year. For those fugitives for whom Federal arrest process is outstanding, the office of prosecution shall verify once a year that the process is still outstanding and contact the USA to determine whether USA still desires to prosecute the fugitive if apprehended within the United States. Fugitive cases involving non-Mexicans in Mexico and others previously located abroad should be reopened and the subjects relocated every two years through the above procedures.

EFFECTIVE: 10/24/85

21-19.4 | Fugitives Outside the United States |

(1) | When it is determined a fugitive has left the United States, the office of origin should immediately establish and maintain a lookout notice (Form FD-315) with the U.S. Immigration and Naturalization Service (INS). Upon the fugitive's apprehension or dismissal of process, it is likewise the responsibility of the office of origin to discontinue this notice (see Part II, 10-7.5.2 of this manual for procedures for establishing and canceling INS stops).

(2) | As soon as it appears likely that a fugitive may be located in a foreign country, you should notify the prosecutor, either the U.S. Attorney or the local prosecutor in unlawful flight cases, that he or she should contact the Office of International Affairs (OIA), Criminal Division, U.S. Department of Justice, promptly. In addition, as soon as such an arrest appears likely, you are to notify the substantive division at FBIHQ, with copy to the Office of Liaison and International Affairs, so that FBIHQ may notify OIA. |

EFFECTIVE: 10/25/89

Sensitive

PRINTED: 02/18/98

XXXXXX
XXXXXX
XXXXXXFEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET3

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 552Section 552a☐ (b)(1)☐ (b)(7)(A)☐ (d)(5)☒ (b)(2)☐ (b)(7)(B)☐ (j)(2)☐ (b)(3)☐ (b)(7)(C)☐ (k)(1)☐ (b)(7)(D)☐ (k)(2)☒ (b)(7)(E)☐ (k)(3)☐ (b)(7)(F)☐ (k)(4)☐ (b)(4)☐ (b)(8)☐ (k)(5)☐ (b)(5)☐ (b)(9)☐ (k)(6)☐ (b)(6)☐ (k)(7)

- ☐ Information pertained only to a third party with no reference to the subject of your request or the subject of your request is listed in the title only.

- ☐ Documents originated with another Government agency(ies). These documents were referred to that agency(ies) for review and direct response to you.

Pages contain information furnished by another Government agency(ies). You will be advised by the FBI as to the releasability of this information following our consultation with the other agency(ies).

Page(s) withheld inasmuch as a final release determination has not been made. You will be advised as to the disposition at a later date.

Pages were not considered for release as they are duplicative of _____

Page(s) withheld for the following reason(s): _____

- ☒ The following number is to be used for reference regarding these pages:

MI09 21-19.5

XXXXXXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X for this page X
XXXXXXXXXXXXXXXXXXXX

XXXXXX
XXXXXX
XXXXXX

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 21 - 24

21-20 FUGITIVE INVESTIGATIONS FOR OTHER FEDERAL AGENCIES

(1) Special requests are occasionally received by the field from other Federal agencies or from USAs to conduct investigation to locate fugitives wanted for Federal violations within the primary jurisdiction of other Federal agencies.

(2) When such requests are received, promptly submit to FBIHQ by airtel or teletype, depending on the urgency, the complete details including the reasons for the request. Hold all investigation in abeyance pending FBIHQ instructions.

(3) All fugitive investigations conducted by the FBI for other Federal agencies (example: DEA Fugitives) should be classified as 62E matters.

EFFECTIVE: 10/25/89

21-20.1 Fugitive Inquiries Abroad on Behalf of U.S. Marshals Service (USMS)

(1) Based upon an agreement reached with the FBI, the USMS may request, through FBIHQ, investigative assistance of our Legal Attaches to conduct limited agency-type inquiries in fugitive matters within the jurisdiction of their agency.

(2) Requests for assistance will be forwarded, by letter to FBIHQ, reviewed, and transmitted to the appropriate Legal Attache for handling, if such requests conform to the existing agreement; i.e., are merely agency checks and do not involve the location or apprehension of a fugitive. Conduct no inquiries unless they are forwarded from FBIHQ.

(3) Upon completion of the inquiry by the Legal Attache, it should be forwarded to FBIHQ, Attention: Fugitive/Government Reservation Crimes Unit, in a form suitable for dissemination to USMSHQ.

(4) As requests should be few in number, Legal Attaches are to establish a control file in the "62" classification and handle inquiries out of such file. All correspondence to FBIHQ should utilize the caption noted above and include, as a subcaption, the name(s) of the subject(s). Appropriate serializing and indexing should be made for record and retrieval purposes.

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 21 - 25

EFFECTIVE: 10/25/89

21-21 FUGITIVE INQUIRIES

When attempting to determine if an individual is a Bureau fugitive or is wanted by another agency, the following procedures should be followed:

- (1) Obtain all known background, descriptive data and identifying numbers.
- (2) If identifying numbers, such as date of birth or SSAN, are known, make an inquiry of NCIC through the terminal located in the field office.
- (3) Inquiry can be made through another agency's NCIC terminal when advantageous or convenient; however, your office's NCIC identifier must be used to identify the inquiry as Bureau originated.
- (4) If NCIC is negative or cannot be utilized because of the lack of an identifying number, direct a teletype or electronic communication, depending on the urgency, to FBIHQ. Set forth the details and data along with the results of the NCIC check and request a check of the FBIHQ fugitive index and Criminal Justice Information Services Division records. (See MIOG, Part II, 21-4(2).)
- (5) Whenever possible, inquiries should be worded "Advise only if fugitive or wanted" to avoid the need for a negative reply.
- (6) If a reply is desired, specifically indicate by stating "Advise whether or not a fugitive or wanted."
- (7) Avoid ambiguous language such as "Advise if fugitive" or "Advise if wanted." Such requests will be interpreted to mean "Advise only if fugitive or wanted."
- (8) In those instances where a reply is desired and an electronic communication is used, one extra copy of the electronic communication should be submitted to FBIHQ for each office that is to be advised.
- (9) If there is no record of being a Bureau fugitive or wanted by another agency, FBIHQ will appropriately stamp copies of the

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 21 - 26

incoming communication and forward same to the interested offices by routing slip.

EFFECTIVE: 05/13/96

21-22 FBIHQ FUGITIVE INDEX (See MAOP, Part II, 7-2.1(1).)

(1) An alphabetical fugitive index containing all currently designated Bureau fugitives is maintained in the Violent Crimes/Fugitive Unit, Criminal Investigative Division, FBIHQ.

(2) When attempting to determine if an individual is a Bureau fugitive and identifying numbers are not available in order to check NCIC, an inquiry based on the individual's name can be made of these fugitive indexes at FBIHQ.

(3) Fugitive inquiries may be made using only the fugitive's name, if no other data is available, by calling [REDACTED] 7 a.m. - 5:30 p.m., Eastern Time, Monday through Friday, or by calling [REDACTED] during off-hours. b2

EFFECTIVE: 08/18/94

21-23 POSSIBLE FUGITIVE LEADS

The following possible fugitive leads are not intended to be all inclusive, but should be utilized when appropriate in addition to the usual investigative steps taken in a fugitive investigation in an effort to locate and apprehend the subject:

(1) If it is known or suspected that the subject has left the country, request WMFO to cause a search of the records of the Passport Office, Department of State, Washington, D.C., to determine if the subject has applied for or received a passport. b2 b7E

(2) If the subject is an alien, request WMFO to cause a search of the records of the Alien Registration Division, INS, Washington, D.C., for information alien is required to furnish under the provisions of the Alien Registration Act of 1940.

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 21 - 27

(3) If the subject is a former military person, contact the nearest regional office of the Department of Veterans Affairs which will advise which regional office has subject's records on file through which any compensation or insurance benefits can be determined.

(4) If the subject is or was a merchant seaman, request WMFO to contact U.S. Coast Guard Headquarters, Washington, D.C., for a record check. The number of the subject's seaman's certificate of identification (Z-number), if known, should be furnished.

(5) If the subject previously served in the Air Force, Army, Marines, or Navy, request the proper office to cause a review of subject's military records.

(6) Utilization of a circular letter if appropriate and with FBIHQ approval.

(7) [REDACTED]

(8) [REDACTED]

(9) [REDACTED]

(See [REDACTED] for restrictions on the use of this technique.)

(10) Use of the All Writs Act (AWA), Title 28, USC, Section 1651, to obtain records to locate federal fugitives. All Writs Act orders for the production of records may be requested in all federal fugitive investigations, including unlawful flight fugitives, subject to the following requirements:

(a) There must be an outstanding arrest warrant for the fugitive issued by the U.S. District Court (USDC) or the U.S. Magistrate.

(b) The AWA order can only be issued in the federal district court where the criminal case is pending. Such orders are valid and may be executed in any federal judicial district. Therefore, where the records sought are located in a district other than the district of issuance the order should be transmitted to the field office where the records are located and the records should be produced to Agents of that office.

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 21 - 28

(c) The order should be obtained from a judge of the USDC unless the USDC has delegated appropriate authority to the U.S. Magistrate. The USA's office should be able to make this determination.

(d) The orders should allow sufficient time (10-12 days) between the date of the orders and the required production of the records to allow the affected company to challenge the order in the district court of issuance if it desires to do so. This requirement does NOT preclude more timely production of the records if the company is cooperative.

(e) The affidavit should demonstrate the reasonable belief that the records sought may be of assistance in locating the fugitive.

(f) Although [REDACTED] will probably be the most common records sought with this procedure, AWA orders may be used for the production of other records which might assist in the location of the fugitive. However, AWA orders may not be utilized to obtain records to locate federal parole violators who are wanted on federal parole violators warrants because there is no pending case in the USDC and the court thus lacks jurisdiction. Also, AWA orders may not be utilized to obtain records to locate mandatory release violators (MRVs) since they have the same status as federal parole violators (no pending case in the USDC).

(g) Memorandum to All SACs, dated 10/19/83, captioned "USE OF ALL WRITS ACTS TO OBTAIN RECORDS TO LOCATE FEDERAL FUGITIVES," provided sample forms designed to facilitate the use of this technique.

[REDACTED]

[REDACTED]

b2
b7E

b2
b7E

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 21 - 29

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

(16) Leads should be set forth to review police reports, and an inquiry of the Interstate Identification Index should be performed for criminal history data on the subject.

(17) The cooperation of the subject's bondsmen may be sought if circumstances indicate that this procedure is advisable.

[REDACTED]

[REDACTED]

(20) Consider obtaining return information concerning the fugitive from the Internal Revenue Service (IRS). See Part II, Section 19, of this manual.

(21) Consider requesting the issuance of an Interpol International Wanted Notice if the fugitive is believed to be traveling abroad. (See Part I, Section 163-10, of this manual for procedures to request issuance of these notices.)

(22) Placing of Fugitive Stops in State and Local Identification Bureaus: The office of origin in fugitive matters should disseminate copies of fugitive fingerprint cards to auxiliary offices requesting that the fingerprints be searched and/or filed in local and state identification bureaus. In order to ensure the full

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 21 - 30

cooperation of state and local identification bureaus, the office of origin should disseminate only photographic or laminated copies of fingerprint cards to auxiliary offices to place fugitive stops with these bureaus. Request laminated copies of fingerprint cards from the Criminal Justice Information Services Division, West Virginia Operations (Attention: Module D-2 AHTW). (See Part II, 14-12.3.5 and 21-4 (3) of this manual.)

(23) (See Part I, Section 88-7.5, of this manual, for access to information from the Federal Parent Locator Service (FPLS), UFAP - Parental Kidnapping - Child Abduction Matters.)

(24) See Part II, Section 19, of this manual, entitled "Location Of Other Government, Industrial, and Organizational Records," which sets forth a multitude of federal, state, territorial and private industry records by location and field offices covering same that may be the basis for record checks and stops.

(25) See Part II, Section 10, of this manual, entitled "Records Available and Investigative Techniques," which sets forth, either directly or by MIOG cross-reference, numerous investigative techniques that may be utilized in fugitive investigations.

refer
D-21
[REDACTED]

[REDACTED]

refer
SSA
[REDACTED]

[REDACTED]

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 21 - 31

[REDACTED]

[REDACTED]

for
SSA

[REDACTED]

[REDACTED]

(28)

[REDACTED]

b2
b7E

[REDACTED]

[REDACTED]

XXXXXX
XXXXXX
XXXXXXFEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET2

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 552Section 552a☐ (b)(1)☐ (b)(7)(A)☐ (d)(5)☒ (b)(2)☐ (b)(7)(B)☐ (j)(2)☐ (b)(3)☐ (b)(7)(C)☐ (k)(1)☐ (b)(7)(D)☐ (k)(2)☒ (b)(7)(E)☐ (k)(3)☐ (b)(7)(F)☐ (k)(4)☐ (b)(4)☐ (b)(8)☐ (k)(5)☐ (b)(5)☐ (b)(9)☐ (k)(6)☐ (b)(6)☐ (k)(7)

- ☐ Information pertained only to a third party with no reference to the subject of your request or the subject of your request is listed in the title only.

- ☐ Documents originated with another Government agency(ies). These documents were referred to that agency(ies) for review and direct response to you.

Pages contain information furnished by another Government agency(ies). You will be advised by the FBI as to the releasability of this information following our consultation with the other agency(ies).

Page(s) withheld inasmuch as a final release determination has not been made. You will be advised as to the disposition at a later date.

Pages were not considered for release as they are duplicative of _____

Page(s) withheld for the following reason(s): _____

- ☒ The following number is to be used for reference regarding these pages:

MI09 21-24

XXXXXX
XXXXXX
XXXXXX
 XXXXXXXXXXXXXXXXXXXX
 X Deleted Page(s) X
 X No Duplication Fee X
 X for this page X
 XXXXXXXXXXXXXXXXXXXX

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 21 - 34

EFFECTIVE: 07/23/90

21-25 IDENTIFICATION ORDERS, WANTED FLYERS, AND CHECK CIRCULARS

EFFECTIVE: 02/16/89

21-25.1 Basis for Issuance

(1) Identification orders (IO) and wanted flyers may be issued by FBIHQ in our more important fugitive cases involving badly wanted fugitives who have committed or been charged with crimes of a more serious or violent nature having considerable public interest.

(2) Check circulars may be issued by FBIHQ in cases of fugitives who are notorious fraudulent check passers and who are engaged in a continuing operation of passing checks.

(3) These wanted notices are issued by FBIHQ in the above appropriate cases to aid the fugitive investigation through increased

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 21 - 35

publicity and cooperation when all logical productive investigation has been conducted and the fugitive investigation is at a standstill, or when the earlier issuance is merited due to the magnitude of the crimes or notoriety of the fugitive involved.

EFFECTIVE: 02/16/89

21-25.2 Requesting Issuance

(1) In the event that the issuance of an IO, wanted flyer or check circular is desired and appropriate, the office of origin may request its issuance during any stage of the fugitive investigation by self-explanatory Form FD-61. In addition, when submitting an FD-61 each office should also submit a comprehensive nonprosecutive summary report setting forth significant investigation conducted to locate the fugitive as well as information relative to leads outstanding.

(2) The original and one copy of the FD-61 should be submitted to FBIHQ by cover airtel marked to the attention of the Fugitive/Government Reservation Crimes Unit, Criminal Investigative Division, to ensure prompt receipt and consideration.

(3) Since the purpose of a wanted flyer is to cause immediate nationwide circularization of the flyer, usually at the outset of the fugitive investigation, the office of origin may request the issuance of a wanted flyer, if desired and appropriate, by teletype or telephone confirmed by teletype.

(4) An existing wanted flyer on file should be utilized as a guide in providing the necessary data needed and this data should be furnished in both the telephone call and teletype to FBIHQ. An FD-61 should subsequently be furnished to FBIHQ since the wanted flyer will be followed up by the issuance of an identification order.

(5) Since an identification order is promptly issued by FBIHQ for the subject after the issuance of the wanted flyer, wanted flyers will only be issued in very extraordinary fugitive situations because of the duplication and cost factors involved.

(6) In regard to requests from the field for issuance of these wanted notices, they will be issued by FBIHQ only after close scrutiny. If additional information is needed by FBIHQ before rendering a determination the office of origin will be requested to submit additional details.

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 21 - 36

(7) In certain instances, FBIHQ based on its judgment, will direct the office of origin to submit an FD-61 for the issuance of an identification order or check circular or provide necessary data for the issuance of a wanted flyer.

EFFECTIVE: 02/16/89

21-25.3 Procedures After Issuance

(1) After the issuance of the wanted flyer, identification order or check circular, the office of origin should modify its NCIC record on the subject to include the wanted flyer, identification order or check circular number in the "miscellaneous" field.

(2) Upon issuance of an identification order or check circular, FBIHQ will prepare a letter to all offices enclosing five smooth finished copies of the subject's photograph to be utilized for press or news media purposes.

(3) Upon the issuance of an identification order, wanted flyer, or check circular and the above letter by FBIHQ, the office of origin should, by cover airtel, promptly forward to FBIHQ and each office four copies of an LHM setting forth pertinent background and descriptive information concerning the fugitive. The airtel should be appropriately noted "Summary - Background Airtel," while the LHM should include separate headings as follows: Facts of Offense; Federal Process; Brief Personal History; Modus Operandi, and Other Interesting Facts; Identification Record; Facts as to Dangerousness and/or Suicidal Tendencies; and Detailed Physical Description.

(4) Each office, upon receipt of the "Summary - Background Airtel," should carefully review it to determine if the facts suggest the basis of self-initiated investigation and if so, a case should be promptly opened and assigned. A case should not be opened unless this review results in specific leads. In all instances, this case should be closed within 90 days in the absence of generating specific leads.

(5) Following the submission of the "Summary - Background Airtel," on a regular basis at intervals not to exceed 120 days, the office of origin should furnish FBIHQ a comprehensive summary airtel setting forth information as to the progress and direction of its

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 21 - 37

fugitive inquiries.

(6) To assist FBIHQ in monitoring and evaluating the effectiveness of this program, the apprehending office should advise in its apprehension teletype to FBIHQ whether or not the particular wanted notice contributed to the fugitive's location and apprehension. If positive, state how the information was obtained and from whom.

(7) Upon receipt of an identification order, wanted flyer or check circular, each office will conduct driver's license and vehicle registration checks of all state licensing agencies covered by the division using true name and all aliases of subject. These checks are also to be conducted upon receipt of additional aliases and on true names and aliases of known associates that may subsequently be furnished to each field division. Dates and results of these checks are to be recorded in the appropriate fugitive file.

EFFECTIVE: 01/21/86

21-25.4 Administrative Handling by Field Office of Identification Orders (IOs), Wanted Flyers, and Check Circulars

A list of numbers in succession is to be prepared in each field office. As each IO is received, true name of subject is to be written opposite number on list which is identical with number on IO. Draw a line through number to indicate that IO has been received. Same procedure is carried out for wanted flyers and check circulars.

EFFECTIVE: 01/21/86

21-25.4.1 Procedure When Received by Field Office

(1) Check number against list. If any are missing, advise FBIHQ.

(2) Check index for information on all subjects;

(a) If no file exists, prepare index cards for each name and alias. IO, wanted flyer, and check circular numbers are to appear on all cards made.

(b) Prepare a dead investigative file.

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 21 - 38

(3) Put five copies of IO, wanted flyer or check circular in investigative file and date stamp top one.

(4) Put one copy on bulletin board.

(5) Send one copy to each Agent having a need for same. All Agents will not receive them.

(6) Keep FBIHQ advised of number of IOs, wanted flyers, and check circulars required for investigative purposes.

(7) Put one copy in appropriate 66 classification file of outstanding IOs, wanted flyers, or check circulars. These files are only for IOs, wanted flyers, or check circulars which have not been discontinued.

EFFECTIVE: 01/21/86

21-25.4.2 Miscellaneous Instructions Regarding IOs, Check Circulars and Wanted Flyers

(1) Agents may keep those IOs, check circulars, and wanted flyers which may be of value to them.

(2) Use apprehension communications to keep 66 administrative file current.

(3) An outstanding list showing identity of all IOs, wanted flyers, and check circulars is published as of March 31 and September 30 of each year. List will contain sequence numbers of such items which have been discontinued since previous list.

EFFECTIVE: 01/21/86

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 21 - 39

21-26 TEN MOST WANTED FUGITIVES PROGRAM

(1) Individuals selected as the Ten Most Wanted Fugitives are chosen by FBIHQ from existing IO subjects.

(2) Ten Most Wanted Fugitive cases, after being so designated, must be kept pending in all field offices until a complete review of the case has been made and all logical investigation has been conducted. Thereafter, all offices except origin may place such matters in closed status, if the fugitive has not been located by that time.

(3) While primary responsibility for direction of each case is with the office of origin, all offices are expected to participate fully in the initiation of logical investigation, which should include full exploitation of various news media outlets throughout their territory.

(4) During this investigation each office must initiate investigation suggested by characteristics, background, and habits of the fugitive, as well as on the geography, climate, employment, and recreation facilities unique to a particular office area. Fully exploit investigative techniques which are readily available, including informants, auto vehicle bureaus, other Government records, and general sources and avenues of employment, including spot-labor pools.

(5) On an annual basis, each subject in the Ten Most Wanted Fugitives Program will be examined to determine if the individual fits the criteria for the Ten Most Wanted Fugitives Program. The review will be conducted one year from the date placed on the Ten Most Wanted Fugitives List. When conducting the review, office of origin and local police agencies having an interest in the individual will be contacted for input concerning retention of the individual on the Ten Most Wanted Fugitives List.

EFFECTIVE: 02/19/85

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 21 - 40

21-27 DISTRIBUTION OF WANTED NOTICES (IDENTIFICATION ORDERS,
WANTED FLYERS, AND CHECK CIRCULARS)

(1) When a wanted flyer is issued, 50 unfranked and unfolded copies will be sent to each office by first-class mail. Each Legal Attache will receive five copies. Upon receipt of these wanted flyers, each field office should immediately distribute them to major law enforcement agencies, news media representatives, including television, and to appropriate Agent personnel. File copies, of course, should be retained.

(2) In most situations where a wanted notice would be appropriate, an IO, check circular or circular letter should be considered.

EFFECTIVE: 02/19/85

21-27.1 Field Mailing Lists

(1) Field mailing lists previously used to distribute IOs and other wanted notices were centralized and automated at FBIHQ in 1981. Wanted notices are now distributed outside the Bureau by FBIHQ as they are issued. IOs are issued and distributed in pairs depicting different subjects to conserve postage costs.

(2) Although field mailing lists are centralized, automated, and maintained at FBIHQ, individual recipients are identifiable by the field office covering the recipient's address to facilitate corrections, additions, deletions, and possible special mailing uses within a particular division's territory.

(3) Field mailing lists are organized and arranged into seven distinct groups of recipients as follows:

01 - U.S. Post Offices, Branches, and Stations operated by classified U.S. Postal Service personnel.

02 - Federal law enforcement and investigative agencies operated by the Federal Government.

03 - State law enforcement agencies operated by state governments such as the state police, highway patrol, and identification bureaus.

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 21 - 41

04 - City, county, and local law enforcement agencies such as police departments, sheriffs' departments, and town marshals.

05 - Certain foreign law enforcement agencies at all levels which are operated by governments outside the United States and its territories.

06 - All other recipients not included in one of the above categories and designated by an SAC to receive wanted notices.

07 - U.S. Postal Inspectors and Examiners.

(4) In order to ensure delivery of wanted notices to recipients, they are now addressed whenever possible to an official using only his/her title, such as Chief of Police, Sheriff, or Identification Officer, rather than his/her name. Experience has shown that wanted notices addressed to individuals by name are occasionally returned to the Bureau "undeliverable" because the person has retired, resigned, or is otherwise no longer associated with the agency.

(5) When wanted notices are returned to the Bureau as "undeliverable," an attempt will be made to correct the recipient's address listed in the field mailing list from reference material at FBIHQ and/or contact with the appropriate field office. In the event a valid address for the recipient cannot be readily ascertained the record will be removed from the field mailing list.

(6) Field offices should attempt to ensure that all U.S. Postal facilities and law enforcement agencies described in the above categories are included in their respective mailing list. Such verification checks may be accomplished while contacting the particular agency during the regular course of business. Additions, corrections, and deletions may be made by routing slip addressed to the Bureau, Attention: |Fugitive/Government Reservation Crimes|Unit, Criminal Investigative Division. The title only of the official who is to receive wanted notices together with the agency's full address, including ZIP Code, and number of wanted notices required, should be clearly set forth.

(7) Other recipients, as in category 06 described above, may be added to a field office's mailing list on SAC authority. Ensure such recipients both want and can use Bureau wanted notices. Additions, corrections, and deletions to this category of recipients may also be made by routing slip addressed to the Bureau, Attention: ||Fugitive/Government Reservation Crimes|Unit, Criminal Investigative

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 21 - 42

Division. The title only of the person (Security Officer, Manager, etc.) who is to receive the wanted notices together with the organization's full address, including ZIP Code, and the number of wanted notices required, should be clearly set forth.

EFFECTIVE: 07/23/90

21-28 FUGITIVE|SUBPROGRAM|- POLICY ON FUGITIVE APPREHENSION IN
FBI AND DRUG ENFORCEMENT ADMINISTRATION (DEA) CASES AND
U.S. MARSHALS SERVICE (USMS) INVOLVEMENT

EFFECTIVE: 07/23/90

21-28.1 Background|(See MIOG, Part I, 115-1.)|

|(1)|On 8/11/88, the Attorney General authorized the following policy, which went into effect on 9/22/88. This policy applies to fugitives in FBI and DEA cases and foreign fugitives and supersedes all prior interagency Memoranda of Understanding on fugitive apprehension responsibility in FBI and DEA cases, including the 1979 agreement between the FBI and the USMS and the 1982 agreement between the FBI and DEA. |This policy was further clarified by the Attorney General's Office on 12/11/91 wherein a definitive ruling was made that the FBI will maintain primary investigative jurisdiction regarding conspiracies to violate the Escape and Rescue Statutes (ERS).

(2) Since these investigations can be complex, involving

b2
b7E
[REDACTED] these matters should be investigated under Bureau classification 90, Irregularities in Federal Penal Institutions (IFPI). The purpose of this policy is to prevent escape and to ensure appropriate investigation in order to support prosecution of those involved in conspiracies to escape Federal custody or confinement.

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 21 - 43

EFFECTIVE: 09/07/93

21-28.2 Arrest Warrants

(1) The FBI and DEA shall have apprehension responsibility on all arrest warrants resulting from their own investigations.

(2) Notwithstanding paragraph (1), the DEA may delegate apprehension and administrative responsibility (including initial NCIC entry) to the USMS whenever the subject of a DEA arrest warrant is not apprehended within seven days after issuance of the arrest warrant, or it may elect to retain this responsibility in individual cases for investigative purposes. The delegation becomes effective upon notification of USMS by DEA.

(3) In cases of joint FBI-DEA investigations and multiple agency task force investigations, it shall be the decision of the lead agency whether to have the investigating agencies maintain apprehension responsibility themselves or delegate apprehension responsibility to the USMS.

EFFECTIVE: 07/23/90

21-28.3 Post-Arraignment

(1) The FBI, in an FBI case, shall have apprehension responsibility whenever there is a bond default violation prior to adjudication of guilt.

(2) The USMS, in a DEA case, shall have apprehension responsibility whenever there is a bond default violation prior to adjudication of guilt.

EFFECTIVE: 07/23/90

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 21 - 44

21-28.4 Post-Conviction/Other Than Escapes

(1) The USMS shall have apprehension responsibility whenever after adjudication of guilt there is a Federal probation, parole, or bond default or mandatory release violation, except as set forth below.

(2) The USMS will promptly notify the original investigating agency whenever there is such a violation.

EFFECTIVE: 07/23/90

21-28.5 Escapes

(1) The USMS shall have apprehension responsibility whenever there is a violation of the Federal ERS. However, any allegation(s) of conspiracy to escape will be investigated by the FBI under Bureau classification 90 (IFPI). (See 21-28.6(4).)

(2) The USMS will promptly notify the original investigating agency whenever there is an escape.

EFFECTIVE: 09/07/93

21-28.6 Exceptions (See MIOG, Part II, 21-28.8(6).)

(1) Upon written notice to the USMS as provided in paragraph (3) below, the FBI will have exclusive apprehension responsibility in its own cases at any stage when a fugitive, or the organization of which he/she is a current member, is the subject of an existing FBI Foreign Counterintelligence, FBI Organized Crime, or FBI Terrorism investigation. (The term, Organized Crime, covers those organizations being investigated by the FBI as a "racketeering enterprise" pursuant to the Attorney General's Guidelines on Racketeering Enterprise Investigations and the criteria set forth in Part I, Section 92 of this manual.)

(2) Upon written notice to the USMS as provided in paragraph (3) below, the FBI or DEA may assume apprehension responsibility in any case where the FBI or DEA is seeking the

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 21 - 45

fugitive on an arrest warrant based on charges filed by it for an additional offense beyond the one for which the subject is a fugitive.

(3) In those situations where the FBI or DEA elect to assume apprehension responsibility, agency Headquarters shall immediately notify USMS Headquarters. The assumption of apprehension responsibility becomes effective seven calendar days after receipt of notice by USMS Headquarters. During that seven-day period, the investigating agency and USMS shall fully coordinate their fugitive apprehension efforts. The USMS for good cause may request the investigating agency to consent to the continuation of USMS apprehension efforts for a limited or indefinite period of time. Should that consent be declined, the USMS may request the Associate Attorney General to approve a limited or indefinite continuation. Such a request will be made within the seven-day period. In making this decision, the Associate Attorney General will consider the relative interests of each agency and the need for swift apprehension of the fugitive. The Associate Attorney General shall make this decision within 48 hours of receiving a request. The fugitive investigation will continue to be coordinated by the agencies during the time the Associate Attorney General is considering the matter. | (See MIOG, Part II, 21-28.9(1).) |

(4) In the event of an escape, it is particularly important that fugitive apprehension efforts be closely coordinated during the seven-day period following notice given as outlined in paragraph (3). The investigating agency shall assume sole apprehension responsibility at the conclusion of the prescribed period. However, the USMS and the agency shall be responsible for maintaining an orderly transition, which would include capitalizing on leads developed by the USMS during its initial investigation of escape. | Any allegation(s) of conspiracy to escape should be investigated by the FBI as stated in the Escapes Section (21-28.5(1)). |

(5) The investigating agency shall return apprehension responsibility to the USMS if the reason for the exception is no longer applicable. (For example, if the FBI is seeking an escapee, because it has an arrest warrant for him/her, and the arrest warrant is later withdrawn because the case is dismissed, apprehension responsibility for the escape would be returned to the USMS.)

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 21 - 46

EFFECTIVE: 09/07/93

21-28.7 Unlawful Flight Statute

(1) The FBI shall have such jurisdiction in locating fugitives pursuant to the Unlawful Flight Statutes (Title 18, Sections 1073 and 1074), but, in exercising it, the FBI will not seek an Unlawful Flight warrant when the USMS is already seeking the fugitive as an escapee, probation/parole, mandatory release, or bond default violator. Nor will the FBI seek an Unlawful Flight warrant against any fugitive already sought by the USMS pursuant to the Federal Escape and Rescue Statutes. The above provisions shall not preclude the USMS from providing available information to state and local law enforcement agencies about fugitives being sought by their jurisdictions. The initiation of formal fugitive investigations involving state and local fugitives will be done through the Unlawful Flight process set forth above, except for special apprehension program (such as Fugitive Investigative Strike Teams and Warrant Apprehension Narcotics Teams) and other special situations approved by the Associate Attorney General.

(2) The FBI will notify the USMS of any state or local requests for Unlawful Flight assistance in situations described above. The FBI will also notify local or state authorities that the USMS is already seeking that person. In these situations, the USMS will notify the appropriate local or state authorities when a fugitive has been apprehended, so that a local detainer can be placed.

(3) If state or local authorities request the assistance of the USMS in locating or apprehending a fugitive and it is determined that the fugitive is the subject of an FBI or DEA warrant, the USMS shall refer the requesting agency to the FBI or DEA for assistance and notify the FBI or DEA of the request by state or local authority.

EFFECTIVE: 09/20/89

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 21 - 47

21-28.8 Foreign Fugitives

(1) The USMS shall have location and apprehension responsibility for a fugitive sought in the United States by a foreign government, except as provided below.

(2) The FBI shall have location and apprehension responsibility for such a foreign fugitive: (a) whenever the fugitive, or the organization of which he/she is a current member, is the subject of an existing FBI Foreign Counterintelligence, FBI Organized Crime, or FBI Terrorism investigation; (b) whenever the FBI is seeking the fugitive on an arrest warrant for a Federal offense; (c) whenever the fugitive is the subject of an FBI investigation which it is currently conducting at the request of the foreign government concerned; or (d) whenever a referral has been made exclusively to the FBI through one of its legal attaches.

(3) The DEA shall have location and apprehension responsibility for such a foreign fugitive: (a) whenever the fugitive is the subject of a DEA investigation which it is currently conducting at the request of the foreign government concerned; or (b) whenever a referral has been made exclusively to the DEA through one of its country attaches.

(4) INTERPOL-U.S. NATIONAL CENTRAL BUREAU (USNCB) shall, upon receiving from a foreign government a request for the location or apprehension of such a fugitive, refer such a request to the USMS, FBI or DEA in accordance with the provisions of paragraphs (1) through (3) above. However, nothing herein precludes referral of such requests instead, where appropriate, to the U.S. Immigration and Naturalization Service for action under the immigration laws or to state and local law enforcement authorities in accordance with INTERPOL'S internal procedures and practices. (This policy is applicable to Department of Justice agencies only. If a Department of the Treasury agency received an exclusive referral, it would, of course, handle the matter pursuant to Department of the Treasury or agency policy.)

(5) Upon receiving a request from a foreign government for the location or apprehension of a fugitive, the FBI, DEA, USMS or the Office of International Affairs (OIA), Criminal Division, shall notify INTERPOL-USNCB of this fact to determine the existence of any parallel request or investigation with respect to the fugitive.

(6) Once a matter has been referred to the FBI, DEA, or USMS by INTERPOL-USNCB, the notice, coordination, and review

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 21 - 48

procedures set forth in 21-28.6, above, shall govern if either of the other two agencies concludes it should have fugitive apprehension responsibility under the provisions of this policy.

EFFECTIVE: 09/20/89

21-28.9 Interagency Coordination

(1) In cases where the USMS is requested to provide apprehension assistance or to seek the apprehension of a fugitive sought by a Federal agency other than the FBI or DEA, and it is determined by the USMS through an NCIC or other appropriate inquiry that the FBI or DEA has an existing warrant, the USMS will notify the requesting agency of the existing FBI or DEA warrant. If the requesting Federal agency continues to seek USMS assistance, the USMS will notify the FBI or DEA of the request for assistance by the other agency. The FBI or DEA will either defer the USMS the fugitive apprehension responsibility in the particular case or assert the need to continue its apprehension responsibilities in regard to the fugitive. The USMS shall defer in those instances to the FBI or DEA, unless the requesting agency declines to accept the deferral. In such instances, the requesting agency, the USMS, and the FBI or DEA shall confer at the headquarters level to resolve the issue. If a resolution is not reached between the involved agencies on the issue, it will be referred to the Associate Attorney General under the same provisions as set forth in Section 21-28.6(3) above.

(2) The Director of the FBI, the Administrator of DEA, and the Director of the USMS shall each designate a representative to a working group charged with developing procedures to implement this policy. The Chief of Interpol (USNCB) may also designate a representative to attend any meetings concerned with implementation of policy set out in Section 21-28.8.

(3) Nothing in this policy prevents an individual investigating agency from delegating its designated apprehension responsibility in a particular case or category of cases to the USMS, or prevents the USMS in turn from delegating its designated apprehension responsibility to the investigating agency.

EFFECTIVE: 09/20/89

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 21 - 49

21-29 ARREST, LOCATES, AND CRIMINAL SUMMONS STATISTICS (See MIOG, Part I, 25-10, 76-1.8, 76-2.9, 76-3.13, 88-12, & 115-7.)

(1) Statistics or fugitive apprehensions will no longer be scored as such.

(2) In lieu of fugitive apprehensions, all arrests, locates, and criminal summons will be utilized for statistical purposes.

(3) Arrests should be claimed only when Special Agents participate in the actual apprehension. Locates should be claimed in those instances where our investigative efforts or cooperative facilities result in the location of a suspect but Special Agents did not effect the arrest. Criminal summons should be claimed when a subject appears in response to a criminal summons.

(4) Arrests, locates, and criminal summons statistics will only be recorded and credited through the entry of Form FD-515, Accomplishment Report, into the Integrated Statistical Reporting and Analysis Application (ISRAA) by the office entitled to the statistic.

(5) In claiming all arrests and locates, the FD-515 must also reflect the subject's fugitive "A," "B," "C," or "D" priority. This priority is to be applied even where, technically, the subject may not be a fugitive such as a bank robber arrested in the act of the robbery. In claiming a criminal summons, there will be no "A," "B," "C," or "D" priority breakdown.

(6) The FD-515 should be promptly submitted within 30 days after the arrest, locate, or criminal summons.

(7) Submission of the FD-515, concerning arrests, locates, and criminal summons, should not be delayed to report other types of statistical accomplishments covered by said form; however, more than one type of statistic can be claimed on the same FD-515 if appropriate.

(8) In the event the office submitting the FD-515 (and thereby claiming the statistic since this form does not provide for crediting statistics to an office other than the submitting office) is an auxiliary office, a copy of the form should be provided the office of origin for filing in its substantive case file.

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 21 - 50

(9) It will be the responsibility of the office of origin to ensure there is no duplication of reporting statistics.

(10) In all fugitive matters, including deserter cases, a ROUTINE teletype must still be appropriately submitted to FBIHQ and the office of origin to report the fugitive's arrest or location in addition to the FD-515. (See MIOG, Part I, 42-12.)

EFFECTIVE: 11/01/93

21-30 DISPOSITION OF ARRESTS

The disposition of all arrests involving all fugitives should be promptly obtained during the course of the investigation. If appropriate, information obtained from these dispositions should be utilized for lead information.

EFFECTIVE: 12/10/91

|| 21-31 DELETED |

EFFECTIVE: 12/10/91

|| 21-31.1 DELETED |

EFFECTIVE: 12/10/91

|| 21-31.2 DELETED |

EFFECTIVE: 12/10/91

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 22 - 1

SECTION 22. FBI BOMB DATA CENTER

22-1 FBI BOMB DATA CENTER

For information on the Bomb Data Center Program, please refer
to Part II, Section 13-16.9 of this manual.

EFFECTIVE: 09/22/87

22-2 DELETED

EFFECTIVE: 09/22/87

22-3 DELETED

EFFECTIVE: 09/22/87

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 23 - 1

SECTION 23. MISCELLANEOUS

23-1 CRYPTONYMS (CODE NAMES)

EFFECTIVE: 01/31/78

23-1.1 Use In Major Case Title

The Criminal Investigative Division (CID) and the Intelligence Division (INTD) both currently use cryptonyms in major case titles for convenience or security reasons.

Cryptonyms are generated by either FBIHQ or by field offices handling the investigation. In either event, the cryptonym (or code name) should be submitted on a UACB basis for searching through FBIHQ indices to determine if that particular word has been previously utilized or indexed.

EFFECTIVE: 01/31/78

23-2 THE FAIR CREDIT REPORTING ACT (FBI USE OF CREDIT INFORMATION) TITLE 15, USC, SECTION 1681

The Fair Credit Reporting Act (FCRA) which became effective 4/25/71, requires consumer reporting agencies (i.e., credit bureaus) to follow certain procedures designed to protect the confidentiality, accuracy, relevancy, and proper use of credit information. The following provisions of the Act are of interest to the FBI:

EFFECTIVE: 01/31/78

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 23 - 2

23-2.1 Section 1681a. Definitions

(1) Consumer Report - information communicated by a consumer reporting agency which relates to a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living.

(2) Investigative Consumer Report - a consumer report that is based on personal interviews with neighbors, friends, associates, or acquaintances of the consumer.

EFFECTIVE: 01/31/78

23-2.2 Section 1681b. Permissible Purposes of Consumer Reports

Consumer reports may be furnished under the following specified purposes which have relevance to our investigations:

- (1) By appropriate court order.
- (2) According to the written instructions of the consumer (e.g., waivers in Bureau applicant investigations);
- (3) Where the recipient intends to use the information in connection with an employment application;
- (4) Where the recipient has a legitimate business need for the information in connection with a business transaction involving the consumer (e.g., Ascertaining Financial Ability cases).

EFFECTIVE: 01/31/78

23-2.3 Section 1681f. Disclosures to Government Agencies

Notwithstanding the provisions of Section 1681b, consumer reporting agencies may furnish a governmental agency identifying information regarding a consumer limited to:

- (1) His name;
- (2) Address;

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 23 - 3

- (3) Former address;
- (4) Places of employment;
- (5) Former places of employment.

EFFECTIVE: 01/31/78

23-2.4 Section 1681g. Disclosure to Consumers

(1) A consumer, upon his request to a consumer reporting agency may obtain:

(a) The information contained in his credit file;
and,

(b) The identities of those receiving consumer reports concerning him for the 2-year period preceding his request where the reports were for employment purposes or the 6-month period preceding his request if the reports were furnished for any other purpose.

(2) If, for any reason, an investigative consumer report is requested, the consumer reporting agency, under the provisions of Section 1681d, must notify the consumer. This notification must be made not later than 3 days following the request. After receiving notification, the consumer may request the person, etc., who requested the investigative consumer report to provide him with complete disclosure of the nature and scope of the investigation requested not later than 5 days following receipt of the consumer's request.

EFFECTIVE: 01/31/78

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 23 - 4

23-2.5 Section 1681e. Compliance Procedures

(1) Consumer reporting agencies are obligated to develop procedures which are designed to insure that a person, etc., receiving consumer reports uses that information for one of the permissible purposes set forth under Section 1681b and for no other purpose.

(2) To insure that the FBI, through inadvertence, does not improperly use credit data, all consumer reports received from a consumer reporting agency must be clearly identified when reported in any Bureau communication.

(3) All personnel must insure that consumer reports are not used for any purpose not specifically permitted under Section 1681b of the Act. Improper use of consumer reports could result in evidence being suppressed in a criminal proceeding against the consumer; civil litigation seeking to enjoin the FBI's continued use or possession of such information; and/or discovery of FBI files.

(4) Employees who make use of the following form communications should insure that any information, derived from a consumer reporting agency, is clearly identified in completing the form and that it was obtained and disseminated in a manner permissible under FCRA:

(a) FD-125 (Record Request);

(b) FD-159 (Record of Information Furnished Other Agencies).

EFFECTIVE: 01/31/78

23-2.6 Summary

(1) In view of the limitations imposed by this law, information requested of consumer reporting agencies will be restricted to:

(a) Identifying information (name, address, former addresses, place of employment, and former places of employment) which may be obtained in any case and

(b) Consumer reports, which may be obtained for employment purposes of the applicant alone in applicant-type

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 23 - 5

investigations and where the Bureau has a legitimate business need for the information such as Ascertaining Financial Ability cases.

(2) When reporting information obtained from a consumer report, the source of the data should be clearly identified as a consumer reporting agency. Subsequent use of such information contained in Bureau files is prohibited except for the purposes authorized by FCRA.

(3) Consumer reporting agency contract matters including whether a waiver need be signed by applicants in employment cases will be handled on a case-by-case basis as such problems arise.

(4) In light of the preceding disclosure requirements, requests for consumer reports and investigative consumer reports should be made only in exceptional cases, and should never be made if there is any likelihood that the consumer's knowledge that the FBI has requested such information would be detrimental to an investigation.

EFFECTIVE: 01/31/78

23-2.7 Penalties

EFFECTIVE: 01/31/78

23-2.8 Section 1681n, o, q, and r. Civil and Criminal Liability for Willful or Negligent Noncompliance

(1) Negligent failure to comply with any requirement imposed by the FCRA renders the negligent consumer reporting agency or user of credit information liable to the consumer for actual damages suffered by the consumer as well as court costs and reasonable attorney's fees resulting from a successful action to enforce liability under the Act.

(2) Willful noncompliance of the FCRA may result in the awarding of punitive damages in addition to actual damages, court costs and attorney's fees.

(3) Any person who knowingly and willfully obtains credit information from a consumer reporting agency under false pretenses may be fined no more than \$5,000 or imprisoned for not more than one year

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 23 - 6

or both.

(Refer to Part I, Section 62-5 of this manual for details relating to the Bureau's jurisdictional responsibilities under the criminal provisions of the Fair Credit Reporting Act.)

EFFECTIVE: 09/26/90

23-3 INVESTIGATIVE

EFFECTIVE: 09/26/90

23-3.1 Information Desired from Outside the Field Office Territory

(1) Investigative information from another field office is to be obtained by that office unless extraordinary haste requires direct communication. When the exigencies of a case, emergencies, or economy and common sense dictate, an employee, if authorized by his/her SAC, may enter the territory of another field office. The concurrence of the SAC of the entered office is to be obtained prior to the travel.

(2) Information which should be obtained by direct communication even though the addressee is in another field office:

(a) For disposition of arrests, use FD-10 to obtain incomplete information (for New York City, send two copies of FD-10 to the New York Division of Criminal Justice Services, Executive Park Tower, Stuyvesant Plaza, Albany, New York 12203-3764, rather than the New York City Police Department). Make notation on identification record or other pertinent serial in file that FD-10 has been sent. When FD-10 is returned, note pertinent information from form in file; forward FD-10 to Criminal Justice Information Services (CJIS) Division in lieu of a disposition form (R-84), provided it shows the final disposition or shows that the disposition data is unavailable.

- (b) Automobile registrations data
- (c) Driver's license information
- (d) Similar data

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 23 - 7

- (e) Filing of detainers with some agency
- (f) Status of detainers
- (g) Government bonds - Use FD-123, concerning purchase or redemptions; specify information desired; send FD-123 in duplicate.

EFFECTIVE: 12/02/94

23-3.2 Prohibition Against Photographing Money, Securities and Checks

Title 18, USC, Section 474. Prohibits the photographing of any national bank currency, Federal Reserve notes, U.S. or foreign government securities or obligations, except by direction of some proper officer of the United States. However, Part 404, Chapter 4, Title 31, of the Code of Federal Regulations grants authority to all banks and banking institutions to make film records of paper money, U.S. Government securities and checks, and to project such records on a screen provided the film records are maintained as confidential. This part states that no prints, enlargements, and other reproductions of such film records may be made except with the permission of the Secretary of the Treasury, the Treasurer of the U.S., the Commissioner of Public Debt, the Director of the Secret Service, or such officers as may be designated by them.

EFFECTIVE: 09/26/90

23-3.3 Deleted

EFFECTIVE: 10/18/88

23-4 LEGAT OPERATIONS

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 23 - 8

EFFECTIVE: 10/18/88

23-4.1 Definition of a Legal Attache (Legat)

A Legat is an FBI liaison representative stationed in an American Embassy abroad who is responsible for liaison with foreign police and intelligence agencies in matters of interest between these agencies and FBIHQ.

EFFECTIVE: 10/18/88

23-4.2 Jurisdiction of Legal Attaches

FBI Agents have no jurisdiction in foreign countries and Legats and border office Agents, even though invited or requested by foreign authorities to participate in and/or observe arrests and searches of subjects or transportation of prisoners may not do so.

EFFECTIVE: 10/18/88

23-4.3 Official Business in a Foreign Country

Where official business requires more than two days in a foreign country authority must be obtained from FBIHQ. The letter requesting authority is to be sent UACB and should contain an estimate of time to be spent.

EFFECTIVE: 10/18/88

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 23 - 9

23-4.4 Interviews in Foreign Countries

Persons interviewed by FBI Agents while in police custody in a foreign country must be given the usual warning of rights under American Federal law provided there is no objection from the foreign police officer. If he/she objects, feeling our warning is not consistent with the law of his/her country and might work unfavorably on prosecution of the subject there, the officer should be requested to give the warning as required by the law of his/her country. Record the wording of this warning and the time and circumstances of its issuance.

EFFECTIVE: 10/18/88

23-4.5 Foreign Leads

Leads for all foreign countries should be submitted to FBIHQ for coverage through Legat or liaison with U.S. Department of State, Central Intelligence Agency and other established channels. Leads should be set out in LHM furnishing six copies of same to FBIHQ.

EFFECTIVE: 10/18/88

23-4.6 Countries/Areas Covered by Legats

Territorial allocation details are no longer maintained in the manuals. An up-to-date listing is available in the FOIMS Tables Application, "Territorial Allocation, Foreign Territorial Allocation" options.

EFFECTIVE: 11/16/93

CONFIDENTIAL

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 23 - 10

23-4.7 Canadian Border Leads

Normally, Canadian leads are handled through Legat Ottawa; however, offices along the Canadian border, through liaison with cooperative Canadian law enforcement agencies, handle Canadian leads in criminal matters where time is of the essence and in criminal matters of local interest, except in deserter and selective service matters. Leads on security matters where time is of the essence or where previously approved by FBIHQ are handled with RCMP by border offices on a divisional headquarters level.

EFFECTIVE: 03/23/92

23-4.8 Mexican Border Leads

[REDACTED]

(c) b1

EFFECTIVE: 03/23/92

ALL INFORMATION CONTAINED
HERE IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

CONFIDENTIAL

Sensitive

PRINTED: 02/18/98

Administrative 6-298
CLASSIFIED BY: SP5JC/ndm
REASON: 1.5 (2nd)
DECLASSIFY ON: X, 6

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 23 - 11

23-4.9 Leads for the Northern and Central Caribbean Areas - Miami
and San Juan Divisions

Leads for the Northern and Central Caribbean areas are normally covered by the Liaison Officers at the Miami and San Juan Divisions. The Liaison Officer, Miami, has regional responsibilities in the Bahamas, Belize, Bermuda, Cayman Islands, Costa Rica, El Salvador, Guatemala, Honduras, Jamaica, Nicaragua, and the Turks and Caicos Islands. The Liaison Officer, San Juan Division, is responsible for maintaining liaison and the coverage of leads in the countries of Anguilla, Dominican Republic, Haiti, Montserrat, and St. Christopher (formerly St. Kitts-Nevis). At any time that leads are forwarded to the Liaison Officers at Miami and San Juan Divisions, a copy of the communication is to be designated for the Office of Liaison and International Affairs (OLIA), Attention: Foreign Liaison Unit.

EFFECTIVE: 03/23/92

23-5 DELETED

EFFECTIVE: 03/23/92

23-6 TITLE XI, RIGHT TO FINANCIAL PRIVACY ACT OF 1978 (RFPA)

EFFECTIVE: 03/08/79

23-6.1 Statute

The RFPA was passed as Public Law 95-630, effective 3/10/79 (T 12, USC, Section 3401, et seq).

EFFECTIVE: 03/08/79

23-6.2 Access to Financial Records

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 23 - 12

EFFECTIVE: 03/08/79

23-6.2.1 Intent

An individual customer has the right to be notified in advance when the Federal Government is seeking his or her financial records from a financial institution in connection with a law enforcement inquiry and has the right to challenge that intended access. Exceptions to both customer notice and challenge provisions are available in special situations. For exceptions see 23-6.7.2, 23-6.9, and 23-6.10.

EFFECTIVE: 03/08/79

23-6.2.2 Methods Available to FBI (For further information see 23-6.6)

(1) RFPA of 1978

- (a) Customer authorization or waiver
- (b) Search warrant
- (c) Judicial subpoena
- (d) Formal written request to financial institution

(2) Federal Grand Jury Subpoena - access exempt from RFPA
(but new use restrictions)

EFFECTIVE: 03/08/79

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 23 - 13

23-6.2.3 Methods Not Available to FBI

(1) Administrative subpoenas and summons under RFP, except as provided in Title 12, USC, Sections 3402 and 3405. Sections 3402 and 3405 of Title 12, U.S. Code, permit government officials to obtain bank records if relevant to a legitimate law enforcement inquiry.

(2) Informal access - not authorized by RFP

EFFECTIVE: 06/03/97

23-6.3 Definitions

EFFECTIVE: 03/08/79

23-6.3.1 Financial Institution

This includes all banking and banking-type institutions as well as companies issuing credit cards, even though not a bank-type institution, and consumer finance companies located in the United States, District of Columbia, Puerto Rico, Guam, American Samoa, and the Virgin Islands.

EFFECTIVE: 03/08/79

23-6.3.2 Financial Record

Any original, copy of or information "knowingly derived from" a record pertaining to present or past customer's relationship with a financial institution. Excluded are records or information not identifiable with an individual customer or those which reside in the account of a third party such as check endorsements or items deposited by third party and obtained from that person or corporation. There should be no conscious circumvention of RFP.

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 23 - 16

EFFECTIVE: 03/08/79

23-6.6.1 Customer Authorization

Customers may authorize access to identified records up to 90 days by signing a revocable statement specifying the recipient, purpose for disclosure and that the customer is aware of his or her rights under RFPA. Certification of Compliance is required when the records are obtained. This would apply in applicant-type investigations or where financial records of a cooperative witness are being sought.

EFFECTIVE: 03/08/79

23-6.6.2 Search Warrants

A search warrant may be used under RFPA with notice to the customer of the search occurring within 90 days after execution. There is no change in the procedures to obtain a search warrant. Additional delays of up to 90 days may be granted by a court when it is shown that notice would seriously jeopardize a continuing investigation (see 23-6.7.2). The institution may be prohibited from notifying the customer by court order issued when the delay is authorized.

EFFECTIVE: 03/08/79

23-6.6.3 Formal Written Request

The FBI is authorized by T 28, CFR, Section 47.1, to use the written request provided for in RFPA. This is a new method of access and requires the cooperation of the financial institution. Required notice advises the customer his or her records are being sought and the nature of the inquiry which may include a statement to the effect that the customer is not the subject of the investigation. The customer has 10 days if notice is served and 14 days if notice is mailed to complete and file an affidavit detailing why the records are not relevant to a legitimate law enforcement inquiry. The customer must then serve a copy of the affidavit on the Government authority and be prepared to present in court additional facts. If the customer

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 23 - 15

order. Other recourse such as Obstruction of Justice is available. Judicial subpoenas require the financial institution to commence compiling the records upon service.

EFFECTIVE: 03/08/79

23-6.5 Certification of Compliance

Before records may be obtained under any provision of the RFPFA, a supervisory official of the FBI must submit to the financial institution a certificate stating that all applicable provisions of the Act have been complied with. Good faith reliance by the employees and agents of the financial institution upon the Government certification of compliance absolves the institution of civil liability for any improper disclosure of records. This certification is not required when customer records are sought pursuant to a Federal Grand Jury subpoena. For the purpose of RFPFA, "supervisory official" is defined and limited to (other than FCI activities) any Headquarters or field division supervisor (including Supervisory Senior Resident Agent) or officially designated relief supervisor acting for the supervisor or any official of higher rank.

EFFECTIVE: 03/08/79

23-6.6 Methods of Access

For access in cases of emergency see 23-6.9. If account identification information is being sought the notice and challenge provisions and restrictions on interagency transfers do not apply when only identification information about a customer is needed, i.e., name, address, type of account and account number. This data must be obtained through a written request. In addition to account information only, more specific inquiries such as the account number associated with a particular transaction or class of transactions may be obtained. Once the existence and identification of a customer account is established, then one of the access methods listed below must be used to obtain any additional information. For dissemination of information see MAOP, Part II, 9-10, and MIOG, Part II, 23-6.11.

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 23 - 14

EFFECTIVE: 03/08/79

| 23-6.3.3 Government Authority

| RFPA applies to all Federal agencies including FBI or any officer, employee or agent thereof.

EFFECTIVE: 03/08/79

| 23-6.3.4 Customers Covered

| Any natural person or partnership of five or fewer individuals are covered. Not covered by RFPA are corporations, associations, larger partnerships or other legal entities.

EFFECTIVE: 03/08/79

| 23-6.3.5 Law Enforcement Inquiry

| Any lawful investigation or official proceeding inquiring into a violation of or failure to comply with any criminal or civil statute or a regulation, rule or order issued thereunder is considered as a law enforcement inquiry.

EFFECTIVE: 03/08/79

| 23-6.4 Responsibility of Financial Institutions

| RFPA prohibits financial institutions from providing financial records to the Government, unless access is authorized by one of the exceptions such as grand jury subpoenas or unless access is accomplished by one of four methods under procedures mandated. Notwithstanding these restrictions, financial institutions are permitted to notify Government authorities of possible violations of law reflected in their records. Financial institutions do not have to comply with formal written request or a customer authorization. In addition, there are no criminal penalties under RFPA to prevent an institution from notifying its customer in the absence of a court

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 23 - 17

does not comply with the above within prescribed time limits, the records may be made available. As a practical matter, a reasonable period (possibly four days) should be allowed prior to access where the customer files challenge by mail on the last day of the 10- or 14-day period. In effect, the 10- or 14-day period becomes a 14- to 18-day period to be cautious. A written request may be executed by any supervisory official, previously defined (see 23-6.5), of the FBI. Notice to the customer may be delayed for period of up to 90 days.

EFFECTIVE: 03/08/79

23-6.6.4 Judicial Subpoena

Judicial subpoenas are any court order to produce records, other than a grand jury subpoena, the most common of which is the trial subpoena directed at a party not involved in litigation. When used, a copy of the subpoena, together with mandatory customer notice, is served or mailed to the customer. The notice provisions for the judicial subpoena are the same as for the written request, above.

EFFECTIVE: 03/08/79

23-6.6.5 Grand Jury Subpoena (See MIOG, Part II, 23-6.10.5.)

Such subpoenas are not covered by RFPA with respect to access and notification. However, the RFPA does place restrictions on the handling and use of customer financial records obtained by a grand jury. Access to such records, or information abstracted for reporting or lead purposes, must be limited to authorized persons, i.e., those assisting an attorney for the government in a specific criminal investigation; and, when records are not in use, they must be placed in a subfile which is locked in a container with a combination lock (see MIOG, Part II, 2-9.5 and 2-9.7). Grand jury-subpoenaed financial records should be appropriately marked as both grand jury material (see MIOG, Part II, 2-9.7(2)), and as subject to the RFPA (see MAOP, Part II, 9-10). Information extracted from financial records subject to the RFPA must be treated as grand jury material "unless such record has been used in the prosecution of a crime for which the grand jury issued an indictment or presentment . . ." (see MIOG, Part II, 2-9.5.1 (4)(a)).

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 23 - 18

EFFECTIVE: 07/12/95

| 23-6.7 Customer Notice

EFFECTIVE: 03/08/79

| 23-6.7.1 Contents of Notice

The purpose of the investigation must be stated but without reference to specific title and section of the U. S. Code. Generic terms may be used to describe the offense such as: fraud, bribery, extortion, etc., similar to the character of cases we now use. Notice must state the name and business address of the supervisory official to be served with copies of customer challenge papers. The supervisory official is he or she who initiated the access process.

EFFECTIVE: 03/08/79

| 23-6.7.2 Delay of Notice

(1) Delays of customer notice may be obtained for access sought through judicial subpoenas, formal written request, search warrants and subsequent interagency transfer. Delays of up to 90 days (or 180 days in case of a search warrant) may be applied for to a court where there is a reason to believe (lesser standard than probable cause) that notice would cause danger to life or physical safety, flight from prosecution, destruction of evidence, intimidation of a witness, or other serious jeopardy to an investigation or a trial.

(2) To obtain a delay of notice, a sworn written statement must be presented to a judge or magistrate that one or more of above situations exist. Extensions of the delay of notice may be similarly obtained based on necessity.

(3) In addition to delaying the timing of the Government notification to the customer, the court order issued will prohibit the

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 23 - 19

financial institution from disclosing to the customer that records pertaining to that customer are being sought. There is no such provision in the RFPA with respect to access through grand jury subpoenas to prohibit the financial institution from notifying the customer.

EFFECTIVE: 03/08/79

23-6.8 Customer Challenges

(1) A customer may challenge a judicial subpoena or a formal written request in instances where notice was not delayed. Grand jury subpoenas, being generally excepted by RFPA and having no notice provisions, are not challengeable at the time of access. Within 10 or 14 days (more practically, 14 or 18 days, see 23-6.6.3), depending on the method of notice (served or mailed), the customer may file in U.S. District Court a motion to quash a judicial subpoena or an application to enjoin the Government from pursuing a formal written request. In support of the motion or application, the customer must file a sworn statement that he or she:

(a) is the person whose records are being sought and,

(b) has reason to believe the records sought are not relevant to the inquiry, or

(c) That the RFPA has not been substantially complied with, or

(d) any other legal reason for denying access.

(2) The challenge does not shift the burden of proof to the customer, but does require more than only an allegation. The Government must then convince the judge or magistrate the records sought are relevant to a legitimate law enforcement inquiry. Relevance covers anything that might be Used as evidence or that might logically lead to evidence. The Government may have to file a response, in camera if appropriate, and the court may require additional proceedings but all within seven days from the filing of the Government's response. Denial of customer challenge motions or applications are not appealable until after the trial or other proceeding.

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 23 - 20

(3) If the Government fails to justify its attempted access, the subpoena is quashed or the formal written request enjoined. If the Government does support its burden, the subpoena will be enforced and the formal written request may be pursued with the financial institution. The financial institution is not compelled to comply with the formal written request.

(4) If, after access following an unsuccessful challenge, no prosecution or other proceeding is to be brought against the customer (always the case when customer is witness and not subject), customer must be so notified by the requesting Government agency. Close coordination between the field office and the U.S. Attorney's Office will be required.

(5) Any applicable statute of limitations is suspended during the time the customer's motion or application is pending in court.

(6) In the case of judicial subpoenas, venue for the customer challenge is restricted to the court issuing the subpoena. When a formal written request is used, the customer may challenge in any one of three districts:

- (a) the District of Columbia,
- (b) the site of the financial institution
- (c) the site of the residence of the customer.

EFFECTIVE: 03/08/79

23-6.9 Emergency Access

(1) In instances where notice and challenge delays could create imminent danger of physical injury, serious property damage or flight from prosecution, access may be had immediately by merely presenting the financial institution with the certificate of compliance. However, post notice to customer is required as soon as possible.

(2) Within five days after access, a supervisory official must file in court a signed sworn statement setting forth the grounds for the emergency access.

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 23 - 21

EFFECTIVE: 03/08/79

| 23-6.10 Exceptions to RFPA

EFFECTIVE: 03/08/79

| 23-6.10.1 Financial Institutions

The RFPA does not require customer notice when the institution in possession of such records is the subject of the investigation. However, the certificate of compliance is necessary. Customer records obtained under this exception may only be used or transferred in furtherance of that specific investigation. If evidence of another violation is developed, enough information (not records) may be given the appropriate agency, including FBI, to identify the record and violation. Thereafter, the receiving agency may proceed as if independent of the initial inquiry.

EFFECTIVE: 03/08/79

| 23-6.10.2 Corporations or Other Legal Entities

Investigations directed at corporations or other legal entities not protected by RFPA may be conducted in same fashion as 23-6.10.1 above.

EFFECTIVE: 03/08/79

| 23-6.10.3 Not Identifiable with Customer

Records can be disclosed by a financial institution if they or the information contained therein are not identified with or identifiable as being derived from the records of a particular customer.

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 23 - 22

EFFECTIVE: 03/08/79

| 23-6.10.4 Parties in Interest

| The RFPA does not apply when the Government and the customer are litigants in a judicial or an administrative adjudicatory proceeding.

EFFECTIVE: 03/08/79

| 23-6.10.5 Federal Grand Jury

| The RFPA does not affect the obtaining of customer financial records (see 23-6.6.5). No compliance certificate is required.

EFFECTIVE: 03/08/79

| 23-6.10.6 Foreign Counterintelligence

| See "Foreign Counterintelligence Manual" for instructions.

EFFECTIVE: 03/08/79

| 23-6.10.7 Telephone Company Toll Records

| These records are not covered by the provisions of RFPA.

EFFECTIVE: 03/08/79

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 23 - 23

23-6.10.8 Other

Other exemptions specifically excluded are:

(1) Certain designated supervisory agencies of financial institutions.

(2) Internal Revenue Service.

(3) General Accounting Office.

(4) Certain reports required of financial institutions.

(5) Identifying account information only (see 23-6.6).

(6) The administration of guaranty or loan insurance programs. Notification of potential violation indicated in the customer financial record may be given the appropriate investigative agency on the same basis as 23-6.10.1.

EFFECTIVE: 03/08/79

23-6.11 Dissemination of Information (Refer to MAOP, Part II, 9-10.)

EFFECTIVE: 03/08/79

23-6.11.1 To Department of Justice

Transfers between and among the components of the Department are not restricted by RFPA except that customer record obtained in an investigation targeted at the financial institution where there is no notice or challenge opportunity may not be used for a separate inquiry. Enough information about the separate inquiry may be given to another component in order that access may be sought independently.

EFFECTIVE: 03/08/79

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 23 - 24

23-6.11.2 To Other Departments

Financial records obtained on or after 3/10/79 under RFPA may be transferred to another agency only if the transferring agency certifies in writing to the file that there is reason to believe the records are relevant to a legitimate law enforcement inquiry of the receiving agency. This may require a statement from the receiving agency. Post notice to the customer within 14 days of the transfer is required unless a delay of notice is obtained as discussed above (23-6.7.2).

EFFECTIVE: 03/08/79

23-6.12 Penalties

EFFECTIVE: 08/28/91

23-6.12.1 Civil

Any Federal agency or financial institution is liable to the customer for violation of RFPA as follows:

- involved,
- (1) \$100.00 without regard to the volume of records
 - (2) actual damage,
 - (3) punitive damages, and
 - (4) court costs and reasonable attorney's fees.

EFFECTIVE: 08/28/91

23-6.12.2 Disciplinary Action

If a court determines that a violation may have been willful or intentional, Office of Personnel Management (formerly Civil Service Commission) must determine if the Government employee is primarily responsible and subject to disciplinary action.

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 23 - 25

EFFECTIVE: 08/28/91

23-6.12.3 Other

Even though RFPA has no criminal sanctions, customer records covered by RFPA would also be covered by the Privacy Act of 1974 which does provide for criminal penalties.

EFFECTIVE: 08/28/91

23-6.13 Cost Reimbursement

(1) Generally, for all customer records obtained by the RFPA access methods, the financial institution must be reimbursed starting 10/1/79 for such records at a rate established by the Governors of the Federal Reserve System.

(2) Reimbursement should be accomplished through the routine commercial vouchering procedures (MAOP, Part II, 6-9). Financial institutions should be encouraged to submit an invoice to the field office covering the cost of obtaining the customer records. The field office draft system should not be routinely used to reimburse financial institutions.

EFFECTIVE: 12/07/93

23-6.14 Reporting Requirements

EFFECTIVE: 08/28/91

23-6.14.1 Dissemination of Information Obtained (See MAOP, Part II, 9-10 and MIOG, Part II, 23-6.11)

EFFECTIVE: 08/28/91

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 23 - 26

23-6.14.2 Statistical Reporting

| Pursuant to the terms of the RFPA within the Federal
Reports Elimination and Sunset Act of 1995, each field division will
no longer be required to compile annual RFPA statistics for submission
to FBIHQ and Congress. |

EFFECTIVE: 06/11/96

23-7 INTERNATIONAL CRIMINAL POLICE ORGANIZATION (INTERPOL)

| See Part I, Section 163-10, of this manual. |

EFFECTIVE: 10/18/88

23-8 TRAVEL - INVESTIGATIVE

EFFECTIVE: 03/23/89

23-8.1 Interdivisional Travel of FBI Personnel on Official
Business

Interdivisional travel of investigative and support
personnel may be authorized by the SAC with the concurrence of the SAC
of the office to be visited. Only the ASAC, in the absence of the
SAC, may approve such travel.

EFFECTIVE: 03/23/89

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 23 - 27

23-8.2 Foreign Travel of FBI Personnel on Official Business
(See MIOG, Part I, 281-6.2; Legal Attache Manual, 4-8.)

(1) The FBI is represented abroad by Legal Attache (Legat) Offices. The services of the Legat should be utilized by FBI Headquarters personnel and domestic field offices requiring investigative assistance abroad as the Legat is qualified to handle the full range of FBI matters overseas. Where a country not covered by a Legat is involved, Interpol or U.S. Department of State (USDS) channels can be used. However, where unique expertise in a complex matter is needed to facilitate interviews and/or investigations by foreign authorities; where travel is necessary for attendance at international symposiums of conferences with police officials; or travel is desired for some other official liaison or related purpose, consideration will be given to requests for participation of FBI Headquarters personnel and field Special Agents on a case-by-case basis. In any event, foreign travel should be coordinated with the Legat Office covering the country concerned and the International Relations Section (IRS), Criminal Investigative Division. The Legat should be kept informed as to contemplated activity to ensure appropriate coordination with foreign agencies. The Legat will also be able to comment as to any other current activity or circumstance in the foreign country which may have some effect on the travel activity.

(2) Due to a wide variety of requirements imposed by other countries on visits of foreign police officials and the fact that each visit is different and presents diversified problems, no attempt is being made to set forth country-by-country guidelines as to exact procedures that should be followed for such travel. However, the following minimal requirements must be met before approval of any contemplated foreign travel will be considered by FBIHQ:

All requests for foreign travel on official business must be in writing and include, where applicable, but not be limited to:

(a) Name of employee(s) traveling. (Include name and title of other U.S. Government persons accompanying.)

(b) Synopsis of case. Include information on investigation or prosecution of any foreign nationals. State if case is in the investigative, indictment, or trial stage.

(c) Purpose and nature of trip to include unique circumstances which make it necessary that employee must personally make the trip as opposed to matter being handled through appropriate liaison channels by Legat, Interpol or USDS.

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 23 - 28

(d) Name of country to be visited, identifying authorities/agencies to be contacted and whether or not they have requested and/or agreed to the visit.

(e) Identity and nationality of persons and/or firms involved as suspects or witnesses, if known. Specifically identify foreign nationals being interviewed or deposed.

(f) Proposed itinerary (Include mode of travel, accommodation arrangements or requirements, etc.).

(g) Estimated cost of transportation, per diem, and other expenses.

(h) Request for authority to travel for the purpose of interviews or undercover operations outside the United States must be supported by full justification and must include the personal recommendation of the SAC.

(i) Provide the identity of any foreign embassy consular or diplomatic officials who have been consulted regarding travel. Specify if assistance of American embassy/consulate or other personnel is required (e.g., consular officer to administer oath) or if office space at post is required. Also state if assistance of a stenographer, court reporter or interpreter is required.

(j) Other factors

All of the above questions must be answered as fully as possible if foreign travel is for the purpose of obtaining evidence suitable for U.S. Court presentations, e.g., interview under oath or obtaining physical evidence such as bank documents. In all foreign countries, certain certifications to the U.S. Government are necessary regarding evidence and a responsible U.S. Embassy Consular Officer must further certify the material for U.S. Courts. Arranging for U.S. Court certifications requires at least two weeks' notice and travel relating to same must be scheduled with the appropriate Embassy, usually by the prosecuting U.S. Attorney.

In addition to answering the above questions, advise FBIHQ if foreign travel is being performed while carrying official or classified documents or equipment since a NonPROCOURIER letter is required for same. The IRS will aid in arranging for the courier letter and for the diplomatic pouching and sealing of the material being transported.

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 23 - 29

(3) Special Agents may not carry firearms or participate in arrests abroad. FBI credentials may be carried while on official travel abroad; however, use and/or display of credentials in a foreign country is inappropriate.

(a) FBI Agents have no jurisdiction in foreign countries. The reason for this is that no U.S. laws can override a foreign country's right to protect the integrity of its sovereignty. However, FBI Agents have investigative responsibilities overseas under several Federal statutes which provide for extraterritorial application. Though not limited to terrorist activity, generally such investigations have been conducted in terrorist's attacks. In cases where the FBI has been authorized to investigate abroad under these statutes, FBI Agents may conduct those investigative activities which have been coordinated and approved by FBIHQ. FBIHQ will conduct appropriate coordination with the Department of State to obtain host country approval to allow the FBI Agents to conduct the necessary investigative activity abroad. (See MIOG, Part II, 11-2.3.3(2), 23-4.2; Legal Handbook for Special Agents, 3-11.)

(b) Legats, border office Agents, and other FBI Special Agents or employees, even though invited or requested by foreign authorities to participate in and/or observe arrests and searches of subjects or transportation of prisoners, may not do so.

(4) Official passports and visas are required for all FBI personnel traveling abroad on official business and are issued only by the USDS Passport Office in Washington, D.C., upon receipt of a request signed by the Director, FBI. A tourist passport is not appropriate for official travel but is permitted if safety of the traveler is a concern. (See Legal Attache Manual, 4-8.)

(a) U.S. Passport law is contained in the Code of Federal Regulations, Title 22, Chapter 1, Part 51. The IRS, CID, maintains contact with the USDS Passport Office for the purpose of obtaining official passports for FBI personnel. Proof of U.S. citizenship, two 2 x 2-inch photos, an acceptable certified birth certificate, or certificate of naturalization and a signed passport application are necessary to obtain a passport. When applying for the initial passport, the applicant must appear in person before a passport official empowered to certify the applicant's identity. The applicant must sign the passport application in this official's presence. Subsequent passports can be obtained by providing a previous passport with the application and personal appearance is not required. The prospective traveler should contact IRS, CID, for an official passport after receiving authority to travel. The subject,

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 23 - 30

date of the Bureau communication authorizing travel, the Bureau file number and dates of travel should be provided. A passport application should be obtained locally, completed, appropriately certified and forwarded with all necessary information to the IRS, CID, as expeditiously as circumstances warrant. The official passport will be obtained along with any visas needed and the passport will be returned to the requesting official. Official passports will be valid for five years. Utilization of normal liaison channels requires approximately two weeks for the issuance and return of an official passport, plus three days for each visa.

(b) Official passports issued to FBI personnel in the field should be returned to the SAC for retention at the conclusion of the official foreign travel. The passport should be returned to IRS, CID, FBIHQ, on expiration, separation from official status with the FBI, or when no longer needed. It will then be returned to the USDS Passport Office. An official passport is not to be used for personal or pleasure travel, and any loss should be reported at once.

(c) A visa is a permit, entered on the passport of a national of one country, by the consular of another. This permit allows the bearer entry to, or transit through, the country issuing the permit. The time for which visas are issued usually depends on the length of the trip. Applications, pictures, International Health Cards, and other certified documents may be required before visas are issued. Official travel to most countries requires a visa. The visa is stamped in the U.S. passport used for travel. Visas are obtained from that country's Embassy or Consulate in the U.S. Foreign diplomatic establishments require a USDS, Washington, D.C., Passport Office letter before they will issue a visa for official travel.

On request, the IRS, CID, will also obtain visas necessary for official travel. In addition to time needed to obtain a passport, should a visa(s) be necessary, an additional three days will be needed to obtain each one.

(5) U.S. government travel regulations dictate that a government employee traveling on official business must use a U.S. carrier, whenever available. GSA travel regulations also require use of contract air carriers, if available. GSA has awarded international city-pair contracts for foreign travel by federal civilian employees. The use of the contract carriers between the designated city-pairs is mandatory. (See MAOP, Part II, 6-1.1.2, re city-pairs.)

Before leaving the U.S., foreign travelers, even on

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 23 - 31

official business, may wish to check on U.S. Customs regulations. Customs regulations require filing a declaration of personal property in excess of certain monetary amounts. Reentry processing is eased if a Customs declaration is submitted before leaving the U.S.

(6) Since official passports and visas provide no immunity for the bearer, he/she (the bearer) can be held fully liable for all actions while abroad. This liability is both civil and criminal under the laws of the host country, which are often different to those in the United States.

(7) All of the foregoing instructions do not necessarily apply to investigations in Canada and Mexico. However, with exception of established liaison visits by border offices, no Special Agent or person under FBI operational direction and control is to travel to Canada or Mexico without prior coordination with Legat, Ottawa, or Legat, Mexico City, through FBIHQ. Furthermore, if a border office contemplates the utilization of the undercover technique, wherein a Special Agent or person under FBI operational direction or control may be required to enter into Canada or Mexico, authority from FBIHQ must first be obtained. Requests for such authority must be in writing, must be supported by full justification, and must include the personal recommendation of the SAC. In an emergency, FBIHQ authority may be requested telephonically, but such a request must be followed by teletype that sets forth the required information without delay.

(8) In compliance with Title 22, USC, Section 3927, and an agreement between the Attorney General and Secretary of State, Legal Attaches must keep Chiefs of Mission (usually the U.S. Ambassador in a country) fully and currently informed about all FBI programs and activities carried out in their countries of accreditation. If a Chief of Mission believes an FBI activity might impair relations with the country to which Chief is accredited, the Chief is authorized to suspend such activity pending further resolution. Therefore, when activity abroad by personnel of FBIHQ or domestic offices is proposed, full facts must be furnished because, as a law enforcement agency, FBI activity overseas may have unforeseen ramifications. It will be necessary to inform and obtain the concurrence of the host country government at an appropriate policy level regarding the proposed FBI activity. In cases where it is proposed to visit a country not covered by a Legat, arrangements should be made through the USDS. In either case, the FBIHQ substantive desk supervisor, with the assistance of IRS, CID, personnel, will initiate needed action. Action by FBIHQ substantive desk supervisors entails obtaining FBIHQ approval for foreign travel; preparing a written no-foreign-policy-objection notification to USDS

~~CONFIDENTIAL~~

Sensitive

Administrative 6-2-98

CLASSIFIED BY: SP5E/ham
REASON: 1.5 (C)
DECLASSIFY ON: X1

Manual of Investigative Operations and Guidelines
Part II

PAGE 23 - 32

headquarters; notifying the appropriate DOJ officials and/or obtaining DOJ decision on FBI extraterritorial investigative jurisdiction; and ensuring that an FBI Legal Attache or USDSHQ has obtained the concurrence of the appropriate U.S. Chief of Mission in the country to be visited. Therefore, as much advance notice as possible should be given. In the case of routine meetings with established foreign liaison contacts or conferences with other U.S. agencies abroad, notification of the host country government will not normally be required. The notification decision, however, is the prerogative of the U.S. Chief of Mission abroad. (See MIOG, Part I, 163-6; Part II, 21-19.5(2)(c).7.)

(9) FBI Special Agents from domestic offices may not independently conduct investigations in foreign countries and may not conduct independent interviews without concurrence of host government. There may be an exception to this such as in the case of an American citizen voluntarily appearing for interview on premises of U.S. Embassy or U.S. Consulate. However, the interview of an American citizen off U.S. diplomatically protected premises or interview of a foreign national on or off U.S. diplomatically protected premises may be participated in by a Special Agent only with permission and/or invitation of appropriate authorities of host country. Such off-premises interviews would normally be conducted by the host government authorities. (See MIOG, Part I, 163-6; II, 23-4.4.)

(10) The Government of the United Kingdom has promulgated guidelines entitled "Guidelines for Law Enforcement Agents Representing Foreign Governments." (See MIOG, Part I, 163-6.)

These guidelines, issued to all Missions in London on May 30, 1986, read as follows:

(a) "Officials representing foreign governments, when conducting investigations in the United Kingdom relating to the possible contravention of their laws, should make inquiries in the United Kingdom only with the prior permission of the United Kingdom Government or agency representing the Government. Such permission may be withheld or given conditionally."

(b) "Reasonable notice should be given of any visit of the matters under investigation, and the future of the inquiries which are intended to be conducted in the United Kingdom."

(c) "The United Kingdom Government or agency representing the Government maintain the right to have an official present at any interview. Interviews may only be conducted with the

ALL INFORMATION CONTAINED
HERE IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

~~CONFIDENTIAL~~

Sensitive

PRINTED: 02/18/98

~~CONFIDENTIAL~~

Sensitive


Manual of Investigative Operations and Guidelines
Part II

PAGE 23 - 33

consent of the person to be interviewed, or with the support of judicial authority within the United Kingdom which may permit examination of a person in response to an order of a Court."

(d) "Officials representing foreign governments must advise the United Kingdom Government or agency representing the Government of the developments in the enquiry conducted within the United Kingdom in the form requested by the Government or agency."

FBI Agents conducting investigations in the United Kingdom should abide by these guidelines. Notify the Deputy Director promptly if a request or demand is issued by United Kingdom authorities to disclose the contents or results of interviews of United States persons with their consent in Great Britain by FBI Agents in those instances in which no information is developed about an offense within the United Kingdom, or to disclose any details of an investigation by the FBI, other than the results of an interview of non-United States persons.

(C)  b1
(C)

EFFECTIVE: 02/14/97

~~CONFIDENTIAL~~

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 23 - 34

23-9 CLASSIFIED INFORMATION PROCEDURES ACT (CIPA) (SEE MIOG,
PART I, 259-2.)

The CIPA of 1980 (Public Law 96-456, 94 Stat. 2025), Title 18, United States Code, app. III, established certain pretrial, trial and appellate procedures for criminal cases in which there is a possibility that classified information will be disclosed. The Act required that the Chief Justice of the United States issue instructions establishing procedures for the protection against unauthorized disclosure of any classified information in the custody of the United States District Courts, Courts of Appeal, or Supreme Court.

EFFECTIVE: 04/12/94

23-9.1 Notification to United States Attorney

(1) Prior to any factual discussion of such a case, ensure that the United States Attorney (USA) possesses the clearances necessary for access to classified material, noting that USAs do not necessarily have security clearances. To verify a USA's clearance, contact the Security Programs Manager (SPM), FBIHQ. USAs requiring a clearance should refer to the United States Attorney's Manual for guidance.

(2) Upon the initial presentation for a prosecutive opinion to the USA, the USA should be advised that the case will or may involve the disclosure of classified information.

(3) The USA should also be advised that should it become necessary to clear persons for access to classified information, the clearance granting procedure will consume approximately 90 days. If exigencies of the situation dictate priority handling of the processing, the clearance may be granted more expeditiously, but as much advance notice as possible should be provided.

EFFECTIVE: 03/23/89

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 23 - 35

23-9.2 Notification to FBIHQ

Upon making the determination that the litigation of a case will or may involve the disclosure of classified information, promptly notify the FBIHQ component responsible for supervision of the substantive violation and the Office of the General Counsel (OGC). Include in the notification a brief synopsis of the case, the identity of the USA to whom the case was presented and the date it was presented.

EFFECTIVE: 09/09/94

23-9.3 Court Security Officer

The procedures issued in accordance with the Act by the Chief Justice of the United States require the appointment of a Court Security Officer in any proceedings in which classified information is involved, or is reasonably expected to be involved.

(1) The field office Security Officer or Alternate Security Officer will be the FBI nominee to serve as Court Security Officer. The designation of the Court Security Officer is left to the discretion of the judge presiding at the trial.

(2) If a Special Agent (SA) is appointed to serve as Court Security Officer, insofar as the SA's duties pertaining to the trial are concerned, the SA is considered an officer of the Court and is, therefore, guided by the Court.

(3) Once an SA is selected, he/she is to promptly contact the Department of Justice (DOJ) Security Officer and the FBI SPM for guidance as to the responsibilities attendant to the appointment.

(4) If any conflict develops between the Court Security Officer duties and FBI regulations governing an SA's other responsibilities, the SAC, OGC and the SPM at FBIHQ are to be immediately notified.

EFFECTIVE: 09/09/94

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 23 - 36

23-9.4 Duties of Court Security Officer

The Court Security Officer is responsible to the Court for document, physical, personnel and communications security and is to take measures reasonably necessary to fulfill these responsibilities as set forth in the "Security Procedures Established Pursuant to Public Law 96-456, 94 Stat. 2025, by the Chief Justice of the United States for the Protection of Classified Information."

EFFECTIVE: 12/10/91

23-9.5 Procedures for Obtaining Security Clearances

Excluding the presiding judge and jury no person appointed by the Court or designated for service at the trial shall be given access to any classified information in the custody of the Court unless such person has been granted a security clearance up to the level of the material to which they will have access.

(1) The Court Security Officer shall obtain from the Court the identities of the person(s) requiring security clearances and promptly notify the DOJ Security Officer, who will initiate the clearance granting procedures. Upon confirmation of the clearances, the DOJ Security Officer will notify the Court in writing as to the identities of the cleared personnel.

(2) The DOJ Security Officer will advise the Security Programs Office, FBIHQ, of the identity(s) of the person(s) requiring a background investigation, which shall be conducted in accordance with Part I, Section 259; and Part II, Section 17, of this manual; and/or the FCI Manual, Part II, 1-10; or MIOG, Part II, 26-10, as applicable.

(3) The FBI will conduct the background investigations in all CIPA cases and report the investigative results to the DOJ Security Officer.

EFFECTIVE: 12/10/91

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 24 - 1

SECTION 24. TERRITORIAL ALLOCATION LIST

24-1 PURPOSE

This list is maintained as a reference that shows the geographic area assigned to each field office, including Legal Attaches. Each office's specific territory is listed for the purpose of setting out investigative leads and for liaison coverage.

EFFECTIVE: 01/31/78

24-2 THE STATES

EFFECTIVE: 01/31/78

24-2.1 ALABAMA

Resident agency(s) listed has direct mail service.

COUNTY	COVERED BY OFFICE (RA)
Autauga	Mobile (Montgomery)
Baldwin	Mobile
Barbour	Mobile
Bibb	Birmingham
Blount	Birmingham
Bullock	Mobile (Montgomery)
Butler	Mobile (Montgomery)
Calhoun	Birmingham
Chambers	Mobile
Cherokee	Birmingham
Chilton	Mobile (Montgomery)
Choctaw	Mobile
Clarke	Mobile
Clay	Birmingham
Cleburne	Birmingham
Coffee	Mobile
Colbert	Birmingham

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 24 - 2

Conecuh	Mobile
Coosa	Mobile (Montgomery)
Covington	Mobile
Crenshaw	Mobile (Montgomery)
Cullman	Birmingham
Dale	Mobile
Dallas	Mobile (Montgomery)
De Kalb	Birmingham
Elmore	Mobile (Montgomery)
Escambia	Mobile
Etowah	Birmingham
Fayette	Birmingham
Franklin	Birmingham
Geneva	Mobile
Greene	Birmingham
Hale	Mobile (Montgomery)
Henry	Mobile
Houston	Mobile
Jackson	Birmingham
Jefferson	Birmingham
Lamar	Birmingham
Lauderdale	Birmingham
Lawrence	Birmingham
Lee	Mobile
Limestone	Birmingham
Lowndes	Mobile (Montgomery)
Macon	Mobile
Madison	Birmingham
Marengo	Mobile
Marion	Birmingham
Marshall	Birmingham
Mobile	Mobile
Monroe	Mobile
Montgomery	Mobile (Montgomery)
Morgan	Birmingham
Perry	Mobile (Montgomery)
Pickens	Birmingham
Pike	Mobile (Montgomery)
Randolph	Mobile
Russell	Mobile
St. Clair	Birmingham
Shelby	Birmingham
Sumter	Birmingham
Talladega	Birmingham
Tallapoosa	Mobile
Tuscaloosa	Birmingham

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 24 - 3

Walker	Birmingham
Washington	Mobile
Wilcox	Mobile
Winston	Birmingham

EFFECTIVE: 07/03/97

24-2.2 ALASKA

All counties covered by the office at Anchorage.

EFFECTIVE: 09/08/78

24-2.3 ARIZONA

All counties covered by the office at Phoenix except that part of the Navajo Indian Reservation lying within Apache County is covered by Albuquerque.

EFFECTIVE: 09/08/78

24-2.4 ARKANSAS

All counties are covered by the office at Little Rock.
Resident agency(s) listed has direct mail service.

COUNTY	COVERED BY OFFICE (RA)
Arkansas	Little Rock
Ashley	Little Rock (Fort Smith)
Baxter	Little Rock (Fort Smith)
Benton	Little Rock (Fort Smith)
Boone	Little Rock (Fort Smith)
Bradley	Little Rock (Fort Smith)
Calhoun	Little Rock (Fort Smith)

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 24 - 4

Carroll	Little Rock (Fort Smith)
Chicot	Little Rock
Clark	Little Rock (Fort Smith)
Clay	Little Rock
Cleburne	Little Rock
Cleveland	Little Rock
Columbia	Little Rock (Fort Smith)
Conway	Little Rock
Craighead	Little Rock
Crawford	Little Rock (Fort Smith)
Crittenden	Little Rock
Cross	Little Rock
Dallas	Little Rock
Desha	Little Rock
Drew	Little Rock
Faulkner	Little Rock
Franklin	Little Rock (Fort Smith)
Fulton	Little Rock
Garland	Little Rock (Fort Smith)
Grant	Little Rock
Greene	Little Rock
Hempstead	Little Rock (Fort Smith)
Hot Springs	Little Rock (Fort Smith)
Howard	Little Rock (Fort Smith)
Independence	Little Rock
Izard	Little Rock
Jackson	Little Rock
Jefferson	Little Rock
Johnson	Little Rock (Fort Smith)
Lafayette	Little Rock (Fort Smith)
Lawrence	Little Rock
Lee	Little Rock
Lincoln	Little Rock
Little River	Little Rock (Fort Smith)
Logan	Little Rock (Fort Smith)
Lonoke	Little Rock
Madison	Little Rock (Fort Smith)
Marion	Little Rock (Fort Smith)
Miller	Little Rock (Fort Smith)
Mississippi	Little Rock
Monroe	Little Rock
Montgomery	Little Rock (Fort Smith)
Nevada	Little Rock (Fort Smith)
Newton	Little Rock (Fort Smith)
Ouachita	Little Rock (Fort Smith)
Perry	Little Rock

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 24 - 5

Phillips	Little Rock
Pike	Little Rock (Fort Smith)
Poinsett	Little Rock
Polk	Little Rock (Fort Smith)
Pope	Little Rock
Prairie	Little Rock
Pulaski	Little Rock
Randolph	Little Rock
Saline	Little Rock
Scott	Little Rock (Fort Smith)
Searcy	Little Rock (Fort Smith)
Sebastian	Little Rock (Fort Smith)
Sevier	Little Rock (Fort Smith)
Sharp	Little Rock
St. Francis	Little Rock
Stone	Little Rock
Union	Little Rock (Fort Smith)
Van Buren	Little Rock
Washington	Little Rock (Fort Smith)
White	Little Rock
Woodruff	Little Rock
Yell	Little Rock

EFFECTIVE: 02/10/97

24-2.5 CALIFORNIA

| Resident agencies listed have direct mail service. |

COUNTY	COVERED BY OFFICE (RA)
Alameda	San Francisco (Oakland)
Alpine	Sacramento
Amador	Sacramento
Butte	Sacramento
Calaveras	Sacramento
Camp Roberts	Los Angeles
Colusa	Sacramento
Contra Costa	San Francisco
Del Norte	San Francisco
Edwards Air Force Base	Los Angeles

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 24 - 6

El Dorado	Sacramento
Fresno	Sacramento (Fresno)
Glenn	Sacramento
Humboldt	San Francisco
Imperial	San Diego
Inyo	Sacramento (Fresno)
Kern	Sacramento (Fresno)
(Except Edwards Air Force Base which is covered by Los Angeles)	
Kings	Sacramento (Fresno)
Lake	San Francisco
Lassen	Sacramento
Los Angeles	Los Angeles
Madera	Sacramento (Fresno)
Marin	San Francisco
Mariposa	Sacramento (Fresno)
Mendocino	San Francisco
Merced	Sacramento (Fresno)
Modoc	Sacramento
Mono	Sacramento
Monterey	San Francisco (San Jose)
(Except Camp Roberts which is covered by Los Angeles)	
Napa	San Francisco
Nevada	Sacramento
Orange	Los Angeles (Santa Ana)
Placer	Sacramento
Plumas	Sacramento
Riverside	Los Angeles (Riverside)
Sacramento	Sacramento
San Benito	San Francisco (San Jose)
San Bernardino	Los Angeles (Riverside)
San Diego	San Diego
San Francisco	San Francisco
San Joaquin	Sacramento
San Luis Obispo	Los Angeles
San Mateo	San Francisco
Santa Barbara	Los Angeles
Santa Clara	San Francisco (San Jose)
Santa Cruz	San Francisco (San Jose)
Shasta	Sacramento
Sierra	Sacramento
Siskiyou	Sacramento
Solano	Sacramento

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 24 - 7

Sonoma	San Francisco
Stanislaus	Sacramento
Sutter	Sacramento
Tehama	Sacramento
Trinity	Sacramento
Tulare	Sacramento (Fresno)
Tuolumne	Sacramento
Ventura	Los Angeles
Yolo	Sacramento
Yosemite	Sacramento
National Park	
Yuba	Sacramento

EFFECTIVE: 11/03/95

24-2.6 COLORADO

All counties covered by the office at Denver.

EFFECTIVE: 01/31/78

24-2.7 CONNECTICUT

All counties covered by the office at New Haven.

EFFECTIVE: 01/31/78

24-2.8 DELAWARE

All counties covered by the office at Baltimore.

EFFECTIVE: 01/31/78

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 24 - 8

24-2.9 DISTRICT OF COLUMBIA

Covered by the Field Office at Washington

EFFECTIVE: 01/31/78

24-2.10 FLORIDA

| Resident agencies listed have direct mail service. |

COUNTY	COVERED BY OFFICE (RA)
Alachua	Jacksonville
Baker	Jacksonville
Bay	Jacksonville (Pensacola)
Bradford	Jacksonville
Brevard	Tampa
Broward	Miami
Calhoun	Jacksonville (Pensacola)
Charlotte	Tampa
Citrus	Jacksonville
Clay	Jacksonville
Collier	Tampa
Columbia	Jacksonville
Dade	Miami
De Soto	Tampa
Dixie	Jacksonville
Duval	Jacksonville
Escambia	Jacksonville (Pensacola)
Flagler	Jacksonville
Franklin	Jacksonville (Tallahassee)
Gadsden	Jacksonville (Tallahassee)
Gilchrist	Jacksonville
Glades	Tampa
Gulf	Jacksonville (Pensacola)
Hamilton	Jacksonville
Hardee	Tampa
Hendry	Tampa
Hernando	Tampa
*Highlands	Miami
Hillsborough	Tampa
Holmes	Jacksonville (Pensacola)

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 24 - 9

Indian River	Miami
Jackson	Jacksonville (Pensacola)
Jefferson	Jacksonville (Tallahassee)
Lafayette	Jacksonville (Tallahassee)
Lake	Jacksonville
Lee	Tampa
Leon	Jacksonville (Tallahassee)
Levy	Jacksonville
Liberty	Jacksonville (Tallahassee)
Madison	Jacksonville (Tallahassee)
Manatee	Tampa
Marion	Jacksonville
Martin	Miami
Monroe	Miami
Nassau	Jacksonville
Okaloosa	Jacksonville (Pensacola)
Okeechobee	Miami
Orange	Tampa
Osceola	Tampa
Palm Beach	Miami
Pasco	Tampa
Pinellas	Tampa
*Polk	Tampa
Putnam	Jacksonville
St. Johns	Jacksonville
St. Lucie	Miami
Santa Rosa	Jacksonville (Pensacola)
Sarasota	Tampa
Seminole	Tampa
Sumter	Jacksonville
Suwannee	Jacksonville
Taylor	Jacksonville (Tallahassee)
Union	Jacksonville
Volusia	Jacksonville
Wakulla	Jacksonville (Tallahassee)
Walton	Jacksonville (Pensacola)
Washington	Jacksonville (Pensacola)

*Note: Leads for the Florida State Correctional Institution, also known as the Avon Park Correctional Institution, which has a mailing address of Avon Park, Florida, and the Avon Park Bombing and Gunnery Range are covered by the Tampa Division.

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 24 - 10

EFFECTIVE: 11/03/95

24-2.11 GEORGIA

All counties covered by office at Atlanta. Resident agencies listed have direct mail service.

COUNTY	COVERED BY OFFICE (RA)
Appling	Atlanta (Augusta)
Atkinson	Atlanta (Savannah)
Bacon	Atlanta (Savannah)
Baker	Atlanta (Macon)
Baldwin	Atlanta (Macon)
Banks	Atlanta (Rossville)
Barrow	Atlanta (Rossville)
Bartow	Atlanta (Rossville)
Ben Hill	Atlanta (Macon)
Berrien	Atlanta (Macon)
Bibb	Atlanta (Macon)
Bleckley	Atlanta (Macon)
Brantley	Atlanta (Savannah)
Brooks	Atlanta (Macon)
Bryan	Atlanta (Savannah)
Bulloch	Atlanta (Augusta)
Burke	Atlanta (Augusta)
Butts	Atlanta (Macon)
Calhoun	Atlanta (Macon)
Camden	Atlanta (Savannah)
Candler	Atlanta (Augusta)
Catoosa	Atlanta (Rossville)
Charlton	Atlanta (Savannah)
Chatham	Atlanta (Savannah)
Chattahoochee	Atlanta (Macon)
Cherokee	Atlanta (Rossville)
Clarke	Atlanta (Macon)
Clay	Atlanta (Macon)
Clinch	Atlanta (Macon)
Coffee	Atlanta (Augusta)
Colquitt	Atlanta (Macon)
Columbus	Atlanta (Augusta)
Cook	Atlanta (Macon)

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 24 - 11

Crawford	Atlanta (Macon)
Crisp	Atlanta (Macon)
Dade	Atlanta (Rossville)
Dawson	Atlanta (Rossville)
Decatur	Atlanta (Macon)
Dodge	Atlanta (Augusta)
Dooly	Atlanta (Macon)
Dougherty	Atlanta (Macon)
Early	Atlanta (Macon)
Echols	Atlanta (Macon)
Effingham	Atlanta (Savannah)
Elbert	Atlanta (Macon)
Emanuel	Atlanta (Augusta)
Evans	Atlanta (Augusta)
Fannin	Atlanta (Rossville)
Floyd	Atlanta (Rossville)
Forsyth	Atlanta (Rossville)
Franklin	Atlanta (Macon)
Gilmer	Atlanta (Rossville)
Glascok	Atlanta (Augusta)
Glynn	Atlanta (Savannah)
Gordon	Atlanta (Rossville)
Grady	Atlanta (Macon)
Greene	Atlanta (Macon)
Habersham	Atlanta (Rossville)
Hall	Atlanta (Rossville)
Hancock	Atlanta (Macon)
Haralson	Atlanta (Rossville)
Harris	Atlanta (Macon)
Hart	Atlanta (Macon)
Houston	Atlanta (Macon)
Irwin	Atlanta (Macon)
Jackson	Atlanta (Rossville)
Jasper	Atlanta (Macon)
Jeff Davis	Atlanta (Augusta)
Jefferson	Atlanta (Augusta)
Jenkins	Atlanta (Augusta)
Johnson	Atlanta (Augusta)
Jones	Atlanta (Macon)
Lamar	Atlanta (Macon)
Lanier	Atlanta (Macon)
Laurens	Atlanta (Augusta)
Lee	Atlanta (Macon)
Liberty	Atlanta (Savannah)
Lincoln	Atlanta (Augusta)
Long	Atlanta (Savannah)

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 24 - 12

Lowndes	Atlanta (Macon)
Lumpkin	Atlanta (Rossville)
Macon	Atlanta (Macon)
Madison	Atlanta (Macon)
Marion	Atlanta (Macon)
McDuffie	Atlanta (Augusta)
McIntosh	Atlanta (Savannah)
Miller	Atlanta (Macon)
Mitchell	Atlanta (Macon)
Monroe	Atlanta (Macon)
Montgomery	Atlanta (Augusta)
Morgan	Atlanta (Macon)
Murray	Atlanta (Rossville)
Muscogee	Atlanta (Macon)
Oconee	Atlanta (Macon)
Oglethorpe	Atlanta (Macon)
Paulding	Atlanta (Rossville)
Peach	Atlanta (Macon)
Pickens	Atlanta (Rossville)
Pierce	Atlanta (Savannah)
Polk	Atlanta (Rossville)
Pulaski	Atlanta (Macon)
Putnam	Atlanta (Macon)
Quitman	Atlanta (Macon)
Rabun	Atlanta (Rossville)
Randolph	Atlanta (Macon)
Richmond	Atlanta (Augusta)
Schley	Atlanta (Macon)
Screven	Atlanta (Augusta)
Seminole	Atlanta (Macon)
Stephens	Atlanta (Rossville)
Stewart	Atlanta (Macon)
Sumter	Atlanta (Macon)
Talbot	Atlanta (Macon)
Taliaferro	Atlanta (Augusta)
Tallnall	Atlanta (Augusta)
Taylor	Atlanta (Macon)
Telfair	Atlanta (Augusta)
Terrell	Atlanta (Macon)
Thomas	Atlanta (Macon)
Tift	Atlanta (Macon)
Toombs	Atlanta (Augusta)
Towns	Atlanta (Rossville)
Truetlen	Atlanta (Augusta)
Turner	Atlanta (Macon)
Twiggs	Atlanta (Macon)

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 24 - 13

Union	Atlanta (Rossville)
Upson	Atlanta (Macon)
Walker	Atlanta (Rossville)
Walton	Atlanta (Macon)
Ware	Atlanta (Savannah)
Warren	Atlanta (Augusta)
Washington	Atlanta (Macon)
Wayne	Atlanta (Savannah)
Webster	Atlanta (Macon)
White	Atlanta (Rossville)
Whitfield	Atlanta (Rossville)
Wilcox	Atlanta (Macon)
Wilkes	Atlanta (Augusta)
Wilkinson	Atlanta (Macon)
Worth	Atlanta (Macon)

EFFECTIVE: 11/03/95

24-2.12 HAWAII

Covered by the office at Honolulu.

EFFECTIVE: 08/27/90

24-2.13 IDAHO

All counties covered by the office at Salt Lake City.
Resident agency(s) listed has direct mail service.

COUNTY	COVERED BY OFFICE (RA)
Ada	Salt Lake City (Boise)
Adams	Salt Lake City (Boise)
Bannock	Salt Lake City (Boise)
Bear Lake	Salt Lake City (Boise)
Benewah	Salt Lake City (Boise)
Bingham	Salt Lake City (Boise)
Blaine	Salt Lake City (Boise)
Boise	Salt Lake City (Boise)

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 24 - 14

Bonner	Salt Lake City (Boise)
Bonneville	Salt Lake City (Boise)
Boundary	Salt Lake City (Boise)
Butte	Salt Lake City (Boise)
Camas	Salt Lake City (Boise)
Canyon	Salt Lake City (Boise)
Caribou	Salt Lake City (Boise)
Cassia	Salt Lake City (Boise)
Clark	Salt Lake City (Boise)
Clearwater	Salt Lake City (Boise)
Custer	Salt Lake City (Boise)
Elmore	Salt Lake City (Boise)
Franklin	Salt Lake City (Boise)
Fremont	Salt Lake City (Boise)
Gem	Salt Lake City (Boise)
Gooding	Salt Lake City (Boise)
Idaho	Salt Lake City (Boise)
Jefferson	Salt Lake City (Boise)
Jerome	Salt Lake City (Boise)
Kootenai	Salt Lake City (Boise)
Latah	Salt Lake City (Boise)
Lemhi	Salt Lake City (Boise)
Lewis	Salt Lake City (Boise)
Lincoln	Salt Lake City (Boise)
Madison	Salt Lake City (Boise)
Minidoka	Salt Lake City (Boise)
Nez Perce	Salt Lake City (Boise)
Oneida	Salt Lake City (Boise)
Owyhee	Salt Lake City (Boise)
Payette	Salt Lake City (Boise)
Power	Salt Lake City (Boise)
Shoshone	Salt Lake City (Boise)
Summit	Salt Lake City (Boise)
Teton	Salt Lake City (Boise)
Twin Falls	Salt Lake City (Boise)
Valley	Salt Lake City (Boise)
Washington	Salt Lake City (Boise)

EFFECTIVE: 11/03/95

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 24 - 15

24-2.14 ILLINOIS

Resident agencies listed have direct mail service.

COUNTY	COVERED BY OFFICE (RA)
Adams	Springfield
Alexander	Springfield
Bond	Springfield
Boone	Chicago (Rockford)
Brown	Springfield
Bureau	Springfield
Calhoun	Springfield
Carroll	Chicago (Rockford)
Cass	Springfield
Champaign	Springfield
Christian	Springfield
Clark	Springfield
Clay	Springfield
Clinton	Springfield
Coles	Springfield
Cook	Chicago (North, South & West)
Crawford	Springfield
Cumberland	Springfield
De Kalb	Chicago (Rockford)
De Witt	Springfield
Douglas	Springfield
Du Page	Chicago (North & West)
Edgar	Springfield
Edwards	Springfield
Effingham	Springfield
Fayette	Springfield
Ford	Springfield
Franklin	Springfield
Fulton	Springfield
Gallatin	Springfield
Greene	Springfield
Grundy	Chicago (South)
Hamilton	Springfield
Hancock	Springfield
Hardin	Springfield
Henderson	Springfield
Henry	Springfield
Iroquois	Springfield
Jackson	Springfield

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 24 - 16

Jasper	Springfield
Jefferson	Springfield
Jersey	Springfield
Jo Daviess	Chicago (Rockford)
Johnson	Springfield
Kane	Chicago (West)
Kankakee	Springfield
Kendall	Chicago (West)
Knox	Springfield
Lake	Chicago (North)
La Salle	Chicago (South)
Lawrence	Springfield
Lee	Chicago (Rockford)
Livingston	Springfield
Logan	Springfield
Macon	Springfield
Macoupin	Springfield
Madison	Springfield
Marion	Springfield
Marshall	Springfield
Mason	Springfield
Massac	Springfield
McDonough	Springfield
McHenry	Chicago (Rockford)
McLean	Springfield
Menard	Springfield
Mercer	Springfield
Monroe	Springfield
Montgomery	Springfield
Morgan	Springfield
Moultrie	Springfield
Ogle	Chicago (Rockford)
Peoria	Springfield
Perry	Springfield
Piatt	Springfield
Pike	Springfield
Pope	Springfield
Pulaski	Springfield
Putnam	Springfield
Randolph	Springfield
Richland	Springfield
Rock Island	Springfield
St. Clair	Springfield
Saline	Springfield
Sangamon	Springfield
Schuyler	Springfield

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 24 - 17

Scott	Springfield
Shelby	Springfield
Stark	Springfield
Stephenson	Chicago (Rockford)
Tazewell	Springfield
Union	Springfield
Vermilion	Springfield
Wabash	Springfield
Warren	Springfield
Washington	Springfield
Wayne	Springfield
White	Springfield
Whiteside	Chicago (Rockford)
Will	Chicago (South)
Williamson	Springfield
Winnebago	Chicago (Rockford)
Woodford	Springfield

EFFECTIVE: 03/14/97

24-2.15 INDIANA

All counties covered by the office at Indianapolis.
Resident agency(s) listed has direct mail service.

COUNTY	COVERED BY OFFICE (RA)
Elkhart	Indianapolis (Merrillville)
Fulton	Indianapolis (Merrillville)
Jasper	Indianapolis (Merrillville)
Kosciusko	Indianapolis (Merrillville)
Lake	Indianapolis (Merrillville)
LaPorte	Indianapolis (Merrillville)
Marshall	Indianapolis (Merrillville)
Newton	Indianapolis (Merrillville)
Porter	Indianapolis (Merrillville)
Pulaski	Indianapolis (Merrillville)
St. Joseph	Indianapolis (Merrillville)
Starke	Indianapolis (Merrillville)

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 24 - 18

EFFECTIVE: 11/03/95

24-2.16 IOWA

All counties covered by the office at Omaha.

EFFECTIVE: 01/31/78

24-2.17 KANSAS

All counties covered by the office at Kansas City.
Resident agency(s) listed has direct mail service.

COUNTY	COVERED BY OFFICE (RA)
Allen	Kansas City (Wichita)
Barber	Kansas City (Wichita)
Barton	Kansas City (Wichita)
Butler	Kansas City (Wichita)
Chase	Kansas City (Wichita)
Chautauqua	Kansas City (Wichita)
Comanche	Kansas City (Wichita)
Cowley	Kansas City (Wichita)
Edwards	Kansas City (Wichita)
Elk	Kansas City (Wichita)
Greenwood	Kansas City (Wichita)
Harper	Kansas City (Wichita)
Harvey	Kansas City (Wichita)
Kingman	Kansas City (Wichita)
Kiowa	Kansas City (Wichita)
Marion	Kansas City (Wichita)
McPherson	Kansas City (Wichita)
Montgomery	Kansas City (Wichita)
Neosho	Kansas City (Wichita)
Pawnee	Kansas City (Wichita)
Pratt	Kansas City (Wichita)
Reno	Kansas City (Wichita)
Rice	Kansas City (Wichita)
Rush	Kansas City (Wichita)
Sedgwick	Kansas City (Wichita)

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 24 - 19

Stafford	Kansas City (Wichita)
Sumner	Kansas City (Wichita)
Wilson	Kansas City (Wichita)
Woodson	Kansas City (Wichita)

EFFECTIVE: 11/03/95

24-2.18 KENTUCKY

All counties covered by the office at Louisville.

EFFECTIVE: 01/31/78

24-2.19 LOUISIANA

All counties covered by the office at New Orleans.
Resident agencies listed have direct mail service.

COUNTY	COVERED BY OFFICE (RA)
Acadia	New Orleans (Lafayette)
Allen	New Orleans (Lafayette)
Beauregard	New Orleans (Lafayette)
Blenville	New Orleans (Shreveport)
Bossier	New Orleans (Shreveport)
Caddo	New Orleans (Shreveport)
Calacasiou	New Orleans (Lafayette)
Caldwell	New Orleans (Shreveport)
Cameron	New Orleans (Lafayette)
Claiborne	New Orleans (Shreveport)
DeSoto	New Orleans (Shreveport)
East Carroll	New Orleans (Shreveport)
Evangeline	New Orleans (Lafayette)
Fabine	New Orleans (Shreveport)
Franklin	New Orleans (Shreveport)
Iberia	New Orleans (Lafayette)
Jackson	New Orleans (Shreveport)
Jefferson Davis	New Orleans (Lafayette)
Lafayette	New Orleans (Lafayette)

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 24 - 20

Lincoln	New Orleans (Shreveport)
Madison	New Orleans (Shreveport)
Morehouse	New Orleans (Shreveport)
Ouachita	New Orleans (Shreveport)
Red River	New Orleans (Shreveport)
Richland	New Orleans (Shreveport)
St. Landry	New Orleans (Lafayette)
St. Martin	New Orleans (Lafayette)
St. Mary	New Orleans (Lafayette)
Tenfas	New Orleans (Shreveport)
Union	New Orleans (Shreveport)
Vermilion	New Orleans (Lafayette)
Webster	New Orleans (Shreveport)
West Carroll	New Orleans (Shreveport)

EFFECTIVE: 11/03/95

24-2.20 MAINE

All counties covered by the office at Boston.

EFFECTIVE: 07/26/89

24-2.21 MARYLAND

All counties covered by the office at Baltimore except in certain applicant-type cases. In cases involving other than Bureau applicants, the counties of Montgomery and Prince Georges are handled by the Washington Field Office (WFO). In Bureau support applicant cases, WFO handles recruiting and investigative leads in Montgomery, Prince Georges, Charles and St. Mary's Counties. In Special Agent applicant cases, all recruiting and investigative leads in Maryland are handled by the Baltimore Office.

EFFECTIVE: 03/14/97

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 24 - 21

24-2.22 MASSACHUSETTS

All counties covered by the office at Boston.

EFFECTIVE: 07/26/89

24-2.23 MICHIGAN

All counties covered by the office at Detroit. Resident
agency(s) listed has direct mail service.

COUNTY	COVERED BY OFFICE (RA)
Allegan	Detroit (Grand Rapids)
Barry	Detroit (Grand Rapids)
Berrien	Detroit (Grand Rapids)
Branch	Detroit (Grand Rapids)
Calhoun	Detroit (Grand Rapids)
Cass	Detroit (Grand Rapids)
Ionai	Detroit (Grand Rapids)
Kalamazoo	Detroit (Grand Rapids)
Kent	Detroit (Grand Rapids)
Lake	Detroit (Grand Rapids)
Mason	Detroit (Grand Rapids)
Mecasta	Detroit (Grand Rapids)
Montcalm	Detroit (Grand Rapids)
Muskegon	Detroit (Grand Rapids)
Newaygo	Detroit (Grand Rapids)
Oceana	Detroit (Grand Rapids)
Osceola	Detroit (Grand Rapids)
Ottawa	Detroit (Grand Rapids)
St. Joseph	Detroit (Grand Rapids)
Van Buren	Detroit (Grand Rapids)

EFFECTIVE: 11/03/95

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 24 - 22

24-2.24 MINNESOTA

All counties covered by the office at Minneapolis.

EFFECTIVE: 07/26/89

24-2.25 MISSISSIPPI

All counties covered by the office at Jackson.

EFFECTIVE: 07/26/89

24-2.26 MISSOURI

| Resident agencies listed have direct mail service. |

COUNTY	COVERED BY OFFICE (RA)
Adair	St. Louis
Andrew	Kansas City
Atchison	Kansas City
Audrain	St. Louis
Barry	Kansas City
Barton	Kansas City
Bates	Kansas City
Benton	Kansas City (Springfield)
Bollinger	St. Louis
Boone	Kansas City
Buchanan	Kansas City
Butler	St. Louis
Caldwell	Kansas City
Callaway	Kansas City
Camden	Kansas City
Cape Girardeau	St. Louis
Carroll	Kansas City
Carter	St. Louis
Cass	Kansas City
Cedar	Kansas City (Springfield)
Chariton	St. Louis

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 24 - 23

Christian	Kansas City (Springfield)
Clark	St. Louis
Clay	Kansas City
Clinton	Kansas City
Cole	Kansas City
Cooper	Kansas City
Crawford	St. Louis
Dade	Kansas City
Dallas	Kansas City (Springfield)
Daviess	Kansas City
De Kalb	Kansas City
Dent	St. Louis
Douglas	Kansas City (Springfield)
Dunklin	St. Louis
Franklin	St. Louis
Gasconade	St. Louis
Gentry	Kansas City
Greene	Kansas City (Springfield)
Grundy	Kansas City
Harrison	Kansas City
Henry	Kansas City (Springfield)
Hickory	Kansas City (Springfield)
Holt	Kansas City
Howard	Kansas City
Howell	Kansas City (Springfield)
Iron	St. Louis
Jackson	Kansas City
Jasper	Kansas City
Jefferson	St. Louis
Johnson	Kansas City
Knox	St. Louis
Laclede	Kansas City (Springfield)
Lafayette	Kansas City
Lawrence	Kansas City
Lewis	St. Louis
Lincoln	St. Louis
Linn	St. Louis
Livingston	Kansas City
Macon	St. Louis
Madison	St. Louis
Maries	St. Louis
Marion	St. Louis
McDonald	Kansas City
Mercer	Kansas City
Miller	Kansas City
Mississippi	St. Louis

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 24 - 24

Moniteau	Kansas City
Monroe	St. Louis
Montgomery	St. Louis
Morgan	Kansas City
New Madrid	St. Louis
Newton	Kansas City
Nodaway	Kansas City
Oregon	Kansas City (Springfield)
Osage	Kansas City
Ozark	Kansas City (Springfield)
Pemiscot	St. Louis
Perry	St. Louis
Pettis	Kansas City
Phelps	St. Louis
Pike	St. Louis
Platte	Kansas City
Polk	Kansas City (Springfield)
Pulaski	Kansas City (Springfield)
Putnam	Kansas City
Ralls	St. Louis
Randolph	St. Louis
Ray	Kansas City
Reynolds	St. Louis
Ripley	St. Louis
St. Charles	St. Louis
St. Clair	Kansas City (Springfield)
St. Francois	St. Louis
Sainte Genevieve	St. Louis
St. Louis	St. Louis
St. Louis City	St. Louis
Saline	Kansas City
Schuyler	St. Louis
Scotland	St. Louis
Scott	St. Louis
Shannon	St. Louis
Shelby	St. Louis
Stoddard	St. Louis
Stone	Kansas City (Springfield)
Sullivan	Kansas City
Taney	Kansas City (Springfield)
Texas	Kansas City (Springfield)
Vernon	Kansas City
Warren	St. Louis
Washington	St. Louis
Wayne	St. Louis
Webster	Kansas City (Springfield)

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 24 - 25

Worth
Wright

Kansas City
Kansas City (Springfield)

EFFECTIVE: 11/03/95

24-2.27 MONTANA

All counties covered by the office at Salt Lake City.
Resident agency(s) listed has direct mail service.

COUNTY	COVERED BY OFFICE (RA)
Beaverhead	Salt Lake City (Billings)
Big Horn	Salt Lake City (Billings)
Blaine	Salt Lake City (Billings)
Broadwater	Salt Lake City (Billings)
Carbon	Salt Lake City (Billings)
Carter	Salt Lake City (Billings)
Cascade	Salt Lake City (Billings)
Chouteau	Salt Lake City (Billings)
Custer	Salt Lake City (Billings)
Daniels	Salt Lake City (Billings)
Dawson	Salt Lake City (Billings)
Deer Lodge	Salt Lake City (Billings)
Fallon	Salt Lake City (Billings)
Fergus	Salt Lake City (Billings)
Flathead	Salt Lake City (Billings)
Gallatin	Salt Lake City (Billings)
Garfield	Salt Lake City (Billings)
Glacier	Salt Lake City (Billings)
Golden Valley	Salt Lake City (Billings)
Granite	Salt Lake City (Billings)
Hill	Salt Lake City (Billings)
Jefferson	Salt Lake City (Billings)
Judith Basin	Salt Lake City (Billings)
Lake	Salt Lake City (Billings)
Lewis And Clark	Salt Lake City (Billings)
Liberty	Salt Lake City (Billings)
Lincoln	Salt Lake City (Billings)
Madison	Salt Lake City (Billings)
McCone	Salt Lake City (Billings)
Meagher	Salt Lake City (Billings)

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 24 - 26

Mineral	Salt Lake City (Billings)
Missoula	Salt Lake City (Billings)
Musselshell	Salt Lake City (Billings)
Park	Salt Lake City (Billings)
Petroleum	Salt Lake City (Billings)
Phillips	Salt Lake City (Billings)
Pondera	Salt Lake City (Billings)
Powder River	Salt Lake City (Billings)
Powell	Salt Lake City (Billings)
Prairie	Salt Lake City (Billings)
Ravalli	Salt Lake City (Billings)
Richland	Salt Lake City (Billings)
Roosevelt	Salt Lake City (Billings)
Rosebud	Salt Lake City (Billings)
Sanders	Salt Lake City (Billings)
Sheridan	Salt Lake City (Billings)
Silver Bow	Salt Lake City (Billings)
Stillwater	Salt Lake City (Billings)
Sweet Grass	Salt Lake City (Billings)
Teton	Salt Lake City (Billings)
Toole	Salt Lake City (Billings)
Treasure	Salt Lake City (Billings)
Valley	Salt Lake City (Billings)
Wheatland	Salt Lake City (Billings)
Wibaux	Salt Lake City (Billings)
Yellowstone	Salt Lake City (Billings)

EFFECTIVE: 11/03/95

24-2.28 NEBRASKA

All counties covered by the office at Omaha.

EFFECTIVE: 08/27/90

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 24 - 27

24-2.29 NEVADA

All counties covered by the office at Las Vegas. Resident agency(s) listed has direct mail service.

COUNTY	COVERED BY OFFICE (RA)
Churchill	Las Vegas (Reno)
Douglas	Las Vegas (Reno)
Elko	Las Vegas (Reno)
Eureka	Las Vegas (Reno)
Humboldt	Las Vegas (Reno)
Lander	Las Vegas (Reno)
Lyon	Las Vegas (Reno)
Mineral	Las Vegas (Reno)
Pershing	Las Vegas (Reno)
Storey	Las Vegas (Reno)
Washoe	Las Vegas (Reno)
White Pine	Las Vegas (Reno)

EFFECTIVE: 11/03/95

24-2.30 NEW HAMPSHIRE

All counties covered by the office at Boston.

EFFECTIVE: 08/27/90

24-2.31 NEW JERSEY

All counties covered by the office at Newark except Camden, Gloucester, and Salem, which are handled by Philadelphia.

EFFECTIVE: 09/21/81

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 24 - 28

24-2.32 NEW MEXICO

All counties covered by the office at Albuquerque.
Resident agency(s) listed has direct mail service.

COUNTY	COVERED BY OFFICE (RA)
Dona Ana	Albuquerque (Las Cruces)
Grant	Albuquerque (Las Cruces)
Hidalgo	Albuquerque (Las Cruces)
Luna	Albuquerque (Las Cruces)
Otero	Albuquerque (Las Cruces)
Sierra	Albuquerque (Las Cruces)

EFFECTIVE: 03/14/97

24-2.33 NEW YORK

Resident agencies followed by RA have direct mail service.

COUNTY	COVERED BY OFFICE (RA)
Albany	Albany
Allegany	Buffalo
Bronx	New Rochelle
Broome	Albany
Cattaraugus	Buffalo
Cayuga	Albany
Chautauqua	Buffalo
Chemung	Buffalo
Chenango	Albany
Clinton	Albany
Columbia	Albany
Cortland	Albany
Delaware	Albany
Dutchess	New Rochelle
Erie	Buffalo
Essex	Albany
Franklin	Albany
Fulton	Albany
Genesee	Buffalo

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 24 - 29

Greene	Albany
Hamilton	Albany
Herkimer	Albany
Jefferson	Albany
Kings	Brooklyn-Queens - RA
Lewis	Albany
Livingston	Buffalo
Madison	Albany
Monroe	Buffalo
Montgomery	Albany
Nassau	Long Island - RA
New York	New York
Niagara	Buffalo
Oneida	Albany
Onondaga	Albany
Ontario	Buffalo
Orange	New Rochelle
Orleans	Buffalo
Oswego	Albany
Otsego	Albany
Putnam	New Rochelle
Queens	Brooklyn-Queens - RA
Rensselaer	Albany
Richmond	Brooklyn-Queens - RA
Rockland	New Rochelle
St. Lawrence	Albany
Saratoga	Albany
Schenectady	Albany
Schoharie	Albany
Schuyler	Buffalo
Seneca	Buffalo
Steuben	Buffalo
Suffolk	Long Island - RA
Sullivan	New Rochelle
Tioga	Albany
Tompkins	Albany
Ulster	Albany
Warren	Albany
Washington	Albany
Wayne	Buffalo
Westchester	New Rochelle
Wyoming	Buffalo
Yates	Buffalo

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 24 - 30

EFFECTIVE: 03/14/97

24-2.34 NORTH CAROLINA

All counties covered by the office at Charlotte.

EFFECTIVE: 01/31/78

24-2.35 NORTH DAKOTA

All counties covered by the office at Minneapolis.

EFFECTIVE: 01/31/78

24-2.36 OHIO

| Resident agencies listed have direct mail service. |

COUNTY	COVERED BY OFFICE (RA)
Adams	Cincinnati
Allen	Cleveland
Ashland	Cleveland
Ashtabula	Cleveland
Athens	Cincinnati (Columbus)
Auglaize	Cleveland
Belmont	Cincinnati (Columbus)
Brown	Cincinnati
Butler	Cincinnati (Dayton)
Carroll	Cleveland
Champaign	Cincinnati (Dayton)
Clark	Cincinnati (Dayton)
Clermont	Cincinnati
Clinton	Cincinnati (Dayton)
Columbiana	Cleveland
Coshocton	Cincinnati (Columbus)
Crawford	Cleveland

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 24 - 31

Cuyahoga	Cleveland
Darke	Cincinnati (Dayton)
Defiance	Cleveland
Delaware	Cincinnati (Columbus)
Erie	Cleveland
Fairfield	Cincinnati (Columbus)
Fayette	Cincinnati (Columbus)
Franklin	Cincinnati (Columbus)
Fulton	Cleveland
Gallia	Cincinnati (Columbus)
Geauga	Cleveland
Greene	Cincinnati (Dayton)
Guernsey	Cincinnati (Columbus)
Hamilton	Cincinnati
Hancock	Cleveland
Hardin	Cleveland
Harrison	Cincinnati (Columbus)
Henry	Cleveland
Highland	Cincinnati
Hocking	Cincinnati (Columbus)
Holmes	Cleveland
Huron	Cleveland
Jackson	Cincinnati
Jefferson	Cincinnati (Columbus)
Knox	Cincinnati (Columbus)
Lake	Cleveland
Lawrence	Cincinnati
Licking	Cincinnati (Columbus)
Logan	Cincinnati (Dayton)
Lorain	Cleveland
Lucas	Cleveland
Madison	Cincinnati (Columbus)
Mahoning	Cleveland
Marion	Cleveland
Medina	Cleveland
Meigs	Cincinnati (Columbus)
Mercer	Cleveland
Miami	Cincinnati (Dayton)
Monroe	Cincinnati (Columbus)
Montgomery	Cincinnati (Dayton)
Morgan	Cincinnati (Columbus)
Morrow	Cincinnati (Columbus)
Muskingum	Cincinnati (Columbus)
Noble	Cincinnati (Columbus)
Ottawa	Cleveland
Paulding	Cleveland

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 24 - 32

Perry	Cincinnati (Columbus)
Pickaway	Cincinnati (Columbus)
Pike	Cincinnati
Portage	Cleveland
Preble	Cincinnati (Dayton)
Putnam	Cleveland
Richland	Cleveland
Ross	Cincinnati
Sandusky	Cleveland
Scioto	Cincinnati
Seneca	Cleveland
Shelby	Cincinnati (Dayton)
Stark	Cleveland
Summit	Cleveland
Trumbull	Cleveland
Tuscarawas	Cleveland
Union	Cincinnati (Columbus)
Van Wert	Cleveland
Vinton	Cincinnati (Columbus)
Warren	Cincinnati (Dayton)
Washington	Cincinnati (Columbus)
Wayne	Cleveland
Williams	Cleveland
Wood	Cleveland
Wyandot	Cleveland

EFFECTIVE: 11/03/95

24-2.37 OKLAHOMA

All counties covered by the office at Oklahoma City.

EFFECTIVE: 09/21/81

24-2.38 OREGON

All counties covered by the office at Portland.

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 24 - 33

EFFECTIVE: 09/21/81

24-2.39 PENNSYLVANIA

The following counties in New Jersey are covered by the office at Philadelphia: Camden, Gloucester, and Salem. Resident agency(s) listed has direct mail service.

COUNTY	COVERED BY OFFICE (RA)
Adams	Philadelphia
Allegheny	Pittsburgh
Armstrong	Pittsburgh (Monongahela Valley)
Beaver	Pittsburgh
Bedford	Pittsburgh (Monongahela Valley)
Berks	Philadelphia
Blair	Pittsburgh (Monongahela Valley)
Bradford	Philadelphia
Bucks	Philadelphia
Butler	Pittsburgh
Cambria	Pittsburgh (Monongahela Valley)
Cameron	Philadelphia
Carbon	Philadelphia
Centre	Philadelphia
Chester	Philadelphia
Clarion	Pittsburgh
Clearfield	Pittsburgh (Monongahela Valley)
Clinton	Philadelphia
Columbia	Philadelphia
Crawford	Pittsburgh
Cumberland	Philadelphia
Dauphin	Philadelphia
Delaware	Philadelphia
Elk	Pittsburgh
Erie	Pittsburgh
Fayette	Pittsburgh (Monongahela Valley)
Forest	Pittsburgh
Franklin	Philadelphia
Fulton	Philadelphia
Greene	Pittsburgh (Monongahela Valley)
Huntingdon	Philadelphia
Indiana	Pittsburgh (Monongahela Valley)
Jefferson	Pittsburgh (Monongahela Valley)

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 24 - 34

Juniata	Philadelphia
Lackawanna	Philadelphia
Lancaster	Philadelphia
Lawrence	Pittsburgh
Lebanon	Philadelphia
Lehigh	Philadelphia
Luzerne	Philadelphia
Lycoming	Philadelphia
McKean	Pittsburgh
Mercer	Pittsburgh
Mifflin	Philadelphia
Monroe	Philadelphia
Montgomery	Philadelphia
Montour	Philadelphia
Northampton	Philadelphia
Northumberland	Philadelphia
Perry	Philadelphia
Philadelphia	Philadelphia
Pike	Philadelphia
Potter	Philadelphia
Schuylkill	Philadelphia
Snyder	Philadelphia
Somerset	Pittsburgh (Monongahela Valley)
Sullivan	Philadelphia
Susquehanna	Philadelphia
Tioga	Philadelphia
Union	Philadelphia
Venango	Pittsburgh
Warren	Pittsburgh
Washington	Pittsburgh (Monongahela Valley)
Wayne	Philadelphia
Westmoreland	Pittsburgh (Monongahela Valley)
Wyoming	Philadelphia
York	Philadelphia

EFFECTIVE: 03/14/97

24-2.40 RHODE ISLAND

All counties covered by the office at Boston.

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 24 - 35

EFFECTIVE: 01/31/78

24-2.41 SOUTH CAROLINA

All counties covered by the office at Columbia.

EFFECTIVE: 01/31/78

24-2.42 SOUTH DAKOTA

All counties covered by the office at Minneapolis. The
Pierre RA has supervisory responsibility over all counties and has
direct mail service.

EFFECTIVE: 11/03/95

24-2.43 TENNESSEE

Resident agencies listed have direct mail service.

COUNTY	COVERED BY OFFICE (RA)
Anderson	Knoxville
Bedford	Knoxville (Chattanooga)
Benton	Memphis
Bledsoe	Knoxville (Chattanooga)
Blount	Knoxville
Bradley	Knoxville (Chattanooga)
Campbell	Knoxville
Cannon	Memphis (Nashville)
Carroll	Memphis
Carter	Knoxville (Johnson City)
Cheatham	Memphis (Nashville)
Chester	Memphis
Claiborne	Knoxville (Johnson City)
Clay	Memphis (Nashville)
Cocke	Knoxville (Johnson City)

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 24 - 36

Coffee	Knoxville (Chattanooga)
Crockett	Memphis
Cumberland	Memphis (Nashville)
Davidson	Memphis (Nashville)
Decatur	Memphis
De Kalb	Memphis (Nashville)
Dickson	Memphis (Nashville)
Dyer	Memphis
Fayette	Memphis
Fentress	Memphis (Nashville)
Franklin	Knoxville Chattanooga
Gibson	Memphis
Giles	Memphis (Nashville)
Grainger	Knoxville (Johnson City)
Greene	Knoxville (Johnson City)
Grundy	Knoxville (Chattanooga)
Hamblen	Knoxville (Johnson City)
Hamilton	Knoxville (Chattanooga)
Hancock	Knoxville (Johnson City)
Hardeman	Memphis
Hardin	Memphis
Hawkins	Knoxville (Johnson City)
Haywood	Memphis
Henderson	Memphis
Henry	Memphis
Hickman	Memphis (Nashville)
Houston	Memphis (Nashville)
Humphreys	Memphis (Nashville)
Jackson	Memphis (Nashville)
Jefferson	Knoxville (Johnson City)
Johnson	Knoxville (Johnson City)
Knox	Knoxville
Lake	Memphis
Lauderdale	Memphis
Lawrence	Memphis (Nashville)
Lewis	Memphis (Nashville)
Lincoln	Knoxville (Chattanooga)
Loudon	Knoxville
Macon	Memphis (Nashville)
Madison	Memphis
Marion	Knoxville (Chattanooga)
Marshall	Memphis (Nashville)
Maury	Memphis (Nashville)
McMinn	Knoxville (Chattanooga)
McNairy	Memphis
Meigs	Knoxville (Chattanooga)

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 24 - 37

Monroe	Knoxville
Montgomery	Memphis (Nashville)
Moore	Knoxville (Chattanooga)
Morgan	Knoxville
Obion	Memphis
Overton	Memphis (Nashville)
Perry	Memphis
Pickett	Memphis (Nashville)
Polk	Knoxville (Chattanooga)
Putnam	Memphis (Nashville)
Rhea	Knoxville (Chattanooga)
Roane	Knoxville
Robertson	Memphis (Nashville)
Rutherford	Memphis (Nashville)
Scott	Knoxville
Sequatchie	Knoxville (Chattanooga)
Sevier	Knoxville (Johnson City)
Shelby	Memphis
Smith	Memphis (Nashville)
Stewart	Memphis (Nashville)
Sullivan	Knoxville (Johnson City)
Sumner	Memphis (Nashville)
Tipton	Memphis
Trousdale	Memphis (Nashville)
Unicoi	Knoxville (Johnson City)
Union	Knoxville
Van Buren	Knoxville (Chattanooga)
Warren	Knoxville (Chattanooga)
Washington	Knoxville (Johnson City)
Wayne	Memphis (Nashville)
Weakley	Memphis
White	Memphis (Nashville)
Williamson	Memphis (Nashville)
Wilson	Memphis (Nashville)

EFFECTIVE: 11/03/95

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 24 - 38

24-2.44 TEXAS

| Resident agencies listed have direct mail service. |

COUNTY	COVERED BY OFFICE (RA)
Anderson	Dallas (Tyler)
Andrews	El Paso
Angelina	Dallas (Tyler)
Aransas	Houston (Corpus Christi)
Archer	Dallas (Fort Worth)
Armstrong	Dallas (Lubbock)
Atascosa	San Antonio
Austin	Houston
Bailey	Dallas (Lubbock)
Bandera	San Antonio
Bastrop	San Antonio
Baylor	Dallas (Fort Worth)
Bee	Houston (Corpus Christi)
Bell	San Antonio
Bexar	San Antonio
Blanco	San Antonio
Borden	Dallas (Lubbock)
Bosque	San Antonio
Bowie	Dallas (Plano)
Brazoria	Houston (Texas City)
Brazos	Houston
Brewster	El Paso
Briscoe	Dallas (Lubbock)
Brooks	Houston (Corpus Christi)
Brown	Dallas (Lubbock)
Burleson	San Antonio
Burnet	San Antonio
Caldwell	San Antonio
Calhoun	Houston (Corpus Christi)
Callahan	Dallas (Lubbock)
Cameron	San Antonio (McAllen)
Camp	Dallas (Plano)
Carson	Dallas (Lubbock)
Cass	Dallas (Plano)
Castro	Dallas (Lubbock)
Chambers	Houston (Texas City)
Cherokee	Dallas
Childress	Dallas (Lubbock)
Clay	Dallas (Fort Worth)

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 24 - 39

Cochran	Dallas (Lubbock)
Coke	Dallas (Lubbock)
Coleman	Dallas (Lubbock)
Collin	Dallas (Plano)
Collingsworth	Dallas (Lubbock)
Colorado	Houston (Texas City)
Comal	San Antonio
Comanche	Dallas (Lubbock)
Concho	Dallas (Lubbock)
Cooke	Dallas (Plano)
Coryell	San Antonio
Cottle	Dallas (Fort Worth)
Crane	El Paso
Crockett	Dallas (Lubbock)
Crosby	Dallas (Lubbock)
Culberson	El Paso
Dallam	Dallas (Lubbock)
Dallas	Dallas
Dawson	Dallas (Lubbock)
Deaf Smith	Dallas (Lubbock)
Delta	Dallas (Plano)
Denton	Dallas (Plano)
De Witt	Houston (Corpus Christi)
Dickens	Dallas (Lubbock)
Dimmit	San Antonio
Donley	Dallas (Lubbock)
Duval	Houston (Corpus Christi)
Eastland	Dallas (Lubbock)
Ector	El Paso
Edwards	San Antonio
Ellis	Dallas
El Paso	El Paso
Erath	Dallas (Fort Worth)
Falls	San Antonio
Fannin	Dallas (Plano)
Fayette	Houston (Texas City)
Fisher	Dallas (Lubbock)
Floyd	Dallas (Lubbock)
Foard	Dallas (Fort Worth)
Fort Bend	Houston
Franklin	Dallas (Plano)
Freestone	San Antonio
Frio	San Antonio
Gaines	Dallas (Lubbock)
Galveston	Houston (Texas City)
Garza	Dallas (Lubbock)

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 24 - 40

Gillespie	San Antonio
Glasscock	Dallas (Lubbock)
Goliad	Houston (Corpus Christi)
Gonzales	San Antonio
Gray	Dallas (Lubbock)
Grayson	Dallas (Plano)
Gregg	Dallas (Tyler)
Grimes	Houston
Guadalupe	San Antonio
Hale	Dallas (Lubbock)
Hall	Dallas (Lubbock)
Hamilton	San Antonio
Hansford	Dallas (Lubbock)
Hardeman	Dallas (Fort Worth)
Hardin	Houston (Beaumont)
Harris	Houston
Harrison	Dallas (Tyler)
Hartley	Dallas (Lubbock)
Haskell	Dallas (Lubbock)
Hays	San Antonio
Hemphill	Dallas (Lubbock)
Henderson	Dallas (Tyler)
Hidalgo	San Antonio (McAllen)
Hill	San Antonio (McAllen)
Hockley	Dallas (Lubbock)
Hood	Dallas (Fort Worth)
Hopkins	Dallas (Plano)
Houston	Dallas (Tyler)
Howard	Dallas (Lubbock)
Hudspeth	El Paso
Hunt	Dallas (Plano)
Hutchinson	Dallas (Lubbock)
Irion	Dallas (Lubbock)
Jack	Dallas (Fort Worth)
Jackson	Houston (Texas City)
Jasper	Houston (Beaumont)
Jeff Davis	El Paso
Jefferson	Houston (Beaumont)
Jim Hogg	San Antonio
Jim Wells	Houston (Corpus Christi)
Johnson	Dallas (Fort Worth)
Jones	Dallas (Lubbock)
Karnes	San Antonio
Kaufman	Dallas
Kendall	San Antonio
Kenedy	Houston

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 24 - 41

Kent	Dallas (Lubbock)
Kerr	San Antonio
Kimble	San Antonio
King	Dallas (Fort Worth)
Kinney	San Antonio
Kleberg	Houston (Corpus Christi)
Knox	Dallas (Fort Worth)
Lamar	Dallas (Plano)
Lamb	Dallas (Lubbock)
Lampasas	San Antonio
LaSalle	San Antonio
Lavaca	Houston (Texas City)
Lee	San Antonio
Leon	San Antonio
Liberty	Houston (Beaumont)
Limestone	San Antonio
Lipscomb	Dallas (Lubbock)
Live Oak	Houston (Corpus Christi)
Llano	San Antonio
Loving	El Paso
Lubbock	Dallas (Lubbock)
Lynn	Dallas (Lubbock)
Madison	Houston
Marion	Dallas (Tyler)
Martin	El Paso
Mason	San Antonio
Matagorda	Houston (Texas City)
Maverick	San Antonio
McCulloch	San Antonio
McLennan	San Antonio
McMullen	San Antonio
Medina	San Antonio
Menard	Dallas (Lubbock)
Midland	El Paso
Milam	San Antonio
Mills	Dallas (Lubbock)
Mitchell	Dallas (Lubbock)
Montague	Dallas (Fort Worth)
Montgomery	Houston
Moore	Dallas (Lubbock)
Morris	Dallas (Plano)
Motley	Dallas (Lubbock)
Nacogdoches	Dallas (Tyler)
Navarro	Dallas
Newton	Houston (Beaumont)
Nolan	Dallas (Lubbock)

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 24 - 42

Nueces	Houston (Corpus Christi)
Ochiltree	Dallas (Lubbock)
Oldham	Dallas (Lubbock)
Orange	Houston (Beaumont)
Palo Pinto	Dallas (Fort Worth)
Panola	Dallas (Tyler)
Parker	Dallas (Fort Worth)
Parmer	Dallas (Lubbock)
Pecos	El Paso
Polk	Houston (Beaumont)
Potter	Dallas (Lubbock)
Presidio	El Paso
Rains	Dallas (Tyler)
Randall	Dallas (Lubbock)
Reagan	Dallas (Lubbock)
Real	San Antonio
Red River	Dallas (Plano)
Reeves	El Paso
Refugio	Houston (Corpus Christi)
Roberts	Dallas (Lubbock)
Robertson	San Antonio
Rockwall	Dallas (Plano)
Runnels	Dallas (Lubbock)
Rusk	Dallas (Tyler)
Sabine	Houston (Beaumont)
San Augustine	Houston (Beaumont)
San Jacinto	Houston
San Patricio	Houston (Corpus Christi)
San Saba	San Antonio
Schleicher	Dallas (Lubbock)
Scurry	Dallas (Lubbock)
Shackelford	Dallas (Lubbock)
Shelby	Dallas (Tyler)
Sherman	Dallas (Lubbock)
Smith	Dallas (Tyler)
Somervell	San Antonio
Starr	San Antonio (McAllen)
Stephens	Dallas (Lubbock)
Sterling	Dallas (Lubbock)
Stonewall	Dallas (Lubbock)
Sutton	Dallas (Lubbock)
Swisher	Dallas (Lubbock)
Tarrant	Dallas (Fort Worth)
Taylor	Dallas (Lubbock)
Terrell	San Antonio
Terry	Dallas (Lubbock)

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 24 - 43

Throckmorton	Dallas (Lubbock)
Titus	Dallas (Plano)
Tom Green	Dallas (Lubbock)
Travis	San Antonio
Trinity	Houston (Beaumont)
Tyler	Houston (Beaumont)
Upshur	Dallas (Tyler)
Upton	El Paso
Uvalde	San Antonio
Val Verde	San Antonio
Van Zandt	Dallas (Tyler)
Victoria	Houston (Corpus Christi)
Walker	Houston
Waller	Houston
Ward	El Paso
Washington	San Antonio
Webb	San Antonio
Wharton	Houston (Texas City)
Wheeler	Dallas (Lubbock)
Wichita	Dallas (Fort Worth)
Wilbarger	Dallas (Fort Worth)
Willacy	San Antonio (McAllen)
Williamson	San Antonio
Wilson	San Antonio
Winkler	El Paso
Wise	Dallas (Fort Worth)
Wood	Dallas (Tyler)
Yoakum	Dallas (Lubbock)
Young	Dallas (Fort Worth)
Zapata	San Antonio
Zavala	San Antonio

EFFECTIVE: 11/03/95

24-2.45 UTAH

All counties covered by the office at Salt Lake City.

EFFECTIVE: 01/31/78

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 24 - 44

24-2.46 VERMONT

All counties covered by the office at Albany, N.Y.

EFFECTIVE: 01/31/78

24-2.47 VIRGINIA

Resident agencies listed have direct mailing addresses.

INDEPENDENT CITIES

CITY	COVERED BY OFFICE (RA)
Alexandria	Washington Field Office (WFO)
Bedford	Richmond
Bristol	Richmond
Buena Vista	Richmond
Charlottesville	Richmond (Fredericksburg)
Chesapeake	Norfolk
Clifton Forge	Richmond
Colonial Heights	Richmond
Covington	Richmond
Culpeper	Richmond
Danville	Richmond
Emporia	Richmond
Fairfax	WFO
Falls Church	WFO
Franklin	Norfolk
Fredericksburg	Richmond (Fredericksburg)
Galax	Richmond
Hampton	Norfolk
Harrisonburg	Richmond (Fredericksburg)
Hopewell	Richmond
Leesburg	WFO
Lexington	Richmond
Lynchburg	Richmond
Manassas	WFO
Martinsville	Richmond
Newport News	Norfolk
Norfolk	Norfolk
Norton	Richmond

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 24 - 45

Petersburg	Richmond
Portsmouth	Norfolk
Quantico	WFO
Radford	Richmond
Richmond	Richmond
Roanoke	Richmond
Salem	Richmond
South Boston	Richmond
Staunton	Richmond (Fredericksburg)
Suffolk	Norfolk
Vienna	WFO
Virginia Beach	Norfolk
Warrenton	WFO
Waynesboro	Richmond (Fredericksburg)
Williamsburg	Norfolk
Winchester	Richmond (Fredricksburg)

COUNTIES

COUNTY	COVERED BY OFFICE (RA)
Accomack	Norfolk
Albemarle	Richmond (Fredericksburg)
Alleghany	Richmond
Amelia	Richmond
Amherst	Richmond
Appomattox	Richmond
Arlington	WFO
Augusta	Richmond (Fredericksburg)
Bath	Richmond
Bedford	Richmond
Bland	Richmond
Botetourt	Richmond
Brunswick	Richmond
Buchanan	Richmond
Buckingham	Richmond
Campbell	Richmond
Caroline	Richmond (Fredericksburg)
Carroll	Richmond
Charles City	Richmond
Charlotte	Richmond
Chesterfield	Richmond
Clarke	Richmond (Fredericksburg)
Craig	Richmond
Culpeper	Richmond (Fredericksburg)

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 24 - 46

Cumberland	Richmond
Dickenson	Richmond
Dinwiddle	Richmond
Essex	Richmond (Fredericksburg)
Fairfax	WFO
Fauquier	WFO
Floyd	Richmond
Fluvanna	Richmond (Fredericksburg)
Franklin	Richmond
Frederick	Richmond (Fredericksburg)
Giles	Richmond
Gloucester	Norfolk
Goochland	Richmond
Grayson	Richmond
Greene	Richmond (Fredericksburg)
Greensville	Richmond
Halifax	Richmond
Hanover	Richmond
Henrico	Richmond
Henry	Richmond
Highland	Richmond (Fredericksburg)
Isle of Wight	Norfolk
James City	Norfolk
King and Queen	Richmond (Fredericksburg)
King George	Richmond (Fredericksburg)
King William	Richmond
Lancaster	Richmond (Fredericksburg)
Lee	Richmond
Loudoun	WFO
Louisa	Richmond (Fredericksburg)
Lunenburg	Richmond
Madison	Richmond (Fredericksburg)
Mathews	Norfolk
Mecklenburg	Richmond
Middlesex	Richmond (Fredericksburg)
Montgomery	Richmond
Nansemond	Norfolk
Nelson	Richmond (Fredericksburg)
New Kent	Richmond
Northampton	Norfolk
Northumberland	Richmond (Fredericksburg)
Nottoway	Richmond
Orange	Richmond (Fredericksburg)
Page	Richmond (Fredericksburg)
Patrick	Richmond
Pittsylvania	Richmond

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 24 - 47

Powhatan	Richmond
Prince Edward	Richmond
Prince George	Richmond
Prince William	WFO
Pulaski	Richmond
Rappanhannock	Richmond (Fredericksburg)
Richmond	Richmond (Fredericksburg)
Roanoke	Richmond
Rockbridge	Richmond
Rockingham	Richmond (Fredericksburg)
Russell	Richmond
Scott	Richmond
Shenandoah	Richmond (Fredericksburg)
Smyth	Richmond
Southampton	Norfolk
Spotsylvania	Richmond (Fredericksburg)
Stafford	WFO
Surry	Richmond
Sussex	Richmond
Tazewell	Richmond
Warren	Richmond (Fredericksburg)
Washington	Richmond
Westmoreland	Richmond (Fredericksburg)
Wise	Richmond
Wythe	Richmond
York	Norfolk

AGENCIES

CIA	WFO
Pentagon	WFO

AIRPORTS

Dulles International	WFO
National	WFO

MILITARY BASES

Dahlgren Naval Station	Richmond (Fredericksburg)
Fort A. P. Hill	Richmond (Fredericksburg)
Fort Monroe	Norfolk
Navy Annex	WFO

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 24 - 48

EFFECTIVE: 03/14/97

24-2.48 WASHINGTON

All counties covered by the office at Seattle.

EFFECTIVE: 08/27/90

24-2.49 WEST VIRGINIA

All counties covered by the office at Pittsburgh.
Resident agency(s) listed has direct mail service.

COUNTY	COVERED BY OFFICE (RA)
Barbour	Pittsburgh (Monongahela Valley)
Berkeley	Pittsburgh (Monongahela Valley)
Braxton	Pittsburgh (Monongahela Valley)
Brooke	Pittsburgh (Monongahela Valley)
Calhoun	Pittsburgh (Monongahela Valley)
Doddridge	Pittsburgh (Monongahela Valley)
Gilmer	Pittsburgh (Monongahela Valley)
Grant	Pittsburgh (Monongahela Valley)
Hampshire	Pittsburgh (Monongahela Valley)
Hancock	Pittsburgh (Monongahela Valley)
Hardy	Pittsburgh (Monongahela Valley)
Harrison	Pittsburgh (Monongahela Valley)
Jefferson	Pittsburgh (Monongahela Valley)
Lewis	Pittsburgh (Monongahela Valley)
Marion	Pittsburgh (Monongahela Valley)
Marshall	Pittsburgh (Monongahela Valley)
Mineral	Pittsburgh (Monongahela Valley)
Monongalia	Pittsburgh (Monongahela Valley)
Morgan	Pittsburgh (Monongahela Valley)
Ohio	Pittsburgh (Monongahela Valley)
Pendleton	Pittsburgh (Monongahela Valley)
Pleasants	Pittsburgh (Monongahela Valley)
Pocahontas	Pittsburgh (Monongahela Valley)
Preston	Pittsburgh (Monongahela Valley)
Randolph	Pittsburgh (Monongahela Valley)

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 24 - 49

Ritchie	Pittsburgh (Monongahela Valley)
Taylor	Pittsburgh (Monongahela Valley)
Tucker	Pittsburgh (Monongahela Valley)
Upshur	Pittsburgh (Monongahela Valley)
Webster	Pittsburgh (Monongahela Valley)
Wetzel	Pittsburgh (Monongahela Valley)

EFFECTIVE: 03/19/97

24-2.50 WISCONSIN

All counties covered by the office at Milwaukee.

EFFECTIVE: 08/27/90

24-2.51 WYOMING

All counties covered by the office at Denver except
| Yellowstone National Park, covered by | Salt Lake City. |

EFFECTIVE: 08/27/90

24-3 POSSESSIONS AND COMMONWEALTHS

EFFECTIVE: 08/27/90

24-3.1 GUAM

Guam covered by the office at Honolulu.

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 24 - 50

EFFECTIVE: 08/27/90

24-3.2

NORTHERN MARIANAS

Commonwealth of Northern Marianas covered by office at
Honolulu.

EFFECTIVE: 08/27/90

24-3.3

PUERTO RICO

Commonwealth of Puerto Rico covered by the office at San
Juan.

EFFECTIVE: 08/27/90

24-3.4

VIRGIN ISLANDS

Virgin Islands covered by the office at San Juan.

EFFECTIVE: 08/27/90

24-4

STATE CAPITOLS

STATE	CAPITAL	COVERED BY OFFICE AT
Alabama	Montgomery	Mobile
Alaska	Juneau	Anchorage
Arizona	Phoenix	Phoenix
Arkansas	Little Rock	Little Rock
California	Sacramento	Sacramento
Colorado	Denver	Denver
Connecticut	Hartford	New Haven
Delaware	Dover	Baltimore

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 24 - 51

Florida	Tallahassee	Jacksonville
Georgia	Atlanta	Atlanta
Hawaii	Honolulu	Honolulu
Idaho	Boise	Salt Lake City
Illinois	Springfield	Springfield
Indiana	Indianapolis	Indianapolis
Iowa	Des Moines	Omaha
Kansas	Topeka	Kansas City
Kentucky	Frankfort	Louisville
Louisiana	Baton Rouge	New Orleans
Maine	Augusta	Boston
Maryland	Annapolis	Baltimore
Massachusetts	Boston	Boston
Michigan	Lansing	Detroit
Minnesota	St. Paul	Minneapolis
Mississippi	Jackson	Jackson
Missouri	Jefferson City	Kansas City
Montana	Helena	Salt Lake City
Nebraska	Lincoln	Omaha
Nevada	Carson City	Las Vegas
New Hampshire	Concord	Boston
New Jersey	Trenton	Newark
New Mexico	Santa Fe	Albuquerque
New York	Albany	Albany
North Carolina	Raleigh	Charlotte
North Dakota	Bismarck	Minneapolis
Ohio	Columbus	Cincinnati
Oklahoma	Oklahoma City	Oklahoma City
Oregon	Salem	Portland
Pennsylvania	Harrisburg	Philadelphia
Rhode Island	Providence	Boston
South Carolina	Columbia	Columbia
South Dakota	Pierre	Rapid City
Tennessee	Nashville	Memphis
Texas	Austin	San Antonio
Utah	Salt Lake City	Salt Lake City
Vermont	Montpelier	Albany
Virginia	Richmond	Richmond
Washington	Olympia	Seattle
West Virginia	Charleston	Pittsburgh
Wisconsin	Madison	Milwaukee
Wyoming	Cheyenne	Denver

Sensitive

PRINTED: 02/18/98

~~CONFIDENTIAL~~

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 24 - 52

EFFECTIVE: 08/27/90

24-5

UNITED STATES - MEXICO BORDER

[REDACTED]

[REDACTED]

[REDACTED]

(C) [REDACTED]

[REDACTED]

(C)

b1

All other requests for investigations in foreign countries should be sent to the Bureau.

EFFECTIVE: 11/03/95

ALL INFORMATION CONTAINED
HERE IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

Administrative 6-2-98
CLASSIFIED BY: S05J/129m
REASON: 1.5 (b)(5)
DECLASSIFY ON: X 26

~~CONFIDENTIAL~~

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 24 - 53

24-6 FOREIGN COUNTRIES

| Territorial allocation details are no longer maintained in the manuals. An up-to-date listing is available in the FOIMS Tables Application, "Territorial Allocation, Foreign Territorial Allocation" options. |

EFFECTIVE: 11/16/93

Sensitive
PRINTED: 02/18/98

XXXXXX
XXXXXX
XXXXXXFEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET29

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 552Section 552a☐ (b)(1)☐ (b)(7)(A)☐ (d)(5)☒ (b)(2)☐ (b)(7)(B)☐ (j)(2)☐ (b)(3)☐ (b)(7)(C)☐ (k)(1)☐ (b)(7)(D)☐ (k)(2)☒ (b)(7)(E)☐ (k)(3)☐ (b)(7)(F)☐ (k)(4)☐ (b)(4)☐ (b)(8)☐ (k)(5)☐ (b)(5)☐ (b)(9)☐ (k)(6)☐ (b)(6)☐ (k)(7)

- ☐ Information pertained only to a third party with no reference to the subject of your request or the subject of your request is listed in the title only.

- ☐ Documents originated with another Government agency(ies). These documents were referred to that agency(ies) for review and direct response to you.

Pages contain information furnished by another Government agency(ies). You will be advised by the FBI as to the releasability of this information following our consultation with the other agency(ies).

Page(s) withheld inasmuch as a final release determination has not been made. You will be advised as to the disposition at a later date.

Pages were not considered for release as they are duplicative of _____

Page(s) withheld for the following reason(s): _____

- ☒ The following number is to be used for reference regarding these pages:

MIOG Pt II Sec 25

XXXXXXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X for this page X
XXXXXXXXXXXXXXXXXXXX

XXXXXX
XXXXXX
XXXXXX

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 26 - 1

SECTION 26. CLASSIFIED NATIONAL SECURITY INFORMATION AND MATERIAL

26-1 DELETED

EFFECTIVE: 02/12/92

26-2 GENERAL CLASSIFICATION INSTRUCTIONS

When material is prepared in the FBI which relates to national security and which meets the criteria of Executive Order 12356, it must be classified and marked in accordance with the provisions of that Order as outlined in this section. Information may be classified or reclassified after an agency has received a request for it under the Freedom of Information Act or the Privacy Act, if such classification meets the requirements for classification and is accomplished personally and on a document-by-document basis by an individual with original Top Secret classification authority. Information shall not be declassified automatically as a result of any unofficial publication or inadvertent or unauthorized disclosure in the United States or abroad of identical or similar information. The Attorney General may reclassify information previously declassified and disclosed if it is determined in writing that (1) the information requires protection in the interest of national security; and (2) the information may reasonably be recovered. These reclassification actions shall be reported promptly to the Director of the Information Security Oversight Office (ISOO). See ISOO Directive Number One, Section 2001.6 for reporting requirements.

EFFECTIVE: 02/12/92

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 26 - 2

26-2.1 Authority to Classify, Declassify, Upgrade and Downgrade

(1) Classification may be accomplished through use of a prepared guide which contains instructions for its use and which details the information to be classified, lists the classifying authority, and shows the level of classification and the length of time to remain classified. An example of such a guide is "Classification Guide No. 1" (G-1) regarding Foreign Government Information.

(2) Information may also be classified by incorporating, paraphrasing, restating, or generating in new form information that is already classified. This type of classification, including the use of classification guides, is known as "derivative classification." If previously classified information is used as the basis for classification, the previous markings must be honored and the original source documents must be shown on the "Classified by" line in a manner that will afford retrieval of the source document. Information to be classified which is not classified derivatively may only be classified by an individual having the authority to classify and in accordance with procedures set forth hereinafter.

(3) Authority to classify (or upgrade) material is strictly limited to specifically designated officials and supervisors approved in writing by the Attorney General. Such approval is handled through the Security|Clearances|Unit, Security|Countermeasures|Section,|Intelligence|Division, at FBIHQ.

(4) Agents or support personnel preparing national security material should determine whether there is a basis for classification, the level of classification, and the reasons, but only authorized classifiers may approve such classification (unless it is derivative classification), and only their credential numbers may be used as the classifying authority. In the absence of an authorized classifier, an individual not authorized, such as a relief supervisor, acting on authorized classifier's behalf, may classify material utilizing the authorized classifier's credential number.

(5) Classified material may be downgraded or declassified only by the original classifying authority, by a successor acting in the same capacity, by a supervisory official of either, or by officials delegated such authority in writing by the FBI Security Programs Manager. The successor or supervisory official need not be a classifying authority to downgrade or declassify. Information classified derivatively by classification guides may be downgraded or declassified by Special Agents in Charge and Senior Legal Attaches.

Administrative
ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 6-2-98 BY SP5 JCL/m

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 26 - 3

(6) Those individuals in the FBI who have been designated as Original Top Secret Classification Authorities may not redelegate that (or a lesser) classification authority.

(7) The Attorney General of the United States has established the Department Review Committee (DRC) (see 28, Code of Federal Regulations (CFR), Section 17.135) as Department of Justice's (DOJ's) component responsible for the resolution of all issues concerning the implementation and administration of Executive Order 12356 which concerns national security material. The DRC is composed of representatives from various components within DOJ, including the FBI. Classification actions are discussed and voted upon. The DRC may vote to uphold the FBI classification action or may vote that classification is not warranted. The DRC will review and resolve all issues concerning a number of FBI classification actions, which, in part, may relate to:

(a) Administrative appeals of requests for records under the Freedom of Information Act (Title 5, USC, Section 552) and mandatory reviews for declassification when the FBI's proposed denial of information to the requestor is based upon national security concerns;

(b) All classified material which will require the submission of an affidavit or declaration to the Court to justify the nondisclosure of national security information pursuant to Freedom of Information/Privacy Acts (FOI/PA) exemptions or assertion of a "State Secret Claim."

The Document Classification Unit (DCU), Security Section (SS), Information Management Division (IMD), is responsible for liaison with the DRC and should be consulted in connection with any submission of material to the DRC.

EFFECTIVE: 02/12/92

26-2.2 Basis for Classifying Material

EFFECTIVE: 09/26/90

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 26 - 4

26-2.2.1 Criteria for Classifying Material

For material to be considered for classification, it must meet one or more of the following criteria:

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] b2

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

EFFECTIVE: 09/26/90

26-2.2.2 Damage Requirement

Information that is determined to concern one or more of the categories in 26-2.2.1 shall be classified when an original classification authority also determines that its unauthorized disclosure, either by itself or in the context of other information, reasonably could be expected to cause damage to the national security.

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 26 - 5

EFFECTIVE: 09/26/90

26-2.2.3 Reason for Classifying Otherwise Unclassifiable Material
in Context of Other Material

(1) Certain information which would otherwise be unclassified when standing alone (such as an FD-302, address, or the like), may require classification when combined or associated with other unclassified or classified information. In the context where this normally unclassified information would reveal our investigative interest in certain individuals, organizations, or countries, thereby causing the information now to fall within one of the criteria listed in 26-2.2.1 above, such as an intelligence activity or method, and it meets the criteria in 26-2.2.2, it should be classified.

(2) As a rule, the above basis for classification will be used infrequently inasmuch as the vast majority of classifiable FBI information will be readily identifiable as falling within the categories of (a) foreign government information, (b) intelligence sources, activities, or methods, or (c) foreign relations. Whenever the information is deemed to warrant classification based on the above reason (since it is not readily apparent that it falls within the 26-2.2.1 criteria), a reference must be made to the above reason on the face of the document. This will be accomplished by adding a line below the "Classified by _____" line as follows:

Classified by _____
Reason for Classification: FCIM II, 1-2.2.3
Declassify on: OADR

(3) The above does not apply to situations where the date of the communication, the page number, and otherwise innocuous information warrants classification on the basis that the entire document should be classified to protect the fact that the FBI has an investigation concerning that matter.

EFFECTIVE: 09/26/90

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 26 - 6

26-2.3 Classification Guidance

Section 26-2.2.1, supra, identified the categories of information that shall be considered for classification. Of the categories listed, those most likely to be encountered by FBI classifiers are:

b2

[REDACTED]

To assist classification authorities in rendering classification determinations concerning this information, the following guidance is supplied:

EFFECTIVE: 09/26/90

26-2.3.1 [REDACTED]

b2

XXXXXX
XXXXXX
XXXXXXFEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET5

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 552Section 552a☐ (b)(1)☐ (b)(7)(A)☐ (d)(5)☒ (b)(2)☐ (b)(7)(B)☐ (j)(2)☐ (b)(3)☐ (b)(7)(C)☐ (k)(1)☐ (b)(7)(D)☐ (k)(2)☐ (b)(7)(E)☐ (k)(3)☐ (b)(7)(F)☐ (k)(4)☐ (b)(4)☐ (b)(8)☐ (k)(5)☐ (b)(5)☐ (b)(9)☐ (k)(6)☐ (b)(6)☐ (k)(7)

- ☐ Information pertained only to a third party with no reference to the subject of your request or the subject of your request is listed in the title only.

- ☐ Documents originated with another Government agency(ies). These documents were referred to that agency(ies) for review and direct response to you.

Pages contain information furnished by another Government agency(ies). You will be advised by the FBI as to the releasability of this information following our consultation with the other agency(ies).

Page(s) withheld inasmuch as a final release determination has not been made. You will be advised as to the disposition at a later date.

Pages were not considered for release as they are duplicative of _____

Page(s) withheld for the following reason(s): _____

- ☒ The following number is to be used for reference regarding these pages:

MIOS manual

XXXXXXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X for this page X
XXXXXXXXXXXXXXXXXXXX

XXXXXX
XXXXXX
XXXXXX

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 26 - 12

26-2.4 Categories (Levels) of Classification

(1) There are three categories or levels of classification: "Top Secret," "Secret," and "Confidential."

(a) "Top Secret" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security.

(b) "Secret" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security.

(c) "Confidential" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security.

(2) If there is reasonable doubt about the need to classify information, it shall be safeguarded as if it were classified pending a determination by an original classification authority, who shall make this determination within thirty (30) days. If there is reasonable doubt about the appropriate level of classification, it shall be safeguarded at the highest level of classification pending a determination by an original classification authority, who shall make this determination within thirty (30) days.

EFFECTIVE: 02/23/84

26-2.5 Duration of Classification

Information shall be classified as long as required by national security consideration. The phrase "Originating Agency's Determination Required," as indicated by the abbreviation "OADR," will be utilized to show the duration of classification, except in those rare instances where there is a clear determination the information can be declassified on a specific date or event.

EFFECTIVE: 02/12/92

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 26 - 13

26-2.6 Classification Markings

(1) The following markings must be shown on the front page of all classified documents, except teletypes, which will be covered separately:

(a) Classification level ("Top Secret," "Secret," or "Confidential") at the top and bottom of: the front cover, if any; the title page, if any; the first page; the last page; the reverse side of the last page or cover. In addition, each interior page must be marked at the top and bottom according to the highest overall level of classification of the entire document.

(b) The identity of the classifying authority (credential number), classification guide number, or source document (if derivative).

(c) The notation, "Declassify on: Originating Agency's Determination Required" or "OADR," unless there is a clear determination the information can be declassified on a specific date or event. In the vast majority of cases, OADR will apply.

Example: Classified by (credential number)
Declassify on: OADR

(d) In instances where the identity of the originating agency and office are not apparent on the face of a document, the identity of the originating agency must be placed below the "Classified by" line (ISOO Dir. No. 1, Section 2001.5 (c)). This situation would occur most frequently at FBIHQ in classifying other Government agency information, such as an INS record. The FBI would be considered the originating agency for the classification decision in this instance and would have to be so noted. If this addition warrants classification, the portion should be marked accordingly.

(2) An ISOO booklet entitled "Marking," which is available from the Information Systems Security Unit, Security Countermeasures Section, Intelligence Division, FBIHQ, contains detailed, yet simple, instructions and examples on marking classified documents.

(3) When material is classified solely because of other agency data, it must be appropriately marked to correspond with the other agency's markings.

(4) When classified material is downgraded, upgraded or

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 26 - 14

declassified, a line will be drawn through the previous level of classification and related markings, and the new level, along with "upgraded," "downgraded" or "declassified," noted adjacent thereto, together with the date and credential number of the declassifier or classification authority, whichever is appropriate.

EFFECTIVE: 10/14/93

26-2.6.1 Internal Documents Prior to 1974

Prior to 1974, classification markings were not included on classifiable internal FBI documents. All such documents, when subject to disclosure, must be reviewed and appropriately marked for classification.

EFFECTIVE: 03/23/92

26-2.6.2 Marking of Separate Documents and Transmittal Documents

FBI reports have two parts, the cover page(s) and the report itself. For classification purposes, each part must be considered separately and marked appropriately. There will be instances when the cover page(s) is classified but not the report, and vice versa. Each part must indicate the level of classification, identity of the classifying officer, declassification date, etc. Similarly, a transmittal document, such as a cover letter/airtel to an LHM, a form letter, or a routing slip must be considered separately and marked accordingly. An unclassified transmittal document must be marked top and bottom of the front page with the highest classification level of any information transmitted by it. It must also be marked with an appropriate instruction indicating it is unclassified when separated from classified enclosure(s). If the transmittal document itself contains classified information, mark it as required for all other classified information, except:

(1) conspicuously mark the top and bottom of the front page of the transmittal document with the highest classification level of any information contained in the transmittal document or its enclosures; and

(2) mark the transmittal document with an appropriate

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 26 - 15

instruction indicating its overall classification level when separated from its enclosures.

EFFECTIVE: 03/23/92

26-2.6.3 Marking Separate Paragraphs (See MIOG, Part II, 16-18.8.2(2), 16-18.8.13(5); Correspondence Guide-HQ, 1-4.1(3); Correspondence Guide-Field, 1-21.1(3); FCIM, Part II, 1-2.6.3.)

(1) Whenever portions of classified material require different levels of classification, then each paragraph or portion must be marked to show its classification or that it is unclassified. (A "portion" includes the title or subject, as well as a paragraph, sentence or word of a communication.) In marking individual portions, the appropriate marking ("Top Secret," "Secret," "Confidential," or "Unclassified") should be typed in parentheses immediately following the portion in question. Abbreviations may be used (TS, S, C, or U). An introductory caveat, such as "This document is classified 'Secret' in its entirety, unless otherwise noted," may be used when the majority of the document is at the same level, thereby requiring only the portions that differ to be marked. A similar statement should be used to show the document is classified in its entirety, if that is the case. (See (2) below.)

(2) The FBINET subnetwork is authorized to process up to and including SECRET/collateral data. Under no circumstance may TOP SECRET (TS) or Sensitive Compartmented Information (SCI) be processed by FBINET, or entered into any Automated Information System (AIS) which is accessed by FBINET. AISs which utilize the FBINET subnetwork include: the Field Office Information Management System (FOIMS); the Resource Management System (RMS); the Criminal Law Enforcement Application (CLEA); the Criminal Law Enforcement System (CLES); the Investigative Support Information System (ISIS); the Uniform Crime Reporting System (UCRS); the Legal Counsel Information System (LCIS); and, the Training Division Support System (TDSS). To ensure compliance with this restriction, all correspondence containing TS or SCI data will be "portion marked" to show specific classification levels (i.e., title, each paragraph, etc.) Although a document may have an overall classification of TS and/or SCI, frequently the information to be entered into the AIS may actually be classifiable at a lower level. Portion marking will allow for that information which is classified as SECRET/collateral or below (if any) to be entered

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 26 - 16

into AISs accessed by the FBINET subnetwork. Under no circumstances may SCI, regardless of classification level, be processed on the FBINET subnetwork or entered into any AIS accessed by the FBINET subnetwork. However, SCI material can be appropriately downgraded, based on the approval of the originating agency, to the SECRET/CONFIDENTIAL collateral level through written summaries, etc., so it may be processed via FBINET. (Also see MIOG, Part II, Section 26-2.6.3(1).)

EFFECTIVE: 11/25/94

26-2.6.4 Marking Teletypes

Teletypes are marked with the classification level ("UNCLAS" or "UNCLAS E F T O," if unclassified) preceding the text on the first page and at the top of each succeeding page. The abbreviation "C BY _____; DECL: OADR" will be utilized at the end of the message on teletypes.

EFFECTIVE: 03/23/92

26-2.6.5 Marking Derivatively Classified Documents Being Disseminated Outside the FBI

When documents are being disseminated outside the FBI and have been classified derivatively, they should be treated as follows:

(1) If the derivative source is a single document, mark the outgoing copies "Classified by Derivative Source," and identify the source document on all FBI copies.

(2) If the derivative source is multiple documents or sources, mark the outgoing copies "Classified by Multiple Sources," and identify the multiple sources on all FBI copies.

EFFECTIVE: 03/23/92

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 26 - 17

26-2.7 Material With Different Classification Levels or
Declassification Dates

When classified material consists of two or more items of information which bear different classification levels or declassification dates, the following guidelines apply:

(1) Material containing different levels of classified information must be classified at the level of the highest classified component.

(2) Material containing different declassification dates must be marked with the most distant declassification date.

EFFECTIVE: 02/12/92

26-3 SPECIAL CLASSIFICATION INSTRUCTIONS

The procedures set forth above will not cover all situations involving classification matters. It is emphasized that the objective is to protect national security material in our files in a practical and reasonable manner. In connection with any problems not covered in these instructions which cannot be handled locally, the Security|Clearances|Unit, Security|Countermeasures|Section, Intelligence|Division, should be consulted. Following are some special classification instructions representing classification decisions that have already been made and should be adhered to.

EFFECTIVE: 02/12/92

26-3.1 Classification of Notes

(1) When a note containing classified information is affixed to a communication that is unclassified, they should be treated as a single document and marked accordingly. In actual practice, this would mean that the original communication going to the field would be unmarked and would bear no reference to any classified material, whereas the FBIHQ copies containing the note would be classified and marked accordingly. The classified document would either have to be portion-marked or contain a caveat to the effect that all portions are unclassified unless otherwise noted. This caveat should not appear on the original unclassified document.

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 26 - 18

(2) When classified enclosures are added to the above example, each package should be treated separately. The markings on each transmittal letter would be handled in accordance with instructions set forth in 26-2.6.2 above.

(3) For variations of the above, such as when the original and note are both classified, but at different levels, the same logic would apply, i.e., they would be treated as a single document. The reasoning behind treating the note and communication as a single document is because, generally, they are both prepared at the same time by the same person and are not intended to be utilized separately. In the event a note is added to a document at a later time by someone other than the originator of the document, that person has the responsibility to ensure proper classification procedures are followed with respect to the note.

EFFECTIVE: 02/23/84

26-3.2 Classification of Addenda and Attachments to Documents

(1) The intent behind Executive Order 12356 is that the individual generating information meeting the criteria for classification has the responsibility for ensuring that it is properly classified. In the situation where addenda are added to a communication by someone other than the originator, that person has the responsibility of ensuring that this information is properly classified. Even though an addendum is not likely to be used separately, it should still be marked as separate document, notwithstanding the fact that it might be numbered as if it were a single document. The key element is that it represents another individual's thought, and that individual has the responsibility to classify it. It would, therefore, be possible for a memorandum to be classified "Secret" in its entirety, one addendum to be "Unclassified," and another to be classified in part.

(2) Consideration should be given always to the possibility that an otherwise unclassified addendum might warrant classification by virtue of it being linked with a classified memorandum. If the originator of the memorandum determines an addendum prepared by another individual should have been classified, he/she has the prerogative to classify it.

(3) Since each component is to be marked as a separate

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 26 - 19

document, a notation on the first page of a memorandum, such as "All information contained herein is classified "Secret" unless otherwise noted," would apply only to the memorandum and not to any attachments or addenda. Likewise, the "Secret" markings at the top and bottom of each page of the memorandum should not be applied to the attachments or addenda unless they also are "Secret." They should be marked at the appropriate level of classification of the newly created document(s).

(4) In situations where memoranda with addenda attached are being reviewed for classification, such as pursuant to a Freedom of Information Act request, each part should be treated as a separate document to avoid confusion and enhance uniformity.

EFFECTIVE: 02/23/84

26-3.3

[REDACTED]

b2

EFFECTIVE: 02/23/84

26-3.4

[REDACTED]

Sensitive
PRINTED: 02/18/98

XXXXXX
XXXXXX
XXXXXXFEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET3

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 552Section 552a☐ (b)(1)☐ (b)(7)(A)☐ (d)(5)☒ (b)(2)☐ (b)(7)(B)☐ (j)(2)☐ (b)(3)☐ (b)(7)(C)☐ (k)(1)☐ (b)(7)(D)☐ (k)(2)☐ (b)(7)(E)☐ (k)(3)☐ (b)(7)(F)☐ (k)(4)☐ (b)(4)☐ (b)(8)☐ (k)(5)☐ (b)(5)☐ (b)(9)☐ (k)(6)☐ (b)(6)☐ (k)(7)

☐ Information pertained only to a third party with no reference to the subject of your request or the subject of your request is listed in the title only.

☐ Documents originated with another Government agency(ies). These documents were referred to that agency(ies) for review and direct response to you.

Pages contain information furnished by another Government agency(ies). You will be advised by the FBI as to the releasability of this information following our consultation with the other agency(ies).

Page(s) withheld inasmuch as a final release determination has not been made. You will be advised as to the disposition at a later date.

Pages were not considered for release as they are duplicative of _____

Page(s) withheld for the following reason(s): _____

☒ The following number is to be used for reference regarding these pages:

MIOS manual

XXXXXXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X for this page X
XXXXXXXXXXXXXXXXXXXX

XXXXXX
XXXXXX
XXXXXX

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 26 - 23

26-3.12

b2

EFFECTIVE: 11/21/89

26-3.13

GIA - Classification of Covert Operations

b3
b7c
CIA

EFFECTIVE: 11/21/89

26-4

ACCESS TO CLASSIFIED INFORMATION BY INDIVIDUALS HAVING
OFFICIAL CLEARANCES

All FBI employees are cleared for access to classified national security material up to and including "Top Secret" on a strict need-to-know basis. No individual is to be permitted access to classified or classifiable material appearing in the files of the FBI unless they have been afforded official clearance for such access and have a need to know. It will be incumbent upon each FBI employee permitting such access to be assured the required clearance has been obtained. Questions as to whether an individual is cleared for access to national security material which cannot be resolved locally are to be referred to the Security Programs Manager at FBIHQ. Any instance of unauthorized access or attempted unauthorized access to national security material should be promptly reported to Director, FBI, Attention: Security Programs Manager.

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 26 - 24

EFFECTIVE: 05/26/89

26-4.1 Inadvertent Unauthorized Access to National Security
Information

(1) In cases where national security information has been disclosed to an individual who has not had appropriate clearance(s) or has inadvertently had unauthorized access to national security information, that individual, once interviewed and briefed as to his/her responsibility and obligation not to disclose national security information, is to sign and date the Inadvertent Disclosure Statement, Form FD-722. This form provides an affirmation suitable for execution by any individual who has inadvertently obtained national security information. The form is to be witnessed by the FBI representative present. An individual who does not wish to sign the FD-722 should be briefed as to its contents. The reason for refusal should be noted on the form, which will then be appropriately witnessed.

(2) The original and one copy of the executed FD-722 are to be forwarded to FBIHQ, Attention: Security Programs Manager, as enclosures to a self-explanatory cover memorandum.

EFFECTIVE: 05/26/89

26-5 STORAGE OF CLASSIFIED MATERIAL (See MIOG, Part I, 261-2
(3) (a), (4) (a); Part II, 16-7.2.6 (9) (g), 35-9.4.9; NFIPM,
Part 1, 8-5; Correspondence Guide - Field, 1-21.7.)

Introduction

Classified material, including classified information on storage media used by typewriters, word processors, or remote terminal equipment, shall be protected at all times. Whenever classified material is not under the personal control (observable and sufficiently close to prevent unauthorized access) of an authorized and appropriately cleared person, whether during or outside of working hours, it will be guarded or stored in a locked security container, as described herein, or a secure storage room, as described in Section 26-5.2. FBI employees are responsible for the protection and storage of classified information and material in

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 26 - 25

their custody. It is the responsibility of the holder of classified material to ensure that material is properly protected and, through verification of clearance/access and need to know, not provided to an individual who is neither authorized nor cleared to receive it. Storage equipment not functioning in a normal manner shall be immediately reported to the appropriate Security Countermeasures Program Manager or Security Officer for corrective action. The adjustment or repair of security equipment will be accomplished only by trained personnel. Until repairs have been made, defective equipment shall not be used to safeguard classified items.

EFFECTIVE: 09/09/97

26-5.1 Storage of "Top Secret" Material (See MIOG, Part II, 35-9.4.9; NFIPM, Part 1, 8-5.1; MAOP, Part II, 2-4.3.1 (1)(k); Correspondence Guide - Field, 1-21.7.)

"Top Secret" material must be stored in a General Services Administration (GSA)-approved [REDACTED] b2

[REDACTED] Resident agencies, Legal Attache offices, and field office and FBIHQ off-site facilities are not authorized to process or maintain "Top Secret" material or information unless approved in writing by the Security Programs Manager, National Security Division, FBIHQ. All "Top Secret" material must be segregated from general files, whether pending or closed, and stored in approved containers. Only FBI employees and other specified personnel with a verified security clearance and a "need to know" shall have access to "Top Secret" material.

EFFECTIVE: 09/09/97

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 26 - 26

26-5.2 Storage of "Secret" and "Confidential" Material
(See MIOG, Part II, 26-5, 35-9.4.9; NFIPM, Part 1, 8-5.2; Correspondence Guide - Field, 1-21.7.)

"Secret" and "Confidential" material must be stored in GSA-approved security containers having GSA-approved, [REDACTED] "Secret" and "Confidential" information may be openly stored (not in a GSA-approved safe) in a secure storage room which has been approved in accordance with specific Department of Justice requirements. Although similar in construction, these secure facilities are not Sensitive Compartmented Information Facilities (SCIFs) and are not approved for the storage of Sensitive Compartmented Information (SCI) at any level of classification. The approval for a secure storage room for the open storage of classified material must be obtained in writing from the Security Programs Manager, National Security Division, FBIHQ. Access to "Secret" and "Confidential" material is limited to appropriate personnel with a verified security clearance and a need to know.

EFFECTIVE: 09/09/97

26-5.2.1 Storage of "Sensitive Compartmented Information (SCI)"
(See NFIPM, Part 1, 8-5.2.1; MAOP, Part II, 2-4.3.1
(1) (k); Correspondence Guide - Field, 1-21.7.)

(1) SCI is classified information (Confidential, Secret, or Top Secret) concerning or derived from intelligence sources, methods, or analytical processes, which is required to be handled within formal access control systems established by the Director of Central Intelligence (DCI). SCI is sometimes referred to as "codeword" material.

(2) The Director of Central Intelligence Directive (DCID) 1/21, entitled "Physical Security Standards for Sensitive Compartmented Information Facilities (SCIFs)," requires that all SCI be stored, processed, or discussed within an accredited SCIF. Accreditation is the formal affirmation that the proposed facility meets applicable physical security standards as set forth in DCID 1/21. The accreditation for a SCIF must be obtained in writing from the Security Programs Manager, FBIHQ. For further information regarding the handling of SCI, contact a representative of the

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 26 - 27

Security Countermeasures Section, National Security Division.

EFFECTIVE: 09/09/97

26-5.3 Removal of Classified Material to Residence

(1) Employees may not remove classified material from official premises to their residence during nonworking hours without approval from the Director, the FBIHQ Security Programs Manager (SPM), the SAC for FBI field offices, or the appropriate Assistant Director at FBIHQ. In every instance of approval, the material removed must remain in the personal control of the authorized employee at all times unless a safe and an alarm are installed in the residence by the FBI. Before installing any such equipment in a residence, the SPM at FBIHQ should be contacted for guidance.

(2) Control files are to be established, both at FBIHQ and in the field offices, to document those requests to remove classified material to an employee's residence. The file will include the date and duration of the request, the justification, signature approval granting or denying the request, the name of the authorized individual, and a description of the classified material being charged out.

(3) This authority does not apply to Legats.

EFFECTIVE: 07/23/90

26-5.4 Proper Use and Changing of Lock Combinations and Disposal of Combination Locks/Security Equipment (see also Part II, Section 16-7.2.6(9) of this manual)

(1) Except as otherwise noted, it shall be the responsibility of the supervisory or management official using or overseeing the use of security equipment that appropriate administrative controls are in place to ensure compliance with all requirements set forth herein.

b2

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 26 - 28

b2

(4) Records of combinations must be classified no lower than the highest category of classified material stored in the involved security equipment and must be protected in accordance with established guidelines addressing the handling and storage of NSI.

(a) A central Combination Record File is to be established in each division, Legat, regional computer center, or other off-site Bureau component, and combinations for all security containers used to store classified material are to be maintained in this file. This file is to be securely maintained in a fashion commensurate with the highest classification level of any document in the file.

(b) Standard Form (SF) 700, entitled "Security Container Information," is to be completed each time a combination is changed. This is a three-part, self-explanatory form. Upon completion, Part 1 is to be affixed to the inside of the affected vault, safe, door, or security container. Part 2A is to be completed and sealed inside Part 2, an envelope designed for this purpose, which in turn, is to be maintained in the central Combination Record File.

(c) It shall be the responsibility of the individual Legats and Security Officers to ensure all combination records for all equipment used to store classified material are properly classified and maintained.

(d) Written records of combinations must be maintained only as described herein. They are not to be retained in either "coded" or "uncoded" form on the person of any employee or other individual having access to the affected security equipment, nor are they to be recorded in any form on index cards, calendars,

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 26 - 29

notebooks, etc., which are not being maintained in compliance with established guidelines set forth herein for the protection of NSI.

b2 (5) Combinations shall be changed only by persons having the appropriate security clearance and/or special access, if applicable, for the type of classified material stored in the security container. The same shall apply to the Security Officer (SO), Alternate Security Officer (ASO), or any other individual designated to accompany this person. Clearances/special accesses may be verified by SOs or other designated individuals through the office of the Security Programs Manager, FBIHQ, Extension [REDACTED]

(a) In field offices, resident agencies, and off site locations associated with a field office, all combination changes are to be made by a Technically Trained Agent (TTA) and under the general direction of the field office SO or ASO. A responsible employee designated by the SAC or ASAC and familiar with security requirements governing the protection of NSI should also be present when the combination is changed.

(b) In Legats, all combination changes are to be made by the Legat, Assistant Legat, or other office personnel certified by the Engineering Section (ES), Technical Services Division (TSD). A responsible employee designated by the Legat or Assistant Legat and familiar with the security requirements governing the protection of NSI should also be present when the combination is changed.

(c) In regional computer centers or other FBI components not specifically associated with a field or FBIHQ division, all combination changes are to be made by the SO, ASO, or other personnel certified by ES, TSD. A responsible employee designated by the administrator of that component or his/her senior assistant and familiar with the security requirements governing the protection of NSI should also be present when the combination is changed.

(d) For all FBIHQ divisions, all combination changes are to be made by technically trained Bureau personnel certified by ES, TSD, and under the general direction of the division SO or ASO. A responsible division employee designated by no less than at the Unit Chief level and familiar with security requirements governing the protection of NSI should also be present when the combination is changed.

(e) The same combination will not intentionally be used for more than one lock in any field or FBIHQ division, Legat,

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 26 - 30

regional computer center, or other off-site location. In selecting combination numbers, multiples of five, simple ascending or descending arithmetical series, personal data (such as birthdates), and serial numbers, must be avoided. Only numbers that are widely separated may be used. The last number of a built-in combination lock shall not be set between 90 and 20. To prevent a lockout, a new combination is to be tried at least three consecutive times before closing the door or drawer.

(f) When security equipment is taken out of service, it shall be inspected to ensure no classified information or other FBI data remains, and the built-in combination lock shall be reset to the standard combination 50-25-50. Combination padlocks shall be reset to the standard combination 10-20-30.

(6) To properly secure a combination lock, the dial must be turned four or more complete revolutions in the same direction. Spinning the dial quickly is to be avoided as it shortens the life span of the tumblers/wheels, may cause other damage to the lock, and may not properly secure the lock. Combination locks are not to be left in an unsecured condition and the combination numbers are not to be left predialed to facilitate easy opening after an absence, as such a practice defeats the security protection of a combination-locked repository.

EFFECTIVE: 07/23/90

26-6 CONTROL FORM FOR TOP SECRET (TS) - SENSITIVE COMPARTMENTED INFORMATION (SCI) - NON-SCI CODE WORD MATERIAL - FD-501 - FD-502

Accountability, receipting and control of "Top Secret," Sensitive Compartmented Information (SCI), and Non-SCI Code Word Material within a field office or within FBIHQ is controlled through the use of the FBI "Control Form for Top Secret (TS), Sensitive Compartmented Information (SCI), and Non-SCI Code Word Material," FD-501. An original of an FD-501 will be attached to each copy of the material and the copy of FD-501 will be retained by the Security Officer to ensure he/she is aware of the location of the material at all times. "Top Secret" and/or Sensitive Compartmented Information being transmitted between field offices and/or FBIHQ or to outside agencies is controlled through the use of the "Receipt for Top Secret (TS) - Sensitive Compartmented Information (SCI), and Non-SCI Code Word Material," FD-502, which is attached to the material while being

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 26 - 31

transmitted. The recipient of the material will sign and return the original FD-502 to FBIHQ, Room 5991, or the Security Officer of the transmitting field office.

EFFECTIVE: 01/18/91

26-7 TRANSMITTAL OF CLASSIFIED MATERIAL

EFFECTIVE: 01/18/91

26-7.1 Within Field Offices

Material classified "Top Secret" or containing Sensitive Compartmented Information must be hand carried in an envelope within field offices. Material classified "Secret" or "Confidential" may be routed by messenger within field offices but must be in a messenger envelope except when records processing procedures such as indexing, serializing, filing, etc., are handled by OSM personnel within a field office.

EFFECTIVE: 01/18/91

26-7.2 Between Field Offices and/or Resident Agencies, Outside Agencies and FBIHQ (See MIOG, Part II, 35-9.4.14; MAOP, Part II, 2-2.2.2(1)(d); Correspondence Guide-FBIHQ, 1-4.5(4); Correspondence Guide-Field, 1-21.5(2); and National Foreign Intelligence Program Manual, Part I, 8-7.2.)

Material classified "Top Secret" or containing Sensitive Compartmented Information may only be transmitted between field offices and/or resident agencies, outside agencies and FBIHQ by secure teletype, by FBI courier designated by the SAC or Security Programs Manager or by Defense Courier Service (DCS). (See Part II, 26-6 above for use of control forms.) Material classified "Secret" or "Confidential" must be enclosed in opaque sealed envelopes or in opaque sealed boxes and may be transmitted by United States Postal Service (USPS) Registered Return Receipt, USPS Express Mail, or Federal Express (FedEx) between FBI offices within the United States and Puerto Rico. FedEx does not deliver to post office boxes. To

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 26 - 32

ensure direct delivery to the addressee, the "Waiver of Signature and Indemnity" block on the USPS Express Mail Label, 11-B, and the "Release Signature" block on the FedEx Airbill Label may NOT be executed under any circumstances. All "Confidential" and "Secret" express mail shipments should be prepared by FBI employees and hand-delivered directly to a FedEx representative or a USPS facility representative. The use of collection boxes is prohibited. For marking of transmittal documents, refer to 26-2.6.2 above.

EFFECTIVE: 06/06/96

26-7.3 Defense Courier Service (DCS); FBI Courier

"Top Secret" or Sensitive Compartmented Information which cannot be sent by secure teletype between field offices and/or FBIHQ must be transmitted by DCS or an FBI courier designated by the SAC or Security Programs Manager. "Top Secret" or Sensitive Compartmented Information transmitted between field offices and resident agencies or to outside agencies within the field office territory must be transmitted by an FBI employee designated as a courier by the SAC.

EFFECTIVE: 01/18/91

26-7.4 Wrapping Classified Material

"Top Secret" or Sensitive Compartmented Information transmitted by DCS must be wrapped in accordance with packing standards set forth in Appendix C, DCS Administrations and Operations Regulations. "Top Secret" or Sensitive Compartmented Information transmitted by FBI employees designated couriers by the SAC and "Secret" and "Confidential" material sent by registered mail must be enclosed in opaque sealed envelopes where size permits or in opaque sealed boxes in accordance with instructions set forth in Title 28, Code of Federal Regulations, Part 17.104.

EFFECTIVE: 07/23/90

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 26 - 33

26-8 MATERIAL CLASSIFIED UNDER PRIOR ORDERS

When incorporating information classified under previous Executive orders into a new document and no specific declassification date was indicated thereon, or if it was marked "indefinite," then a date for declassification must be shown or "OADR" (Originating Agency's Determination Required).

EFFECTIVE: 07/23/90

26-9 ATOMIC ENERGY MATERIAL MARKINGS

Additional warning markings "Restricted Data" and "Formerly Restricted Data" are used in connection with atomic energy-type material. These markings must be included on the first page when such classified material is set forth in FBI-originated documents.

EFFECTIVE: 07/23/90

26-10 SENSITIVE COMPARTMENTED INFORMATION (SCI)

EFFECTIVE: 07/23/90

26-10.1 Definition of SCI

(1) SCI access is regulated by the Director of Central Intelligence Directive (DCID) No. 1/14. SCI is all information and material requiring special U.S. Intelligence Community controls indicating restricted handling within present and future Community intelligence collection programs and their end products. These special Community controls are formal systems of restricted access established to protect the sensitive aspects of foreign intelligence programs. DCID No. 1/14 establishes minimum personnel security standards and procedures which govern eligibility for access to SCI.

(2) SCI security control systems depend upon distinctive markings and restricted handling of material, stricter personnel security processing for access, and holding SCI material in "Control Centers" with physical and procedural barriers to preclude access by

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 26 - 34

those who have not been formally approved. The SCI control systems provide an organized program for predetermining a generalized "need-to-know" regarding specific categories of intelligence and/or the sources and methods employed in their collection.

(3) SCI systems cover activities and information of extraordinary sensitivity and fragility from a security standpoint. They serve to restrict access to the protected information to persons who have a clearly established "need-to-know." "Need-to-know" exists only when access to SCI is essential to a person for the performance of official duties. Personnel granted access to SCI must meet rigorous and stringent personnel security criteria. Individuals cleared for Top Secret information are not automatically eligible for access to SCI.

EFFECTIVE: 07/23/90

26-10.2 SCI Access | (See MIOG, Part II, 35-9.2.) |

(1) Persons indoctrinated for SCI accept certain responsibilities and restrictions in a most explicit way. As a condition of access, an individual signs a nondisclosure agreement which is a contractual agreement between the government and the individual. This agreement should be read carefully before signing, because it states obligations imposed upon the individual and the government. Willful disclosure of SCI to unauthorized individuals constitutes criminal or administrative offenses which may result in prosecution or administrative action.

(2) Access to SCI will be granted when the "need-to-know" is established, eligibility determined, SCI nondisclosure agreement (Form 4414) signed, and indoctrination completed.

EFFECTIVE: 04/10/96

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 26 - 35

26-10.2.1 FBIHQ/Field Office/Legat Personnel Security Access
Certification Procedures

DCID No. 1/14 sets forth the minimum personnel security standards and procedures governing eligibility for access to SCI. The purpose of this Directive is to enhance the security protection of SCI through the application of minimum security standards, procedures, and continuing security programs, and to facilitate the security certification process among government departments and agencies.

Accordingly, the following procedures will be followed by FBI Headquarters (FBIHQ) and field divisions when access to SCI is required:

(1) A written communication requesting SCI access shall be directed to the National Security Division, Attention: Security Programs Manager (SPM). The communication should utilize the employee's 67 file number. The communication shall be captioned as follows:

"ACCESS TO SCI, _____ DIVISION."

The following information shall be included for each individual for whom access is being requested:

- A. Bureau name
- B. Position
- C. Social Security Account Number
- D. Supervisor's written certification of employee's "need-to-know"
- E. SCI access or accesses requested

(2) The division Security Officer will be advised in writing of access approval. The written communication will authorize the Security Officer to conduct a formal briefing and security indoctrination in accordance with the minimum requirements set forth in "Annex C," DCID No. 1/14, page 2.

(3) Form 4414, "Sensitive Compartmented Information Nondisclosure Agreement," should be executed prior to the formal briefing and, thereafter, forwarded to the SPM.

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 26 - 36

In emergency cases where immediate access is required, the division Security Officer may, by secure telephone, provide the aforementioned information to the Supervisory Special Agent managing the SCI Program for the SPM, followed by a routine teletype confirming that information. FBIHQ will expedite access approval by secure telephone. If an exception to the investigative requirements is granted to facilitate an immediate interim access, the prescribed investigation shall, nevertheless, go forward.

For TURK purposes, these matters will be handled under the 67E classification, "Reinvestigation of FBI Personnel."

EFFECTIVE: 04/10/96

| 26-10.2.2 | Deleted |

EFFECTIVE: 04/10/96

26-10.2.3 Denial/Revocation

A denial or revocation of access to SCI shall be in accordance with procedures established in "Annex B" to DCID No. 1/14, which is titled "Appeals." For purposes of denial or revocation, the determination authority for the FBI shall be the SPM. The final appeal authority remains with the Director of the FBI or his designated representative at the Associate Deputy Director level.

EFFECTIVE: 12/10/91

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 26 - 37

26-10.2.4 Termination/Debriefing

SCI access must be terminated when an employee no longer has a "need-to-know." This can be occasioned by position transfer, retirement, resignation, suspension, maternity leave, etc. At this time, the Security Officer will debrief the employee in accordance with the guidelines provided in "Annex C," DCID No. 1/14.

EFFECTIVE: 12/10/91

26-10.2.5 Exceptions to DCID No. 1/14

Exceptions to the minimum standards as set forth in DCID No. 1/14 may be granted only by the Senior Official of the Intelligence Community (SOIC). For the purposes of DCID No. 1/14, an SOIC is defined as a head of an organization within the Intelligence Community, as defined by Executive Order (EO) 12333, or their designated representative. EO 12333 defines the intelligence activities of the United States and specifically states the intelligence element of the FBI is part of the Intelligence Community. The SOIC for the FBI is the Director, who specifically delegated the responsibility for the administration of SCI policy and procedures for the FBI to the SPM.

EFFECTIVE: 12/10/91

26-10.2.6 Access to Sensitive Compartmented Information (SCI)
Recertification Procedures, Reinvestigation of FBI
Personnel (See MIOG, Part I, 67-18(1)(e).)

The SCI access mandatory recertification process is to be conducted annually by each Security Countermeasures Programs Manager (SCMPM) or his/her designee.

(1) The Security Programs Manager (SPM), FBIHQ, will forward to each field office and FBIHQ division/office a list of designated employees with SCI access on or about May 1 of each calendar year.

(2) The list will contain each employee's name, social security number, SCI access, briefing date, debriefing date, and

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 26 - 38

comment section.

(3) Each SCMPM will review, verify, and certify the identifiable information pertaining to each employee.

(a) When a determination is made to continue with the SCI access, the SCMPM is required to provide a succinct statement justifying the continuation of the SCI access.

(b) In those instances when the SCI access continuance cannot be fully justified, then steps must be initiated to debrief the employee immediately.

(c) When an employee is debriefed, a blank copy each of Form 4414, entitled "Sensitive Compartmented Information Nondisclosure Agreement," and SF-312, entitled "Classified Information Nondisclosure Agreement," is to be given to each debriefed employee. Both forms are to serve as a reminder of the consequences and statutory requirements for protecting national security information.

(4) The SCMPM is required to maintain a copy of the SCI access recertification list from year to year.

(a) Upon receipt of the current year's list of employees, the previous year's list is to be destroyed.

(b) The list of employees is to be maintained in accordance with established procedures for handling and storing Sensitive Compartmented Information.

(5) The recertification list, with appropriate comments and debriefing form (Form 4414), should be returned to the SPM within 60 calendar days from the date of the SPM's cover communication.

(6) The SCMPM or his/her designee is to ensure those employees whose SCI access is no longer required are debriefed routinely.

(7) Whenever an employee's conduct is no longer commensurate with DCID Number 1/14, Executive Order 10450, and/or the employee's misconduct impacts on his/her trustworthiness, the SCMPM is required to conduct a personnel security interview with the employee and notify the SPM, FBIHQ, providing a recommendation as to whether the employee's SCI access should be suspended, denied, or revoked pending the SPM's final adjudicative decision.

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 26 - 39

EFFECTIVE: 10/12/93

26-11 CERTIFICATION OF CLEARANCES

EFFECTIVE: 12/10/91

26-11.1 Visits to Other Agencies by Current Employees

(1) The Security/Clearances/Unit, FBIHQ will pass/certify all clearances for FBIHQ personnel when required for visits to other agencies. Upon request from the field Security Officer, the Security/Clearances/Unit will also pass/certify clearances for field office personnel when required for visits to other agencies. All requests should include: The level of clearance needed at the meeting; point-of-contact and telephone number; date(s) of visit; and reason for visit. Field Security Officers have the authority to pass/certify employee's security clearances in that field office to other agencies. Frequently, however, many other Government agencies and private sector organizations will not accept security clearances unless they are passed/certified by the Security/Clearances/Unit.

(2) To enable the Intelligence Community to function in a prompt and efficient manner, the Director of Central Intelligence, who has the responsibility for controlling the Sensitive Compartmented Information (SCI) Program, has authorized the passing of specific SCI accesses over unsecured telephones.

SCI digraphs and trigraphs (e.g., SI, TK, etc.) are unclassified, as is their use in connection with an individual whose relationship with the U.S. Government is unclassified and does not warrant classification. SCI access levels (e.g., Signals Intelligence, Talent Keyhole, etc.) in and of themselves are unclassified; however, these access levels become classified when used in conjunction with other information, including the identity of the individual who holds the access level.

EFFECTIVE: 12/10/91

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 26 - 40

26-11.2 Converting FBI Clearances to Clearances for New Employer

(1) When current or former FBI employees apply for positions with other Federal Government agencies or with private industry which require security clearances, inquiries concerning their FBI security clearances should be directed to the Security Clearances Unit (SCU), Security Countermeasures Section, Intelligence Division. SCU personnel should request that all such inquiries be made in writing, to allow for a proper review of the employee's personnel file, and any other file that would be pertinent to the request, such as an Administrative Inquiry Matter.

(2) Executive Order (EO) 10450, "Security Requirements for Government Employment," mandates, in Section 3(a), that Government agencies must, at a minimum, make written inquiry to former employers, among other things, when seeking to hire an individual. Section 8 of this Order specifically details the type of information these written inquiries are designed to obtain, all of which is aimed toward determining the individual's suitability for Federal employment.

(3) DOJ Order 2600.3A, "Requirements for Safeguarding Classified Information and Materials Released to Industry in Connection With Contracts or Grants," and the Department of Defense (DOD) Industrial Security Manual (Section III, paragraph 27), both of which govern the FBI's relationship with private industry, require a similar written inquiry to former employers, as specified above, when attempting to convert a former Government clearance.

(4) In order for the FBI, as a current or former employer, to conform to the requirements in EO 10450, DOJ Order 2600.3A, and DOD Industrial Security Manual, SCU personnel will review all pertinent files concerning the employee, specifically to include personnel and Administrative Inquiry files, and furnish the requester any information deemed pertinent (to include derogatory information) to assist in the proper adjudication of the clearance matter.

EFFECTIVE: 02/12/92

26-12 SPECIAL CONTROL MARKINGS FOR SENSITIVE INTELLIGENCE
SOURCES AND METHODS AND FOR FOREIGN INTELLIGENCE MATERIAL

Sensitive
PRINTED: 02/18/98

Sensitive

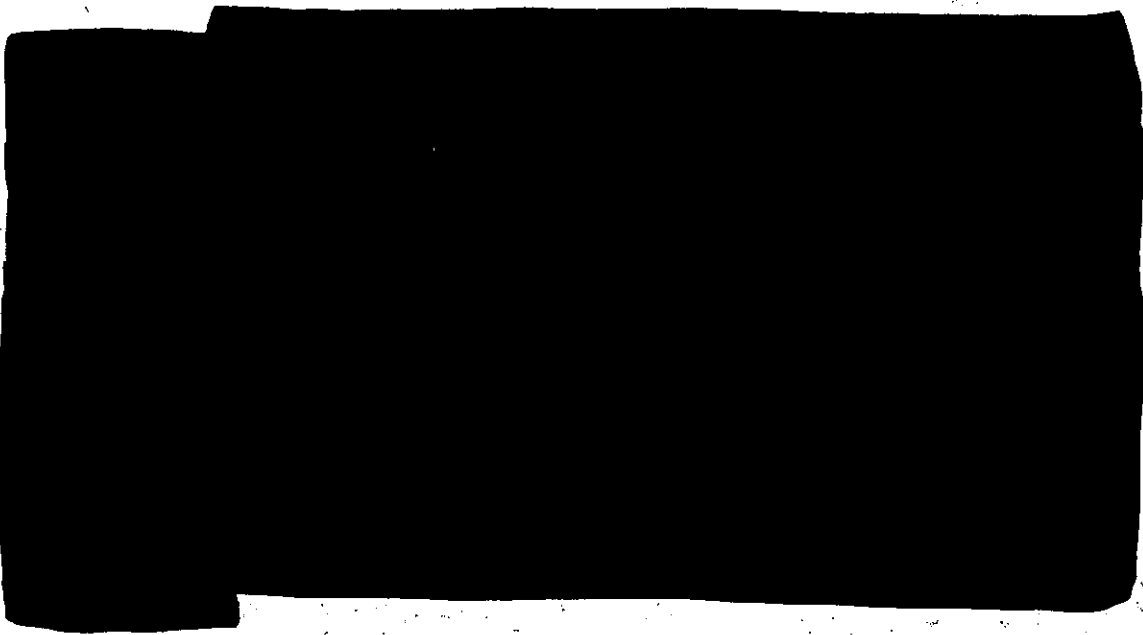
Manual of Investigative Operations and Guidelines
Part II

PAGE 26 - 41

EFFECTIVE: 02/12/92

26-12.1 Warning Notice - Sensitive Intelligence Sources and
Methods Involved (WNINTEL)

(1) In addition to instructions relating to dissemination of classified material set forth in the National Security Council Directive of May 17, 1972 (classified information or material originated in one department shall not be disseminated outside any other department to which it has been made available without the consent of the originating department - known as the "third agency rule"), the Directive also requires that all information and material relating to sensitive intelligence sources and methods be prominently marked "WARNING NOTICE-SENSITIVE INTELLIGENCE SOURCES AND METHODS INVOLVED" (WNINTEL). The Directive instructs that material so marked may not be disseminated in any manner outside authorized channels without permission of the originating department and an assessment by the senior intelligence officer in the disseminating department of the potential risk to the national security and to the intelligence sources and methods involved.



b2

(3) For FBI purposes, the marking "WNINTEL" will be utilized only in connection with Sensitive Compartmented Information (SCI) or uniquely sensitive information.

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 26 - 42

EFFECTIVE: 02/12/92

26-12.2 Foreign Intelligence Material

In addition to level of classification markings ("Top Secret," "Secret," and "Confidential") and WNINTEL markings, the following additional markings may be used on foreign intelligence when, in the opinion of the originating organization, extraordinary circumstances require further restrictions on dissemination of foreign intelligence:

(1) DISSEMINATION AND EXTRACTION OF INFORMATION CONTROLLED BY ORIGINATOR (ORCON) - May not be disseminated outside of the Headquarters of the receiving agency in any form, even extracted or paraphrased, without permission of originator.

(2) NFIB DEPARTMENTS ONLY (NFIBONLY) - May not be disseminated to an organization not represented on the National Foreign Intelligence Board without permission of the originator.

(3) NOT RELEASABLE TO CONTRACTORS OR CONTRACTOR/CONSULTANTS (NOCONTRACT) - May not be disseminated to contractors or contractor-consultants without permission of originator.

(4) CAUTION - PROPRIETARY INFORMATION INVOLVED (PROPIN) - Recipients shall take every precaution to ensure the information is not used to the detriment of the source.

(5) NOT RELEASABLE TO FOREIGN NATIONALS (NOFORN) - May not be released in any form to foreign governments, foreign nationals or non-U.S. citizens without permission of the originator.

EFFECTIVE: 02/12/92

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 26 - 43

26-13. UNAUTHORIZED DISCLOSURE OF CLASSIFIED INFORMATION

Department of Justice and FBI regulations provide for disciplinary action for employees who violate provisions of Executive Order 12356 and stringent administrative action may be taken against any employee determined to have been knowingly responsible for unauthorized disclosure of classified national security material. Whenever a violation of criminal statutes may be involved, prosecution may also be instituted. (See MIOG, Part II, Section 26-4.1.) The National Foreign Intelligence Program Manual (NFIPM), Appendix, 4-1.1, states in part that anyone who willfully delivers or, through gross negligence, loses any defense information is liable to \$10,000 fine or imprisonment for not more than ten years, or both.

EFFECTIVE: 02/14/97

26-13.1 Loss or Possible Compromise of Classified Information (See MIOG, Part I, 261-2(3)(b), II, 26-13.2, 26-13.3 (4); MAOP, Part II, 2-4.3.8(1)(a), 6-7.5(2)(h).3; FCIM, Part I, 65-8.)

Any person who has knowledge of the loss or possible compromise of classified information shall immediately report the circumstances to FBIHQ, Attention: Security Programs Manager (SPM), and the field office Security Countermeasures Program Manager. When appropriate, the SPM will coordinate with the relevant substantive FCI entities within the National Security Division to ensure compliance with the instructions set forth in the FCIM, Part I, Section 65, "Espionage," Section 65-3, "FBIHQ Policy." In addition, the SPM will notify the agency that originated the information of the loss or possible compromise so that a damage assessment may be conducted and appropriate measures taken to negate or minimize any adverse effect of the compromise pursuant to guidelines set forth in Title 32, Code of Federal Regulations (CFR), Part 2001, Section 2001.47, as follows:

"(a) Initiation of Damage Assessments. An agency head shall initiate a damage assessment whenever there has been a compromise of classified information originated by that agency that, in his or her judgment, can reasonably be expected to cause damage to the national security. Compromises may occur through espionage,

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 26 - 44

unauthorized disclosures to the press or other members of the public, unauthorized sales, publication of books and treatises, the known loss of classified information or equipment to foreign powers, or through various other circumstances.

"(b) Content of Damage Assessments. At a minimum, damage assessments shall be in writing and contain the following:

"(1) Identification of the source, date, and circumstances of the compromise.

"(2) Classification of the specific information lost.

"(3) A description of the specific information lost.

"(4) An analysis and statement of the known or probable damage to the national security that has resulted or may result.

"(5) An assessment of the possible advantage to foreign powers resulting from the compromise.

"(6) An assessment of whether (i) the classification of the information involved should be continued without change; (ii) the specific information, or parts thereof, shall be modified to minimize or nullify the effects of the reported compromise and the classification retained; (iii) downgrading, declassification, or upgrading is warranted, and if so, confirmation of prompt notification to holders of any change.

"(7) An assessment of whether countermeasures are appropriate and feasible to negate or minimize the effect of the compromise.

"(8) An assessment of other appropriate corrective, administrative, disciplinary or legal actions.

"(c) System of Control of Damage Assessments. Each agency shall establish a system of control and internal procedures to ensure that damage assessments are performed in all cases described in paragraph (a), and that records are maintained in a manner that facilitates their retrieval and use within the agency.

"(d) Cases Involving More Than One Agency.

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 26 - 45

"(1) Whenever a compromise involves the classified information or interests of more than one agency, each department or agency undertaking a damage assessment shall advise other agencies of the circumstances and findings that affect their information or interests. Whenever a damage assessment, incorporating the product of two or more agencies is needed, the affected agencies shall agree upon the assignment of responsibility for the assessment.

"(2) Whenever a compromise occurs within an agency that is not responsible for the damage assessment, that agency shall provide all data pertinent to the compromise to the agency responsible for conducting the assessment.

"(3) Whenever a compromise of U.S. classified information is the result of actions taken by foreign nationals, by foreign government officials, or by U.S. nationals in the employ of international organizations, the agency performing the damage assessment shall ensure through appropriate intergovernmental liaison channels, that information pertinent to the assessment is obtained. Whenever more than one agency is responsible for the assessment, those agencies shall coordinate the request prior to transmittal through appropriate channels.

"(4) Whenever an action is contemplated against any person believed responsible for the compromise of classified information, damage assessments shall be coordinated with appropriate agency legal counsel. Whenever a violation of criminal law appears to have occurred and a criminal prosecution is contemplated, the agency responsible for the damage assessment shall coordinate with the Department of Justice.

"(5) The designated representative of the Director of Central Intelligence, or other appropriate officials with responsibility for the information involved, will be consulted whenever a compromise of Sensitive Compartmented Information (SCI) has occurred."

EFFECTIVE: 03/15/94

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 26 - 46

26-13.2 Damage Assessment of Missing Files and Serials

A damage assessment must be conducted in accordance with MIOG, Part II, Section 26-13.1 for any classified file or serial missing for 30 days or more. This damage assessment must be reported as outlined in the Manual of Administrative Operations and Procedures, Part II, Section 2-4.3.8(1).

EFFECTIVE: 08/27/90

26-13.3 Cases Involving Loss or Unauthorized Disclosure of Sensitive Compartmented Information (SCI)

(1) The Director of Central Intelligence Directive (DCID) No. 1/19 sets forth the security policy for SCI. Compliance with this policy is mandatory for all Intelligence Community agencies that operate SCI programs.

(2) DCID No. 1/19 refers to the Senior Official of the Intelligence Community (SOIC) or his/her designee as the person responsible for ensuring DCID requirements are met. The SOIC has the responsibility for the granting, denial, and revocation of access to SCI.

(3) The Director, FBI, as the SOIC for the FBI, has delegated the authority to protect SCI to the Security Programs Manager (SPM), who is responsible for ensuring compliance with DCID requirements.

(4) Whenever there is a suspicion that there has been a serious compromise or unauthorized disclosure of SCI, an investigation will be conducted to determine if there is a reasonable likelihood that a compromise of SCI may have occurred, the identity of the person(s) responsible for the unauthorized disclosure, and the need for remedial procedures to preclude a recurrence. (See also 26-13.1.)

(5) If a compromise is determined to have occurred, the SPM will report the incident to the designated representative of the DCI. An investigation is to be conducted to identify full details of the violation/compromise, and to determine what specific information was involved, what damage resulted, and whether culpability was involved in the incident.

(6) If a case involves an inadvertent disclosure, the SPM

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 26 - 47

will exercise his/her judgment as to whether the interests of SCI security are served by seeking written agreements from unindoctrinated persons to whom SCI has been inadvertently disclosed. If the judgment is that those interests are so served, the person(s) involved signs the Inadvertent Disclosure Statement FD-722 (see 26-4.1), and the SPM has reason to believe that the person(s) will maintain absolute secrecy concerning the SCI involved, the report of investigation may conclude that no compromise occurred.

(7) Summaries of investigations and of related actions shall be provided to the DCI through the DCI's Unauthorized Disclosures Analysis Center by the SPM:

(a) when investigations show that the SCI was inadvertently disclosed to foreign nationals or deliberately disclosed to unauthorized persons; or

(b) when cases under investigation involve damage deemed significant by the SPM--espionage, flagrant dereliction of security duties, or serious inadequacy of security policies or procedures.

(8) The SPM will ensure that corrective action is taken in all cases of actual security violations and compromises.

EFFECTIVE: 08/27/90

26-14 CLEARANCES OF PERSONNEL HANDLING SENSITIVE COMPARTMENTED
INFORMATION (SCI) MATERIAL

(1) All FBI employees requiring access to SCI material must be cleared prior to being granted access to that level of material. This includes couriers and individuals who type or otherwise process SCI material.

(2) All teletype operators, including alternates, must be cleared for access to "SI" material in order to facilitate round-the-clock transmission of "SI" information.

EFFECTIVE: 08/27/90

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 26 - 48

26-15 DESTRUCTION OF CLASSIFIED MATERIAL (See MIOG, Part II,
35-9.4.14.)

(1) When no longer needed, classified material shall be destroyed as soon as practicable by shredding, burning, pulverizing, pulping, melting, chemical decomposition, or other mutilation method sufficient to preclude any recognition or reconstruction of the information. (See MAOP, Part II, 2-1.3.)

(2) The destruction of Top Secret and Sensitive Compartmented Information (SCI) must be witnessed and recorded by two employees with security clearances commensurate with the classification of the material being destroyed. This information is to be recorded on the FD-501 and shall include the names of the employees, the reason for destruction, and the date, location and method of destruction.

EFFECTIVE: 07/26/95

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 27 - 1

SECTION 27. WITNESS SECURITY PROGRAM (WSP)

27-1

INTRODUCTION

[REDACTED]

b2
b7E
[REDACTED]

[REDACTED]

[REDACTED]

EFFECTIVE: 10/25/89

Sensitive
PRINTED: 02/18/98

XXXXXX
XXXXXX
XXXXXXFEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

30

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 552Section 552a☐ (b)(1)☐ (b)(7)(A)☐ (d)(5)☒ (b)(2)☐ (b)(7)(B)☐ (j)(2)☐ (b)(3)☐ (b)(7)(C)☐ (k)(1)☐ (b)(7)(D)☐ (k)(2)☒ (b)(7)(E)☐ (k)(3)☐ (b)(7)(F)☐ (k)(4)☐ (b)(4)☐ (b)(8)☐ (k)(5)☐ (b)(5)☐ (b)(9)☐ (k)(6)☐ (b)(6)☐ (k)(7)

- ☐ Information pertained only to a third party with no reference to the subject of your request or the subject of your request is listed in the title only.
- ☐ Documents originated with another Government agency(ies). These documents were referred to that agency(ies) for review and direct response to you.

Pages contain information furnished by another Government agency(ies). You will be advised by the FBI as to the releasability of this information following our consultation with the other agency(ies).

Page(s) withheld inasmuch as a final release determination has not been made. You will be advised as to the disposition at a later date.

Pages were not considered for release as they are duplicative of _____

Page(s) withheld for the following reason(s): _____

- ☒ The following number is to be used for reference regarding these pages:

MIOG Pt II Sec 27 p2-31

XXXXXXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X for this page X
XXXXXXXXXXXXXXXXXXXX

XXXXXX
XXXXXX
XXXXXX

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 27 - 32

EFFECTIVE: 05/13/96

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 28 - 1

SECTION 28. SEARCH AND SEIZURE OF DOCUMENTARY MATERIALS

28-1 ATTORNEY GENERAL'S GUIDELINES ON METHODS OF OBTAINING
DOCUMENTARY MATERIALS HELD BY THIRD PARTIES

Pursuant to Title II, Privacy Protection Act of 1980 (Pub. L. 96-440, Sec. 201 et seq.; 42 U.S.C. 2000aa-11, et seq.), the Attorney General has issued the following guidelines in connection with the obtaining by Federal officers of documentary evidence in possession of third parties:

"Section 59.1 Introduction.

"(a) A search for documentary materials necessarily involves intrusions into personal privacy. First, the privacy of a person's home or office may be breached. Second, the execution of such a search may require examination of private papers within the scope of the search warrant, but not themselves subject to seizure. In addition, where such a search involves intrusions into professional, confidential relationships, the privacy interests of other persons are also implicated.

"(b) It is the responsibility of federal officers and employees to recognize the importance of these personal privacy interests, and to protect against unnecessary intrusions. Generally, when documentary materials are held by a disinterested third party, a subpoena, administrative summons, or governmental request will be an effective alternative to the use of a search warrant and will be considerably less intrusive. The purpose of the guidelines set forth in this part is to assure that federal officers and employees do not use search and seizure to obtain documentary materials in the possession of disinterested third parties unless reliance on alternative means would substantially jeopardize their availability (e.g., by creating a risk of destruction, etc.) or usefulness (e.g., by detrimentally delaying the investigation, destroying a chain of custody, etc.). Therefore, the guidelines in this part establish certain criteria and procedural requirements which must be met before a search warrant may be used to obtain documentary materials held by disinterested third parties. The guidelines in this part are not intended to inhibit the use of less intrusive means of obtaining documentary materials such as the use of a subpoena, summons, or formal or informal request.

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 28 - 2

"Section 59.2 Definitions.

"As used in this part ---

"(a) The term 'attorney for the government' shall have the same meaning as is given that term in Rule 54(c) of the Federal Rules of Criminal Procedure;

"(b) The term 'disinterested third party' means a person or organization not reasonably believed to be ---

"(1) A suspect in the criminal offense to which the materials sought under these guidelines relate; or

"(2) Related by blood or marriage to such a suspect;

"(c) The term 'documentary materials' means any materials upon which information is recorded, and includes, but is not limited to, written or printed materials, photographs, films or negatives, audio or video tapes, or materials upon which information is electronically or magnetically recorded, but does not include materials which constitute contraband, the fruits or instrumentalities of a crime, or things otherwise criminally possessed;

"(d) The term 'law enforcement officer' shall have the same meaning as the term 'federal law enforcement officer' as defined in Rule 41(h) of the Federal Rules of Criminal Procedure; and

"(e) The term 'supervisory official of the Department of Justice' means the supervising attorney for the section, office, or branch within the Department of Justice which is responsible for the investigation or prosecution of the offense at issue, or any of his superiors.

"Section 59.3 Applicability.

"(a) The guidelines set forth in this part apply, pursuant to section 201 of the Privacy Protection Act of 1980 (Sec. 201, Pub. L. 96-440, 94 Stat. 1879, (42 U.S.C. 2000aa-11)), to the procedures used by any federal officer or employee, in connection with the investigation or prosecution of a criminal offense, to obtain documentary materials in the private possession of a disinterested third party.

"(b) The guidelines set forth in this part do not apply to:

"(1) Audits, examinations, or regulatory, compliance,

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 28 - 3

or administrative inspections or searches pursuant to federal statute or the terms of a federal contract;

"(2) The conduct of foreign intelligence or counterintelligence activities by a government authority pursuant to otherwise applicable law;

"(3) The conduct, pursuant to otherwise applicable law, of searches and seizures at the borders of, or at international points of entry into, the United States in order to enforce the customs laws of the United States;

"(4) Governmental access to documentary materials for which valid consent has been obtained; or

"(5) Methods of obtaining documentary materials whose location is known but which have been abandoned or which cannot be obtained through subpoena or request because they are in the possession of a person whose identity is unknown and cannot with reasonable effort be ascertained.

"(c) The use of search and seizure to obtain documentary materials which are believed to be possessed for the purpose of disseminating to the public a book, newspaper, broadcast, or other form of public communication is subject to Title I of the Privacy Protection Act of 1980 (Sec. 101, et seq., Pub. L. 96-440, 94 Stat. 1879 (42 U.S.C. 2000aa, et seq.)), which strictly prohibits the use of search and seizure to obtain such materials except under specified circumstances.

"(d) These guidelines are not intended to supersede any other statutory, regulatory, or policy limitations on access to, or the use or disclosure of particular types of documentary materials, including, but not limited to, the provisions of the Right to Financial Privacy Act of 1978 (12 U.S.C. 3401, et seq.), the Drug Abuse Office and Treatment Act of 1972, as amended (21 U.S.C. 1101, et seq.), and the Comprehensive Alcohol Abuse and Alcoholism Prevention, Treatment, and Rehabilitation Act of 1970, as amended (42 U.S.C. 4541, et seq.).

"Section 59.4 Procedures.

"(a) Provisions governing the use of search warrants generally.

"(1) A search warrant should not be used to obtain documentary materials believed to be in the private possession of a disinterested third party unless it appears that the use of a subpoena,

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 28 - 4

summons, request, or other less intrusive alternative means of obtaining the materials would substantially jeopardize the availability or usefulness of the materials sought, and the application for the warrant has been authorized as provided in paragraph (a) (2) of this section.

"(2) No federal officer or employee shall apply for a warrant to search for and seize documentary materials believed to be in the private possession of a disinterested third party unless the application for the warrant has been authorized by an attorney for the government. Provided, however, that in an emergency situation in which the immediacy of the need to seize the materials does not permit an opportunity to secure the authorization of an attorney for the government, the application may be authorized by a supervisory law enforcement officer in the applicant's department or agency, if the appropriate United States Attorney (or where the case is not being handled by a United States Attorney's Office, the appropriate supervisory official of the Department of Justice) is notified of the authorization and the basis for justifying such authorization under this part within 24 hours of the authorization.

"(b) Provisions governing the use of search warrants which may intrude upon professional, confidential relationships.

"(1) A search warrant should not be used to obtain documentary materials believed to be in the private possession of a disinterested third party physician, lawyer, or clergyman, under circumstances in which the materials sought, or other materials likely to be reviewed during the execution of the warrant, contain confidential information on patients, clients, or parishioners which was furnished or developed for the purposes of professional counseling or treatment, unless ---

"(i) It appears that the use of a subpoena, summons, request or other less intrusive alternative means of obtaining the materials would substantially jeopardize the availability or usefulness of the materials sought;

"(ii) Access to the documentary materials appears to be of substantial importance to the investigation or prosecution for which they are sought; and

"(iii) The application for the warrant has been approved as provided in paragraph (b) (2) of this section.

"(2) No federal officer or employee shall apply for a warrant to search for and seize documentary materials believed to be

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 28 - 5

in the private possession of a disinterested third party physician, lawyer, or clergyman under the circumstances described in paragraph (b)(1) of this section, unless, upon the recommendation of the United States Attorney (or where a case is not being handled by a United States Attorney's Office, upon the recommendation of the appropriate supervisory official of the Department of Justice), an appropriate Deputy Assistant Attorney General has authorized the application for the warrant. Provided, however, that in an emergency situation in which the immediacy of the need to seize the materials does not permit an opportunity to secure the authorization of a Deputy Assistant Attorney General, the application may be authorized by the United States Attorney (or where the case is not being handled by a United States Attorney's Office, by the appropriate supervisory official of the Department of Justice) if an appropriate Deputy Assistant Attorney General is notified of the authorization and the basis for justifying such authorization under this part within 72 hours of the authorization.

"(3) Whenever possible, a request for authorization by an appropriate Deputy Assistant Attorney General of a search warrant application pursuant to paragraph (b)(2) of this section shall be made in writing and shall include:

"(i) The application for the warrant; and

"(ii) A brief description of the facts and circumstances advanced as the basis for recommending authorization of the application under this part.

"If a request for authorization of the application is made orally or if, in an emergency situation, the application is authorized by the United States Attorney or a supervisory official of the Department of Justice as provided in paragraph (b)(2) of this section, a written record of the request including the materials specified in paragraphs (b)(3)(i) and (ii) of this section shall be transmitted to an appropriate Deputy Assistant Attorney General within 7 days. The Deputy Assistant Attorneys General shall keep a record of the disposition of all requests for authorizations of search warrant applications made under paragraph (b) of this section.

"(4) A search warrant authorized under paragraph (b)(2) of this section shall be executed in such a manner as to minimize, to the greatest extent practicable, scrutiny of confidential materials.

"(5) Although it is impossible to define the full range of additional doctor-like therapeutic relationships which involve the furnishing or development of private information, the United States

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 28 - 6

Attorney (or where a case is not being handled by a United States Attorney's Office, the appropriate supervisory official of the Department of Justice) should determine whether a search for documentary materials held by other disinterested third party professionals involved in such relationships (e.g., psychologists or psychiatric social workers or nurses) would implicate the special privacy concerns which are addressed in paragraph (b) of this section. If the United States Attorney (or other supervisory official of the Department of Justice) determines that such a search would require review of extremely confidential information furnished or developed for the purposes of professional counseling or treatment, the provisions of this subsection should be applied. Otherwise, at a minimum, the requirements of paragraph (a) of this section must be met.

"(c) Considerations bearing on choice of methods.

"In determining whether, as an alternative to the use of a search warrant, the use of a subpoena or other less intrusive means of obtaining documentary materials would substantially jeopardize the availability or usefulness of the materials sought, the following factors, among others, should be considered:

"(1) Whether it appears that the use of a subpoena or other alternative which gives advance notice of the government's interest in obtaining the materials would be likely to result in the destruction, alteration, concealment, or transfer of the materials sought; considerations, among others, bearing on this issue may include:

"(i) Whether a suspect has access to the materials sought;

"(ii) Whether there is a close relationship of friendship, loyalty, or sympathy between the possessor of the materials and a suspect;

"(iii) Whether the possessor of the materials is under the domination or control of a suspect;

"(iv) Whether the possessor of the materials has an interest in preventing the disclosure of the materials to the government;

"(v) Whether the possessor's willingness to comply with a subpoena or request by the government would be likely to subject him to intimidation or threats of reprisal;

"(vi) Whether the possessor of the materials has

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 28 - 7

previously acted to obstruct a criminal investigation or judicial proceeding or refused to comply with or acted in defiance of court orders; or

"(vii) Whether the possessor has expressed an intent to destroy, conceal, alter, or transfer the materials;

"(2) The immediacy of the government's need to obtain the materials; considerations, among others, bearing of this issue may include:

"(i) Whether the immediate seizure of the materials is necessary to prevent injury to persons or property;

"(ii) Whether the prompt seizure of the materials is necessary to preserve their evidentiary value;

"(iii) Whether delay in obtaining the materials would significantly jeopardize an ongoing investigation or prosecution; or

"(iv) Whether a legally enforceable form of process, other than a search warrant, is reasonably available as a means of obtaining the materials. The fact that the disinterested third party possessing the materials may have grounds to challenge a subpoena or other legal process is not in itself a legitimate basis for the use of a search warrant.

"Section 59.5 Functions and Authorities of the Deputy Assistant Attorneys General.

"The functions and authorities of the Deputy Assistant Attorneys General set out in this part may at any time be exercised by an Assistant Attorney General, the Associate Attorney General, the Deputy Attorney General, or the Attorney General.

"Section 59.6 Sanctions.

"(a) Any federal officer or employee violating the guidelines set forth in this part shall be subject to appropriate disciplinary action by the agency or department by which he is employed.

"(b) Pursuant to section 202 of the Privacy Protection Act of 1980 (Sec. 202, Pub. L. 96-440, 94 Stat. 1879 (42 U.S.C. 2000aa-12)), an issue relating to the compliance, or the failure to comply, with the guidelines set forth in this part may not be litigated, and a court may not entertain such an issue as the basis for the suppression or exclusion

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 28 - 8

of evidence."

EFFECTIVE: 02/23/84

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 29 - 1

SECTION 29. TERRORIST RESEARCH AND ANALYTICAL CENTER (TRAC)

29-1 DEFINITION

The TRAC is responsible for conducting research on terrorism, analyzing the data received, and making assessments of the potential terrorist threats to the United States.

EFFECTIVE: 02/23/84

29-2 SERVICES

- (1) To computerize data on all domestic and international terrorist groups which pose a threat to the United States.
- (2) To conduct research on terrorist groups, analyze data, and produce assessments of the potential dangers posed by those groups to the United States.
- (3) To record, maintain, analyze, and publish statistical information concerning terrorism and terrorist incidents in the United States and the accomplishments of the FBI's counterterrorism efforts.
- (4) To prepare the terrorism program budget submissions.
- (5) To maintain a terrorist reference library consisting of books, periodicals, newspapers, NEXIS (a computer assisted public information source), slides and audio video cassettes on various terrorist-related incidents, and a vertical file which contains indexed research material consisting of papers produced by TRAC personnel and papers which are primary and secondary sources of information in research as well as papers ephemeral in nature usually of temporary interest.
- (6) To administer a terrorism training program.

EFFECTIVE: 02/23/84

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 30 - 1

SECTION 30. |CRISIS MANAGEMENT PROGRAM|

30-1 |CRISIS MANAGEMENT PROGRAM| (See MIOG, Part I, 261-2(6),
NFIP Manual, Part I, 8-1.1.)|

(1) Crisis management is the process of identifying, acquiring, and planning the use of resources needed to anticipate, prevent, and/or resolve a crisis. The program, as it currently exists in the Bureau, encompasses two other major programs: crisis (hostage) negotiation and special weapons and tactics (SWAT). However, these are not the only resources involved in crisis management.

(2) The components (resources) that may be included on any crisis management team are:

- (a) Managerial
- (b) Negotiators
- (c) Tactical (SWAT/Hostage Rescue Team (HRT))
- (d) Technical
- (e) Investigative
- (f) Support
- (g) Special Operations Groups (SOG)
- (h) Legal
- (i) Media Representative

(3) Crisis management involves planning the use of these components and coordinating their actions at the crisis scene.

EFFECTIVE: 02/27/96

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 30 - 2

30-1.1 Objectives

- (1) To preserve life.
- (2) To enforce the laws over which the FBI has jurisdiction.

In keeping with these objectives, the guiding principle in negotiation/SWAT employment, as in all actions in a given crisis, should be to minimize the risks to all persons involved: hostages, bystanders, subjects, and law enforcement officers.

EFFECTIVE: 01/18/91

30-1.2 Control of a Crisis Management Team (CMT)

(1) Operational and administrative control of crisis management components lies with the SAC within the respective field office, except in certain unusual or major cases such as those involving dignitaries, diplomats, a large hostage population, or cases involving national or international impact, in which direct operational control may be assumed by the Assistant Director (AD), Criminal Investigative Division (CID), or AD, Intelligence Division (INTD), FBIHQ, or their designated representative. The SAC of the office employing crisis management components must personally assume direct management responsibility and control of those components.

(2) The SAC or his/her designated representative must assume the responsibility of on-scene commander (OSC) during a crisis incident. It is the duty of the SAC/OSC to determine the overall strategy for responding to and/or resolving a crisis incident. The crisis management component leaders will then devise specific tactics/procedures to support the SAC/OSC's strategy. These tactics/procedures are all subject to the approval of the SAC/OSC.

(3) The Crisis Management, Negotiation, and SWAT Programs are coordinated at the FBIHQ level by a program manager working in the Special Operations and Research Unit (SOARU) in the Training Division. Training Division, through the SOARU, is responsible for crisis management, negotiation, and SWAT training; doctrinal development; research and evaluation; advisory services; certain logistic support to the field; and operational support to FBIHQ and the field.

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 30 - 3

EFFECTIVE: 01/18/91

30-1.3 Crisis Management Plans

(1) The preparation of plans to anticipate and respond to specific crisis situations is imperative.

(2) The following procedures should be used when preparing such plans:

(a) Identify potential crisis situations.

(b) Prioritize potential crisis situations.

(c) Determine what is expected of the Bureau during the crisis (objectives).

(d) Make provisions to acquire the resources needed to accomplish your objectives.

(e) Identify sources of intelligence:

1. Human--collect background/descriptive information on subjects, employees, occupants, and others having access to crisis site.

2. Physical--conduct a thorough site survey of the crisis site.

(f) Develop strategies and tactics--developing the overall strategy for a particular crisis situation is a command function. Once the strategy is determined, the other components of the CMT develop specific tactics to support the overall strategy of the OSC.

(g) Determine command/control/communications requirements.

1. If it is a joint operation, determine who will be the lead agency. Once this is decided, designate a chain of command.

2. Select location for a command post.

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 30 - 4

3. Design a communications format.

(h) Determine logistics required to support the overall response to the crisis.

(i) Establish liaison and coordination with contributing agencies and services.

(j) Commit plan to paper.

(k) Test the plan and modify accordingly.

(l) Disseminate the plan to appropriate personnel.

EFFECTIVE: 01/18/91

30-1.4 Decision Making

Decisions must be made while working within the context of the crisis management plan to assure an acceptable solution. When in a decision-making mode, it is helpful to include others in the decision-making process and weigh decisions against preestablished criteria.

(1) Action criteria should consider:

(a) Necessity--is the contemplated action necessary at this time within the context of the crisis event?

(b) Risk effectiveness--is the contemplated action warranted because it will reduce risk? Or will it increase risk?

(c) Acceptability--is the contemplated action legally and ethically acceptable?

(2) Having clearly defined objectives when planning for a particular crisis (and being able to prioritize them) will facilitate good decision making.

EFFECTIVE: 01/18/91

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 30 - 5

30-1.5 Command Post (CP) Procedures

(1) Some type of CP is necessary to coordinate the actions of multiple units, especially when they are engaged in multiple activities, or when the number of individuals involved in a crisis situation exceeds the span of control of the OSC.

(2) Prior to setting up the CP, the following steps should be taken:

(a) Establish a command structure to include all crisis management components being used. This chain of command must be communicated and formally posted.

(b) Assign responsibilities to the components of the command structure (mission).

(c) The leader of each component must be delegated the authority to successfully accomplish that component's mission.

(d) Design an organizational format for the CP.

(e) Develop a standing operating procedure (SOP) for the CP. This SOP should outline a procedure for the gathering and processing of intelligence. All components represented in the CP must have a system that enables them to receive, analyze, file, and retrieve intelligence. The SOP should also outline procedures for communicating this intelligence to the on-scene commander and other components in the CP.

(f) When possible, use an advisory staff in the CP. The SAC will designate an individual to act as a representative of each component of the CMT. This individual should preferably be a supervisor who is familiar with the capabilities and limitations of that particular component. This group of supervisors/Special Agents will be called advisors (e.g., SWAT advisor, negotiation advisor) and will form the SAC's advisory staff. In crisis situations where the SAC and his/her CP are in close proximity to the actual component leaders, the use of an advisory staff would not be absolutely necessary. However, in crisis situations where the SAC and his/her CP are not in close proximity to the component leaders, there are certain advantages to using the advisory staff:

1. It enables the component leader to be with, and function with, his/her team, which is the best place for the team leader to be.

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 30 - 6

2. It provides the SAC with a knowledgeable staff that is always in the CP and prepared to answer any questions regarding a particular component.

3. It provides the SAC with an individual in the CP that will receive, analyze, file, and retrieve intelligence from a particular component.

(g) In addition to an advisor for each component of the CMT, the SAC will also designate a crisis management advisor in the CP. This individual will ensure the CP is operating in accordance with the SAC's CP procedures. The crisis management advisor can identify problem areas and correct them before any serious problems occur. This advisor will also ensure all components are communicating and coordinating all their actions at the crisis site.

EFFECTIVE: 01/18/91

30-1.6 Field Office Response to Crisis Situations (See MIOG, Part I, 252-1.7.)

(1) The crisis management assets of most field offices may not be capable of adequately handling a major or protracted crisis situation without additional assets. When it becomes apparent a crisis situation will continue for more than 24 hours, the SAC may contact surrounding field offices for additional resources.

(2) The SOARU has divided the 56 field offices into eight districts and 16 regions. Each district contains one to three regions, and each region contains from two to five field offices. Any field office that is faced with a crisis situation demanding a response exceeding its capability can call upon its region for additional resources. The districts and regions are structured as follows: (See 30-2.2(2) and 30-3.2(3).)

FIELD SWAT DISTRICT/REGION ASSIGNMENTS

DISTRICT 1

Region 1

Region 2

Region 3

b2
b7E

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 30 - 7




DISTRICT 2

Region 4

Region 5

Region 6




DISTRICT 3

Region 7


DISTRICT 4

Region 9

Region 10

Region 11


DISTRICT 5


DISTRICT 6

Region 8

Region 12

Region 13





DISTRICT 7


DISTRICT 8

Region 14

Region 15

Region 16




Sensitive
PRINTED: 02/18/98

b2
b7E

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 30 - 8

[REDACTED] [REDACTED]

* Denotes the 9 Enhanced District Teams
() Denotes SWAT Complement w/56 Field Offices

TOTAL [REDACTED]

b2
b7E

(3) In confrontations necessitating employment of force involving an extraordinary degree of risk and which, in the judgment of the SAC, exceed FBI SWAT capability, the AD, CID, or AD, National Security Division, or their representative, should be advised in the event specialized tactical intervention may be requested. The FBI entity charged with responding to these incidents is the HRT. The HRT may be requested through CID, Violent Crimes and Major Offenders Section, FBIHQ.

EFFECTIVE: 08/29/94

30-1.7 Training

(1) At Quantico:

(a) Four days of crisis management training is conducted during Executive Development Institute (EDI) training sessions.

(b) One day of crisis management training is conducted during FBI Supervisors' Management Seminars.

(2) In the field:

(a) Each field office must conduct at least one training session per year that enables the components of the crisis management team to interact in a realistic crisis scenario. This training session should include a command post exercise (CPX) and field training exercise (FTX).

(b) The SAC and his/her management staff must be directly involved in this training session.

(c) The negotiation and SWAT components are mandated to participate in one regional training session each year. The host field office of the regional training session should conduct their

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 30 - 9

crisis management training during this regional training session (see (a) above).

(d) Training Division recommends that all crisis management components interact and train together whenever possible.

EFFECTIVE: 01/18/91

30-1.8 Reporting Procedures

(1) Each field office will submit semiannual reports on the utilization of their crisis management components, furnishing the following data:

(a) Date of use.

(b) Bureau and field office file number, title, and character of case.

(c) A brief account of the activity, specifically outlining the role played by each component of the CMT.

(d) The negotiation and SWAT components will also include enclosures to this report, detailing specific information regarding these components. Specifics are enumerated in the Crisis Negotiation and SWAT Program sections that follow.

(2) Reports are due by the 15th day of April and October, for the previous six months. They must be transmitted by cover airtel to the Director, FBI, Attention: Training Division, Special Operations and Research Unit.

EFFECTIVE: 01/18/91

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 30 - 10

30-2 CRISIS (HOSTAGE) NEGOTIATION PROGRAM

(1) Crisis negotiation is the process of using specific techniques (relying heavily on verbal communications) to bring about a desired behavioral change on the part of an individual who may pose a threat to himself/herself or others, and to offer an alternative to (or support of) tactical intervention in raids, arrests, and rescues.

(2) Specially trained and equipped Agent volunteers will function as part of a field office crisis management team. This crisis negotiation team can greatly reduce the risks associated with handling hostage, kidnap, barricade, and/or suicide situations and increase the options available to the SAC in dealing with such events.

EFFECTIVE: 01/18/91

30-2.1 Control of Negotiators

(1) Operational and administrative control of negotiators is the same as mentioned in 30-1.2(1).

(2) The SOARU also manages the FBI's Critical Incident Negotiation Team (CINT). The CINT is comprised of the FBI's most experienced negotiators who have a specialized investigative and/or foreign language capability. CINT members are afforded advanced training in negotiation and terrorism to include nuclear, chemical, and biological negotiation considerations. This team is considered a national resource for the FBI and is deployed at the direction of FBIHQ through contact with the SOARU.

EFFECTIVE: 01/18/91

30-2.2 Organization

(1) Each field office will have a crisis negotiation team with a minimum of three trained negotiators. The eight field offices that have the enhanced SWAT district teams will have a minimum of six trained negotiators. Larger field offices or offices with distant resident agencies should have additional Agents trained as negotiators. The total number of negotiators in a field office should be based on the geographical area covered, the population density, and the potential for utilization.

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 30 - 11

(2) Any field office facing an event demanding a response exceeding its capability can call upon its region for negotiator support. The districts and regions are structured as indicated in the district chart at 30-1.6(2).

(3) The configuration of the negotiation team within each field office is left to the discretion of the SAC, but it must always have two negotiators per shift--a primary and a secondary negotiator. This team may be supported by additional negotiators as needed.

(4) SACs will appoint a negotiation coordinator charged with the responsibility of being familiar with team capability. The negotiation coordinator should be an individual who has served satisfactorily as a team member and has a good working knowledge of basic negotiation and tactical concepts.

(5) The negotiation coordinator should act as negotiation advisor and representative in the CP during operations.

EFFECTIVE: 01/18/91

30-2.3 Utilization

Negotiators will deploy with the field office SWAT team in any situation posing a higher-than-normal risk factor in which the SWAT team could anticipate encountering a potential barricade, suicide, or hostage situation. Such deployments should be based on available intelligence concerning the subject, weapons, and location.

EFFECTIVE: 01/18/91

30-2.4 Qualifications for Negotiation Team Members

(1) Agents assigned to negotiation teams in the field must have satisfactorily completed the two-week basic negotiation training course at the FBI Academy.

(2) Negotiation candidates should be:

(a) Volunteers.

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 30 - 12

(b) In excellent physical condition.

(c) Emotionally capable of functioning in a prolonged high-stress situation.

(d) An FBI Agent for at least three years.

Experience as a police officer, military service, or having a behavioral science background is also desirable and could be considered an exception to item (2)(d) above.

EFFECTIVE: 01/18/91

30-2.5 Reporting

As set forth in 30-1.8(1)(a)-(c), each field office is required to submit semiannual crisis management reports. The following additional negotiation data is to be furnished as an enclosure in this designated format:

I. New tactics, techniques, concepts of operations or equipment successfully employed in negotiation operations during the reporting period.

II. Problems encountered relative to negotiation operation during the reporting period.

III. Team status:

A. Specialized training needed by your office.

B. Official Bureau name of each team member.

C. The identity of the negotiation coordinator.

D. Number of days devoted to team training this reporting period.

EFFECTIVE: 01/18/91

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 30 - 13

30-2.6 Training

(1) At Quantico:

(a) Basic negotiation training will consist of a two week course at the FBI Academy.

(b) Specialized regional training courses will be held every year as required.

(2) In the field:

(a) Training will consist of a minimum of six days per year. The maximum is to be determined by the SAC and his/her special needs.

(b) Each field office negotiation team will participate in one regional training session per year where the host office conducts a CPX/FTX. The negotiation team will also participate in the one mandatory crisis management training session per year in their respective field office.

(c) The SAC must personally participate when his/her office is hosting a regional training session. This responsibility is not to be delegated.

EFFECTIVE: 01/18/91

30-2.7 Management of Negotiation Teams

(1) To fully utilize the capabilities of the negotiation team, the command of the team must be delegated to the negotiation coordinator by virtue of his/her training with the team and familiarity with the capabilities of the team.

(2) The SAC or his/her designated representative must assume the responsibility of OSC during a crisis incident. It is the duty of the SAC/OSC to determine the overall strategy for responding to and/or resolving a crisis incident. The negotiation coordinator will then devise specific negotiation tactics/procedures to support the SAC/OSC's strategy. These negotiation tactics/procedures are all subject to the approval of the SAC/OSC.

(3) Negotiation team deployment on a regional or district

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 30 - 14

basis, or when the HRT is operationally deployed, will be supported by the SAC from the host office, or his/her ASAC in the event he/she is not available. The SAC/OSC will promptly designate a senior negotiation coordinator as the overall negotiation commander and ensure that the chain of command is understood by all personnel present.

EFFECTIVE: 01/18/91

30-2.8 Joint Operations

(1) Many FBI operations involve close work with other law enforcement agencies, and this relationship may necessarily extend to hostage or barricade situations involving FBI and police negotiation teams.

(2) Due to the wide divergence of training, procedures, and professional competency of police negotiation teams, the integration of police and FBI negotiation teams in a given operation should be approached with caution from standpoints of effectiveness, safety, and legal liability.

(3) In joint operations, it is imperative that unified negotiation teams be established at the outset with one person clearly in charge of all negotiations, preferably the most experienced FBI negotiation team leader present. The arbitrary assumption of command by the FBI, particularly if police units are first on the scene, as they frequently are, could be a sensitive and provocative maneuver requiring tact and diplomacy on the parts of the SAC and negotiation coordinator.

(4) The decision to engage in a joint operation must be made by the SAC and should be based on the recommendations of the negotiation coordinator, his/her team, and all other factors bearing on mission safety and effectiveness.

EFFECTIVE: 01/18/91

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 30 - 15

30-2.9 Use of FBI Negotiators in Non-FBI Matters

(1) |Office of the General Counsel (OGC)| has reviewed the use of FBI Special Agent negotiators in non-Federal matters. |OGC| opined that FBI negotiators could actively participate in situations lacking clear Federal jurisdiction where the Special Agent negotiator is either the first person on the scene or where there is no state or local negotiator available.

(2) |OGC| further advised hostage situations, by their very nature, involve emergency circumstances that would justify an FBI response even where a Federal violation is not readily apparent. Even if an FBI negotiator was not actually doing the negotiating, the FBI negotiator could still furnish advice or consultation on the scene as part of our training responsibilities under Title 28, Code of Federal Regulations, Section 0.85(e).

(3) Title 42, USC, Section 3774(a) authorizes the Director of the FBI to assist in conducting training of state or local law enforcement entities and conveys some Federal authority on which FBI negotiators can operate in non-Federal situations.

(4) Two guidelines concerning the role of an FBI negotiator providing assistance to local authorities in a non-Federal offense must be adhered to:

(a) The FBI negotiator must remain under the control of his/her SAC as opposed to the local authorities.

(b) FBI negotiators should be extricated from the actual negotiations, using their best professional judgment, once trained local officers arrive and are in a position to safely assume responsibility for the situation.

EFFECTIVE: 09/09/94

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 30 - 16

||30-3| SPECIAL WEAPONS AND TACTICS (SWAT) PROGRAM|

The SWAT Program is a concept based on the premise that a select group of highly motivated and well-conditioned Agent volunteers, specially equipped and trained to function as a team, can greatly reduce the risks associated with handling unusually dangerous raids, arrests, and rescues, and increase the options available to the SAC in dealing with such events.

EFFECTIVE: 01/18/91

||30-3.1| Control of SWAT

Operational and administrative control of SWAT is the same as mentioned in 30-1.2(1).|

EFFECTIVE: 01/18/91

||30-3.2| Organization

(1) Each FBI field|office|has a primary SWAT unit, the size of which varies from|office to office,|depending upon geographical area covered, population density, and the potential for violent crime within FBI jurisdiction. |Additionally, the eight technically enhanced district teams are configured to provide technical and operational support to field offices within their geographic districts.|

(2) The size of|office|primary units may be increased only by FBIHQ, based upon recommendations of the SAC, supported by well documented rationale. |Additional requests for manpower increases will not be approved by FBIHQ without identifying corresponding reductions elsewhere.|

(3) Realizing that the relatively small teams in most|offices|will not be sufficient to handle major or protracted problems, the field has been divided into|eight districts and 16 regions. Each district contains one to three regions and each region contains from two to five offices. |Any|office|facing an event demanding a response exceeding its capability can call upon its region

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 30 - 17

for reinforcement, not only for SWAT personnel, but other crisis management assets. Should an event exceed the capability of any specific region or require specialized equipment not in the possession of that field office, an SAC may request assistance from his/her district team. Requests for regional or district support, however, should be kept to a minimum. When requested, this support may be for equipment only, equipment and a minimum number of operators, or more extensive reinforcement. The districts and regions are structured as indicated in the district chart in 30-1.6(2), with the primary SWAT complement designated in parentheses.

(4) Primary team members will be supported with training and equipment by the Training Division. Each SAC is authorized to develop and maintain reserve teams as needed, but they must be supported by utilizing field resources. Reserve teams will participate in monthly field SWAT training at the discretion of the SAC.

(5) The configuration of teams within each office is left to the discretion of the SAC, except that all primary team members should be assigned to headquarters city.

(6) Each primary team within an office must be directed by a team leader selected by the SAC from the primary members. If an office has more than one team, a senior team leader must be appointed among the primary team leaders to manage all SWAT teams within the office.

(7) SACs will appoint a separate SWAT advisor, preferably a Supervisory Special Agent charged with the responsibility of being familiar with team capability and acting in the capacity of tactical advisor and SWAT representative in the command post during operations.

(8) The SWAT advisor should be an individual who has previously served satisfactorily as a team member and has a good working knowledge of basic tactical concepts but is no longer a participant on a team.

EFFECTIVE: 01/18/91

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 30 - 18

||30-3.3| Utilization

(1) A raid, arrest or other situation posing a higher-than-normal risk factor will necessitate the use of a SWAT unit for planning and execution whenever practicable to reduce the risk to Agents, innocent persons, and subjects.

(2) The determination as to whether a given situation meets "higher-than-normal risk" criteria will be made by the SAC or ASAC based upon assessment of the following factors:

(a) Subjects--number, motivation, training, propensity to violence, and other indicators.

(b) Hostages (if any)--number, location, medical histories, etc.

(c) Objective (crisis point)--location, defensibility, size configuration, avenues of approach, etc.

(d) Weapons--types, numbers, lethality.

(3) It is not the intent of this policy to place all raids and arrests in the hands of SWAT teams, but rather to reduce the risks to all personnel involved in those relatively few situations which would pose unwarranted danger if handled by traditional means.

EFFECTIVE: 01/18/91

||30-3.4| Qualifications for SWAT Team Members

(1) Agents assigned to primary SWAT teams in the field must have satisfactorily completed basic SWAT training at the FBI Academy; however, an Agent who has not met this requirement may be assigned to a primary team provided (a) he/she receives as much basic training in the field as possible and (b) that he/she satisfactorily completes basic SWAT training at the FBI Academy, or the FBIHQ-authorized field equivalent using the SWAT lesson plans at monthly training sessions, as soon as possible following his/her placement on a primary team.

(2) Candidates for SWAT duty should be:

(a) Volunteers.

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 30 - 19

- (b) In excellent physical condition.
- (c) Emotionally stable.
- (d) Proficient and confident in the use of small firearms.

Experience as a police officer, military combatant, firearms, and/or defensive tactics instructor is also desirable.

(3) It is desirable, but not mandatory, that reserve SWAT teams consist of Agents who have completed basic SWAT training.

(4) It is also desirable, but not mandatory, that candidates have at least three years of experience in the field.

EFFECTIVE: 01/18/91

30-3.5 Reporting

As set forth in 30-1.8(1)(a)-(c), each field office is required to submit semiannual crisis management reports. The following additional SWAT data is to be furnished as an enclosure in this designated format:

I. New tactics, techniques, concepts of operation or equipment successfully employed in SWAT operations during the reporting period should be set forth.

II. Problems encountered relative to SWAT operation during the reporting period should be included in the report.

III. Team status to include authorized SWAT complement.

- A. Specialized training needed by your office.
- B. Official name of each primary team member.
- C. Identity of senior team leader (and subordinate team leaders if more than one team).
- D. The identity of SWAT advisor.

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 30 - 20

E. The identities of primary team members who have not completed basic SWAT training.

F. Number of days and hours devoted to team training this reporting period, broken down by tactical subject.

Semiannual reports should include an FD-39, reporting firearms qualification scores.

EFFECTIVE: 01/18/91

30-3.6 Training

(1) At Quantico:

(a) Basic SWAT training will consist of a two-week course at the FBI Academy.

(b) Specialized in-service courses will be held every two to three years or as required.

(c) Only primary team members will be eligible for SWAT training at the FBI Academy.

(2) In the field:

(a) Training will consist of a minimum of the equivalent of one day per month, except district teams which are mandated to conduct a minimum of two days of training each month. The maximum is to be determined by the SAC and his/her special needs, but this training is not to exceed five days per month. Any request in addition to the five days per month must be fully justified and approved by SOARU, Training Division, FBIHQ.

(b) Each field office SWAT team will participate in one regional training session per year where the host office conducts a CPX/FTX. The SWAT team will also participate in the one mandatory crisis management training session per year in their respective field office.

(c) The SAC must personally participate when his/her office is hosting a regional training session. This responsibility is not to be delegated.

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 30 - 21

EFFECTIVE: 01/18/91

||30-3.7| Management of SWAT Teams

(1) To fully utilize the effectiveness and capability of SWAT teams, the direct tactical command of the units must be delegated to the team leader by virtue of his/her training with the team and his/her familiarity with its capabilities. This in no way alters the overall command responsibility and authority of the SAC within his/her field office.

(2) |The SAC or his/her designated representative must assume the responsibility of OSC during a crisis incident. It is the duty of the SAC/OSC to determine the overall strategy for responding to and/or resolving a crisis incident. The SWAT team leader will then devise specific tactics/procedures to support the SAC/OSC's strategy. These tactics/procedures are all subject to the approval of the SAC/OSC, with the exception of emergency self-defense measures and immediate-response deployment. It is the responsibility of the SWAT team leader to personally direct the team in the execution of an approved plan.

|(3)| Time and circumstances permitting, an inspection of personnel and a rehearsal of the tactical plan should be conducted before the plan is executed.

|(4)| SWAT team deployment on a regional or district basis, or when the HRT is operationally deployed, will be supported by the SAC from the host office, or his/her ASAC in the event he/she is not available. This individual will promptly designate a senior SWAT leader as the overall tactical commander and ensure that the chain of command is understood by all personnel present.

EFFECTIVE: 01/18/91

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 30 - 22

30-3.8 Fire Discipline

(1) Any confrontation should be managed with minimal use of weapons fire.

(2) Much emphasis is placed on fire discipline during initial SWAT training and must continue in field training. Personnel on the scene of a confrontation who have not had SWAT training must be thoroughly briefed by the senior SWAT team leader concerning use of firearms in the context of problem solution.

(3) Use of deadly force by SWAT personnel is governed by the same policy applicable to all Special Agents. (See MIOG, Part II, 12-2.1.)

(4) Meeting the above criteria, however, does not justify indiscriminate "area" type firing. All use of firepower must be preceded by acquisition of a known hostile target. This does not preclude the directing of selective suppressive fire at a low visibility target (such as a window from which gunfire is emanating) to cover movement of personnel, rescue of wounded individuals or evacuation of innocents.

(5) The use of shotgun breaching as a forced entry technique is authorized for all SWAT teams. (However, appropriate training is required as set forth in MAOP, Part II, 8-9.) It can be deployed concurrent with SAC approval, consistent with FBI deadly force guidelines, using only Bureau-approved frangible shotgun rounds. Using frangible rounds does not create unreasonable risks; those risks that may exist can be mitigated by ensuring that in each case where the use of this technique is contemplated, the following factors are carefully weighed:

(a) The presence and number of individuals inside the building to be breached;

(b) Proximity of those individuals to the area to be breached;

(c) Whether innocent persons are at risk; and

(d) The risk of primary or secondary fragmentation.
See MAOP, Part II, 8-9.3(4).

(6) Likewise, the use of chemical agents must be extremely judicious, with a minimum number of grenades injected to

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 30 - 23

dislodge subject(s). Use of chemical agents also necessitates standby fire-fighting equipment. Explosive ordnance disposal technicians may be required to remove dud 40 mm munitions. (See MIOG, Part II, 12-14.1 and 12-14.2 for chemical agent policy and procedures.)

EFFECTIVE: 04/07/97

||30-3.9| Joint Operations

(1) Many FBI operations involve close work with other law enforcement agencies; and from a realistic viewpoint, it is realized that this relationship may necessarily extend to raid and arrest situations involving FBI and police tactical units.

(2) Due to the wide divergence of training, procedures, and professional competency of police SWAT units, the integration of police and FBI teams in a given operation should be approached with caution from standpoints of effectiveness, safety, and legal liability. If necessary to combine units, teams should remain intact and be separated by function. For instance, in a raid requiring joint operations, police SWAT units might be assigned the cover function and FBI teams the apprehension function. But under no circumstances should personnel from police SWAT units be integrated into FBI teams or vice versa.

(3) In joint operations, it is imperative that unified tactical command be established at the outset with one person clearly in charge of all operations within the inner perimeter, preferably the most experienced FBI SWAT leader present. Briefing in preparation for joint operations should follow the "operations order" format as set out in Training Division handouts.

(4) It is realized that arbitrary assumption of command by the FBI, particularly if police units are first on the scene as they frequently are, could be a sensitive and provocative maneuver requiring tact and diplomacy on the parts of the SAC and senior SWAT team leader.

(5) The decision to engage in a joint operation must be made by the SAC and should be based on recommendations of the senior team leader, his/her unit, and all other factors bearing on mission safety and effectiveness.

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 30 - 24

(6) In confrontations necessitating employment of force involving an extraordinary degree of risk and which, in the judgment of the SAC, exceed FBI SWAT capability, the AD, CID, or AD, INTD, FBIHQ, or their representative should be advised in the event specialized HRT intervention may be requested.

EFFECTIVE: 01/18/91

30-3.10 Weapons

Certain weapons in the FBI arsenal were acquired specifically for SWAT applications and should be assigned to team members for their exclusive use. They are:



FBI firearms instructors may utilize these weapons when instructing SWAT personnel.

EFFECTIVE: 01/18/91

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 31 - 1

SECTION 31. DEPUTATION PROGRAM

31-1 BACKGROUND

(1) Historically, the Attorney General has had the authority to supervise and direct the United States Marshals Service (USMS) in the performance of public duties. Specifically, the Attorney General is empowered to authorize the appointment of Special Deputy U.S. Marshals. In June 1984, this authority was delegated to the Associate Attorney General. The Associate Attorney General exercised his authority to direct the USMS to deputize state and local law enforcement officers to enable those officers to handle federal law enforcement functions while under the supervision of the FBI. Neither the FBI nor the Drug Enforcement Administration had independent deputation authority.

(2) Effective 10/27/86, Title 21, United States Code, Section 878 was amended by the enactment of the Anti-Drug Abuse Act of 1986. This legislation added state and local law enforcement officers to those who may be deputized by the Attorney General to carry firearms, execute warrants, serve subpoenas, make arrests and seizures, and carry out other federal drug law enforcement duties as determined by the Attorney General. The Attorney General no longer had to rely on the USMS to deputize officers assisting the FBI in drug investigations. In fact, the USMS had taken the position that it does not have the authority to make drug-related deputations. The Attorney General has delegated this deputation authority to the Director and on 8/4/87, the FBI assumed responsibility for deputizing officers assisting in FBI drug investigations. On 3/24/95, the Director delegated Title 21 deputation authority to Special Agents in Charge (SAC). An FBI-deputized officer is referred to as a Special Federal Officer (SFO). The Deputation Program is managed by the Administrative Unit, Operational Support Section, Criminal Investigative Division (CID).

EFFECTIVE: 08/09/95

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 31 - 2

31-2 SCOPE OF DEPUTATION AUTHORITY

(1) Special Federal Officers are authorized to investigate, under FBI supervision, violations of Title 21 and those drug-related violations falling within the FBI's jurisdiction that arise out of an investigation predicated on drug violations.

(2) The scope of this authority is limited to those violations that are so inextricably linked to the Title 21 predicate that it could be fairly said that they would not have been engaged in separate and apart from the drug violations.

(a) For example, if during a drug investigation it was established that the subjects were engaged in money laundering, it would be reasonable to conclude that the subjects would not have engaged in this activity absent their primary involvement in drug trafficking. On the other hand, if during a drug investigation it was determined that the subjects were engaged in criminal activity totally unrelated to their drug trafficking, it would not be reasonable to conclude that there was a connection between the two violations.

(b) The fact that a nondrug violation is developed during a drug investigation is insufficient to empower a Special Federal Officer to investigate the violation if it did not arise out of the Title 21 predicate offense.

(c) Special Federal Officers do not possess general authority to act as FBI Special Agents.

(3) The USMS remains responsible for deputizing officers participating in FBI investigations which do not fall within the scope of the FBI's drug deputation authority. The USMS will not deputize officers to participate in Federal drug investigations.

EFFECTIVE: 01/22/90

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 31 - 3

31-3 CIVIL LIABILITY

(1) Special Federal Officers are considered Federal employees for purposes of civil suits brought under the Federal Tort Claims Act (FTCA). The FTCA provides that the exclusive remedy for common-law torts committed within the scope of a Federal employee's employment (e.g., a Special Federal Officer) is an action against the United States under the FTCA. Therefore, Special Federal Officers who allegedly commit common-law torts while acting within the scope of their authority as Special Federal Officers cannot be sued in their individual capacities. The suit must be brought against the United States and a resulting judgment for monetary damages, if any, will be satisfied by the United States rather than the individual Special Federal Officer. Specifically, judgments in excess of \$2,500 will be paid out of the United States Treasury rather than from FBI appropriations.

(2) Suits brought against a Special Federal Officer for alleged violations of a person's constitutional rights (i.e., Bivens actions) are not brought against the United States but rather against the Special Federal Officer in his/her individual capacity. An adverse judgment for monetary damages, entered against a Special Federal Officer, must be personally satisfied by the Special Federal Officer. However, the Department of Justice (DOJ) may provide legal representation to a Special Federal Officer and may indemnify the officer if it determines that the officer acted within the scope of his/her authority and that representation and indemnification would be in the interest of the United States.

(3) The possibility of civil liability and its potential for adversely impacting on FBI investigations requires that there be tight control and direction over Special Federal Officers. Close supervision of these officers is of critical importance and must be recognized by field office management.

EFFECTIVE: 01/22/90

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 31 - 4

31-4 GENERAL OR CASE-SPECIFIC AUTHORITY

(1) Generally, the deputation authority granted to a Special Federal Officer is restricted to specifically designated cases. The cases on which a Special Federal Officer is authorized to work are listed by file number on the FD-739 (Oath of Office and Credential - Special Deputation) and FD-739a (Credential Card). The officer is prohibited from assisting on any FBI investigation not reflected on these forms unless doing so under his/her normal police powers. All deputations in Organized Crime Drug Enforcement Task Force (OCDETF) cases are handled on a case-specific basis only. (See MIOG, Part II, 31-5(7)(d).)

(2) There may, however, be situations where general Title 21 investigative authority is justified in non-OCDETF drug investigations.

Often officers are detailed to FBI operational squads on a full time semipermanent basis. These officers occupy FBI space and function much the same as Special Agents. The squads may have a large number of drug cases open and cases are constantly being opened and closed. Under these or similar circumstances a request for general deputation authority may be appropriate. Such justification should be included in the initial deputation request submitted to the SAC.

EFFECTIVE: 08/09/95

31-5 GENERAL ADMINISTRATIVE MATTERS

(1) A deputation request will be approved in only two circumstances:

(a) The officer will be monitoring a Title III;

(b) The officer will be conducting investigation outside his/her own jurisdiction.

(2) When initially deputized, all officers must be sworn in by an SAC, or in his/her absence, an ASAC.

(3) Title 21 deputation authority may be granted by the SAC for a period not to exceed 24 months. Unless otherwise specified,

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 31 - 5

all FBI deputations automatically expire on October 1st of the second 12 month period in which the deputation was approved by the SAC. This expiration date appears on the FD-739 and FD-739a. EXAMPLE: If an SFO is deputized in June, 1995, that authority may continue, uninterrupted, until October 1, 1996 or for a period of 16 months. Prior to October 1, 1996 that SFO's deputation authority may be renewed, with SAC approval, for an additional 24 months to expire on October 1, 1998. The sponsoring field division is responsible for monitoring deputation expiration dates and for submitting timely renewal requests to the SAC, or in his/her absence, the ASAC.

(4) If the deputation request involves a renewal of an existing deputation authority, the SFO does not need to appear before the SAC, ASAC, or the case Supervisory Special Agent, to be resworn, as long as the deputation is renewed prior to deputation expiration date. A deputation renewal may be accomplished by submitting a timely renewal request to the SAC and having the SAC or, in his/her absence, the ASAC, execute the Deputation Statement on a new FD-739. The officer and SAC or, in his/her absence, the ASAC then subscribe to the Acknowledgement/Oath of Office on the new FD-739. The SAC or ASAC must also sign the FD-739a. This must be accomplished prior to the expiration of the current deputation.

(5) Close supervision of SFOs is of critical importance. The potential for civil liability and adverse impact on investigations is such that it is vital that there be tight control and direction over SFOs and their efforts on the FBI's behalf. (See MIOG, Part II, 31-3(3).)

(6) The following requirements apply to all FBI deputations:

(a) The officer's immediate FBI case supervisor must be identified on the FD-739;

(b) The officer must review the Memorandum to All Employees 6-89, dated 9/27/89, captioned "Principles of Ethical Conduct for Government Officers and Employees." The Manual of Administrative Operations and Procedures (MAOP), Part I, 1-1 (9), may also be used in the absence of this memorandum. The officer should also be advised that he/she will be expected to abide by these standards of conduct for the duration of their deputation and failure to do so may result in the termination of their deputation. (See MIOG, Part II, 31-6(1) (e).)

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 31 - 6

(c) The officer's deputation authority shall be terminated immediately by the sponsoring field division when it determines that the deputation is no longer necessary, e.g., the officer retires or resigns, is reassigned to other duties, the investigation is closed, etc. The officer must be specifically advised that his/her authority as an SFO is being terminated. The officer's credential card (FD-739a) must be recovered and sent to the SAC as an enclosure to a memorandum notifying the SAC of the termination of the deputation.

(7) The officer will also be required to acknowledge in writing on the FD-739 that he/she has been given instructions set forth below, understands them, and will adhere to them. These instructions are located on the reverse side of copy 3 (white) of the FD-739.

(a) The officer is not to travel out of state on FBI business without being accompanied by a federal Agent unless specifically authorized by an SAC or, in his/her absence, an ASAC.

(b) The officer is not to check federal prisoners out of a federal institution or holding facility unless accompanied by a federal Agent.

(c) The officer is authorized to monitor a federally authorized Title III, acting under the supervision of a federal law enforcement officer.

(d) The officer is deputized only for the specific case(s) authorized in the request for deputation. The officer is not authorized to work on any other federal investigation without specific approval. This deputation is not a general authority to act as a federal Agent.

(e) While this deputation may result in the officer not being liable under Section 1983 actions, the officer is reminded that he/she may nevertheless be liable for BIVENS-type actions.

(f) While engaged in the investigation of cases being directed by the FBI, the officer will remain at all times during the period of this deputation subject to the direction and control of the FBI.

(8) The FD-739a is not intended to be used as a means of primary identification. Any alteration of the FD-739a is specifically prohibited. This includes use of stand-alone credential cases,

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 31 - 7

photographs, official seals, reproductions, or unauthorized signatures.

(9) By October 1st, of each year, SACs are required to submit annual summary reports, by airtel, captioned "FYXX DEPUTATION SUMMARY REPORT," to the Administrative Unit, Operational Support Section, CID, which identifies all currently approved SFOs.

(a) These summary reports should include the following:

1. Full Name
2. State or Local Agency
3. Date Deputized
4. Expiration Date
5. OCDETF Investigation, file number;
Non-OCDETF Investigation, file number

EFFECTIVE: 08/09/95

31-6 DEPUTATION REQUEST PROCEDURES

(1) Title 21 Investigations

(a) All deputation requests must be closely coordinated with the U.S. Attorney's Office to ensure compliance and timely completion. All requests should be submitted at least 30 days prior to the time the deputations are required.

(b) The requesting field office must submit a "Title 21 Deputation Request" Memorandum (FD-815), for approval, to the sponsoring field office SAC. The request must have the original signatures of the SAC, case Supervisory Special Agent, and the authorized state or local law enforcement official.

(c) The requesting office must conduct DEA (NADDIS) and FBI (NCIC and field office indices) name checks on all officers to be deputized. The signature of the case Supervisory Special Agent certifies that these name checks have been completed and are negative.

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 31 - 8

In addition, the signature of the authorized state or local law enforcement official certifies that the officer to be deputized is not the subject of any internal investigations. Finally, the signature of the SAC certifies that the officers to be deputized have been advised of and agree to comply with the instructions set forth in the "Title 21 Deputation Request" Memorandum (FD-815).

(d) Upon approval of the FD-815 by the SAC or, in his/her absence, the ASAC, the requesting office is responsible for preparing the Oath of Office and Credential-Special Deputation (FD-739), securing the appropriate signatures and submitting the FD-739 to the SAC for deputation authority.

(e) The sponsoring office must review the deputation forms for accuracy, particularly file numbers. Any needed corrections should be made and needed descriptive information on the officer obtained. The officer must review the Memorandum to All Employees 6-89, dated 9/27/89, captioned "Principles of Ethical Conduct for Government Officers and Employees." In the absence of this memorandum the MAOP, Part I, 1-1 (9), may be substituted. The officer should be advised that he/she will be expected to abide by these standards of conduct for the duration of his/her deputation and failure to do so may result in termination of their deputation. The name of the officer's FBI case supervisor must be entered in the space provided on the FD-739. (See MIOG, Part II, 31-5(6)(b).)

(f) The instructions located on the reverse side of copy 3 of the FD-739 regarding the officer's responsibilities as an SFO must be given to the officer and acknowledged by signing and dating in the space provided.

(g) When initially deputized, an officer must take the oath of office as presented on the FD-739. The SAC, ASAC, or a Supervisory Special Agent may administer the oath. Both the officer and the SAC or ASAC must sign and date the FD-739 in the spaces provided.

(h) After the FD-739 has been signed by the SAC or ASAC, the FD-739a (Special Deputation Credential) should be detached from copy 3 (white) of the FD-739 and given to the SFO. Copy 1 (blue) of the FD-739 is also given to the SFO. Copies 2 (green) and 3 of the FD-739 should be maintained in the requesting office's deputation control file.

(i) Officers deputized for a non-OCDETF drug investigation do not need to be redeputized in the event the

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 31 - 9

investigation is converted to the 245 classification.

(2) Non-Title 21 Investigations; Drug Violations
Anticipated

(a) Occasionally, deputations may be required for cases not predicated on Title 21 violations; however, Title 21 violations are anticipated. This very narrow category requires deputation by both the FBI and the USMS.

(b) A Non-Title 21; Drug Violations Anticipated, deputation request can be accomplished by following the procedures required for Title 21 investigations and submitting an electronic communication from the SAC, under the caption "FBI Deputation Authority; Non-Title 21 Investigations; Drug Violations Anticipated" to the attention of the Administrative Unit, Operational Support Section, CID. The request must include the following information. (See MIOG, Part II, 31-6 (3) (b).)

1. Identify by title and file number all investigations on which the officer will be working. If general deputation authority is requested, no titles and file numbers are required; however, full justification must be set forth. Note that while an FBI deputation is routinely case specific, USMS deputation authority extends to all federal violations except Title 21.

2. Complete description of the officer, including full name, employing agency, date of birth, social security number, height, weight, sex, race, eye and hair color.

3. Results of field office indices name check, NCIC check, NADDIS check, and a check of the officer's employing agency internal affairs office.

4. U.S. Code violations being investigated.

5. Last firearms qualification date. It must be within the past year.

6. Number of years of law enforcement experience.

7. Contact Special Agent in requesting office.

(c) FBIHQ will prepare a deputation request and forward it to USMS Headquarters. The requesting office (contact

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 31 - 10

Special Agent) will be contacted by the local USMS office in order to arrange for the deputations.

(d) A copy of the approved FD-815 must accompany the
||electronic communication|requesting Non-Title 21 deputation request.

(3) Non-Title 21 Investigations; Drug Violations Not
Anticipated

(a) Officers assisting in investigations which do not involve drug violations are only deputized by the USMS.

(b) The Non-Title 21 Investigation; Drug Violations Not Anticipated deputation request can be accomplished by submitting
|an|electronic communication|from the SAC, under the caption "FBI Deputation Authority; Non-Title 21 Investigation; Drug Violations Not Anticipated" to the attention of the Administrative Unit, Operational Support Section, CID. The request must include the information set forth in Section 31-6 (2) (b).

(c) FBIHQ will prepare a deputation request and forward it to USMS Headquarters. The requesting office (contact Special Agent) will be contacted by the local USMS office in order to arrange for the deputation.

EFFECTIVE: 05/22/96

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 32 - 1

SECTION 32. REWARD POLICY

32-1 REWARDS

A reward is a sum of money or other premium offered by the Government or by a private person for the performance of some special or extraordinary service. By their very nature, offers of rewards are usually made to the public or to a class of persons and, as such, differ from the usual payments to informants set forth in Part I, 137-8, of this manual entitled, "Payments to Informants."

EFFECTIVE: 12/20/93

32-2 AUTHORIZATION

(1) Authorization to offer and pay rewards is in accordance with current confidential funding guidelines as herein set forth:

(a) Special Agent in Charge (SAC)	-	\$20,000
(b) Section Chief	-	\$50,000
(c) Deputy Assistant Director	-	\$150,000
(d) Assistant Director	-	\$250,000
(e) Associate Deputy Director	-	over
\$250,000		

(2) The SAC must approve each reward offer up to \$20,000. At the time the reward is paid the field office informant budget will be charged for the amount of the reward payment. If an SAC desires to offer a reward in excess of available funds, he/she will request additional funding and authorization from the appropriate FBIHQ substantive section prior to offering the reward. This communication should specify the amount of the requested reward offer and a detailed justification which addresses 32-4, (1)(a)-(f) below. (See 32-4(4) below.)

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 32 - 2

EFFECTIVE: 10/07/93

32-3 CRITERIA (See 32-4 below.)

(1) Rewards should only be offered on a selective basis in cases which normally have the following characteristics:

(a) A significant investigation.

(b) Logical avenues of investigation have either been concluded or appear unfruitful.

(c) Individual(s) who may be in possession of useful information are more likely to be motivated by money as opposed to civic duty.

(2) Issues associated with the offering of reward that must be considered are the following:

(a) The legitimate fear that the public offering of a large sum of money could result in the receipt of spurious information and the concomitant need to utilize resources to resolve the truthfulness of the information.

(b) The problem of deciding who is entitled to the reward.

EFFECTIVE: 10/07/93

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 32 - 3

32-4 REPORTING

(1) Where appropriate, the FBIHQ substantive unit should receive UACB notification of the reward offer under the appropriate case caption setting forth the following information: (See 32-2(2) above.)

(a) A detailed narrative of the investigation.

(b) The amount of the reward to be offered.

(c) Detailed justification which addresses the issues in 32-3 above.

(d) The criteria by which an individual will be considered eligible, i.e., "For information leading to the identification, arrest and conviction of the subject of the investigation," or in a kidnaping matter, "for information leading to the recovery of a kidnaping victim and the identification, arrest and conviction of the persons responsible."

(e) The identities of the local news media by which the reward offer will be made.

(f) The prepared text which will be provided to the local news media.

(2) All reward offers in this regard should be in strict accordance with the instructions set forth in the Manual of Administrative Operations and Procedures, Part II, 5-1, entitled, "Policy and Guidelines for Relations with News Media," and 5-2, entitled, "Contacts with News Media."

(3) The appropriate FBIHQ substantive unit should receive, UACB, airtel notification that a reward recipient has been selected and the basis for the selection.

(4) In those cases where FBIHQ authorization is required, the procedures set forth in 32-2 (2) should be followed.

EFFECTIVE: 10/07/93

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 32 - 4

32-5 ATTORNEY GENERAL REWARDS FOR INFORMATION CONCERNING
ESPIONAGE AND TERRORISM CASES

(1) Title 18, USC, Section 3071, provides the Attorney General with the authority to pay rewards to individuals furnishing information in connection with acts of espionage or terrorism when such information:

(a) leads to the arrest or conviction, in any country, of any individual for the commission of espionage or terrorism against the United States;

(b) leads to the arrest or conviction, in any country, of any individual for conspiring or attempting to commit an act of espionage or terrorism against the United States; or

(c) leads to the prevention, frustration, or favorable resolution (in terrorism cases) of an act of espionage or terrorism against the United States.

(2) The Attorney General determines whether an individual providing information concerning acts of espionage or terrorism is entitled to a reward and the amount of the reward. The maximum reward amount is \$500,000. Any reward of \$100,000 or more must be approved personally by the President or the Attorney General.

(3) The Attorney General may take such measures in connection with the payment of the reward to ensure that the identities of the recipient and the recipient's immediate family are protected.

(4) No officer or employee of any governmental entity is eligible for any monetary reward under Title 18, USC, Section 3071, if that person provides information concerning espionage or terrorism while in the performance of his or her official duties.

(5) Any individual who furnishes information that justifies a reward by the Attorney General may, in the discretion of the Attorney General, participate in the witness security program.

EFFECTIVE: 04/10/97

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 33 - 1

SECTION 33. NATIONAL DRUG INTELLIGENCE CENTER (NDIC)

33-1 NATIONAL DRUG INTELLIGENCE CENTER (NDIC)

The NDIC is a multiagency entity operating under the direction of the U.S. Attorney General. The mission of the NDIC is to develop organizational and strategic drug intelligence in support of the U.S. law enforcement community, Intelligence Community, and policy makers. NDIC's mandate necessitates the collection of detailed and relevant information concerning drug enterprises and drug trafficking patterns. On May 4, 1993, the FBI agreed in a Memorandum of Understanding (MOU) to provide NDIC unrestricted access to FBI historical and active investigative information concerning drug trafficking. The following procedures are intended to ensure NDIC's timely access of relevant FBI drug information with appropriate FBI review.

EFFECTIVE: 02/17/94

33-1.1 NDIC Interaction with FBI Field Offices

NDIC may obtain FBIHQ approval to interact directly with FBI field offices.

(1) NDIC will request by written communication FBIHQ approval for NDIC access to specified field offices and FBIHQ elements in furtherance of NDIC's information needs for specified project areas. The Section Chief, Intelligence Section, Criminal Investigative Division (CID) or designee, after consultation with the appropriate operational section, will be responsible for approving NDIC requests.

(2) The affected field offices will be notified by teletype which will detail the scope of NDIC's information needs for specified projects and will include the NDIC point of contact. This teletype will serve as notification of NDIC that their information request has been approved by FBIHQ.

(3) Upon receipt of the teletype, NDIC will communicate directly with the identified FBI field offices and FBIHQ elements. NDIC

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 33 - 2

will direct copies of all NDIC communications with FBI field offices to the Intelligence Section, CID, FBIHQ.

(4) Significant changes in the scope or direction of the project which impacts on FBI resources will require additional Section Chief, Intelligence Section, CID approval.

EFFECTIVE: 02/17/94

33-1.2 NDIC Analytical Support for FBI Drug Investigations

FBI field offices may receive NDIC analytical support for ongoing FBI drug investigations. The following procedures are in place for field offices desirous of NDIC analytical case support:

(1) The field offices will submit a request to the Sensitive Information Unit, Intelligence Section, CID, by teletype. The teletype should provide an overview of the investigation including the identification of the core organization being addressed.

(2) The Section Chief, Intelligence Section, CID, or designee, after consultation with the appropriate operational section, will review field office requests and prioritize the requests in accordance with the FBI Organized Crime/Drug National Strategy.

(3) Approved requests will be forwarded to NDIC by teletype for their evaluation and determination if sufficient resources are available to support the investigation or project.

(4) Upon NDIC approval of the request, NDIC will notify the field office and FBIHQ by teletype. NDIC will then coordinate the analytical support directly with the field office.

EFFECTIVE: 02/17/94

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 33 - 3

33-1.3 NDIC Access to FBI Automated Information Systems (AIS)

(1) NDIC will have access to the following FBI AIS:

- Field Office Information Management System (FOIMS)
- FOIMS Telephone data base
- FBIHQ General Index
- Criminal Law Enforcement Application (CLEA)
- Investigative Support Information System

(2) Only a select number of NDIC Intelligence Research Specialists (IRS) will be authorized access to FBI AIS.

(3) The designated IRSs will query the data bases and, when positive results occur, they will make a recommendation concerning the need for other NDIC personnel to see the data.

(4) The data retrieved from the FBI data bases, along with the recommendation, will be reviewed by an FBI Supervisory Special Agent (SSA) detailed to the NDIC. The review will include a finding as to the relevancy of the FBI data to NDIC projects and a determination whether the information should be disseminated to other NDIC personnel.

(5) The NDIC IRSs and SSAs will be subject to the same personnel rules, regulations, laws, and policies applicable to all FBI employees.

EFFECTIVE: 11/25/94

33-1.4 NDIC Access to Informant Files and Grand Jury Material

(1) NDIC will not be provided access to FBI informant files. FBI field offices will determine what level of access NDIC may have to informant information contained in the substantive case files. This is not intended to deny NDIC access to the information, rather it is intended to protect the identities of FBI confidential informants and cooperating witnesses.

(2) NDIC will not be provided access to Grand Jury 6E material unless specifically requested by the field office and in compliance with all applicable 6E rules.

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 33 - 4

EFFECTIVE: 02/17/94

33-1.5 NDIC Dissemination of FBI Information

NDIC will not disseminate FBI information to other agencies without the concurrence of the Section Chief, Intelligence Section, or designee and in accordance with mutually agreed upon dissemination procedures. The Section Chief of the Intelligence Section, CID or designee will be the FBI approving authority for NDIC dissemination issues.

EFFECTIVE: 02/17/94

33-1.6 NDIC Document Exploitation Branch Service (DocEx)

(1) To further the NDIC's mission of supporting drug law enforcement, the DocEx was created to assist in the storage and analysis of drug-trafficking information obtained through law enforcement activities. The DocEx was established to assist field operations with time-sensitive analysis of information seized pursuant to search warrants, subpoenas, or other enforcement actions which require immediate analysis.

(2) The DocEx Branch consists of Special Agents (SA) and analysts available for travel to field locations to assist in timely analysis of drug-related information. The DocEx is a field support unit and will not conduct unilateral investigations. All information developed by DocEx will be furnished to the field office of the requesting agencies.

DocEx can provide the following services to field offices:

- (a) Forensic computer assistance.
- (b) Link Analysis of telephone toll records.
- (c) Link Analysis of associations and affiliations.

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 33 - 5

- (d) Drug organization profiles.
- (e) Financial analysis including identification of assets.
- (f) Time-line analysis.
- (g) Access to public records databases.
- (h) Assistance to search scenes, including electronic inventory, electronic photography, and computer-generated floor plans.

(3) Initial formal requests from FBI field offices for NDIC DocEx assistance should be sent to FBIHQ for approval. A copy of the initial request should be sent to NDIC. It should be in writing, setting forth a brief summary of the investigation, the priority of the investigation within the division and any known requirements concerning the anticipated volume of materials to be seized and the time frames for the enforcement activity. Requests should be forwarded to FBIHQ, Attention: Unit Chief, Intelligence Development Unit, Intelligence Section, Criminal Investigative Division. The NDIC copy should be sent to the National Drug Intelligence Center, 319 Washington Street, Fifth Floor, Johnstown, Pennsylvania 15901, Attention: Chief, Document Exploitation Branch.

(4) The DocEx Branch should be contacted as far in advance of a proposed enforcement operation as possible. This timely notification will ensure that the DocEx team can work with the field offices in order to appropriately plan, staff, and support the timely analysis of seized documents.

(5) After initial coordination between FBIHQ and NDIC, field offices may thereafter correspond directly with NDIC regarding that particular case, keeping FBIHQ informed of any significant developments.

(6) Upon receipt of an approved request at NDIC, a Team Leader (a DEA/FBI SA assigned to NDIC/DocEx) will contact the Field Supervisor or Case Agent for an assessment of the personnel and equipment needed to support an assignment. A Team Leader may also make an on-site assessment, if necessary.

(7) Materials provided to NDIC will be handled solely by the DocEx team and not released to any other agency until approval is obtained from the submitting agency. This is in accordance with policy set forth in the Memorandum of Understanding between the FBI and NDIC. All information developed by DocEx will be returned to the requesting

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 33 - 6

| agency's field office. |

EFFECTIVE: 01/08/96

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 34 - 1

SECTION 34. VICTIM/WITNESS ASSISTANCE (VWA)

34-1 INTRODUCTION

The purpose of these MIOG guidelines is to establish procedures to be followed by the Federal Bureau of Investigation (FBI) in responding to the needs of crime victims and witnesses.

EFFECTIVE: 09/08/94

34-2 DEFINITIONS USED THROUGHOUT THESE GUIDELINES

(1) The term "victim" means a person that has suffered direct or threatened, physical, emotional, or pecuniary harm as a result of the commission of a crime, including:

(a) In the case of a victim that is an institutional entity, an authorized representative of the entity, and

(b) In the case of a victim who is under 18 years of age, incompetent, incapacitated, or deceased, one of the following (in order of preference): a spouse; a legal guardian; a parent; a child; a sibling; another family member; or another person designated by the court.

(2) The term "witness" means a person who has information or evidence concerning a crime and provides information regarding his/her knowledge to a law enforcement agency. Where the witness is a minor, the term "witness" includes an appropriate family member or legal guardian.

(3) The term "witness" does not include:

(a) a defense witness; or

(b) an individual involved in the crime as a perpetrator or accomplice.

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 34 - 2

(4) The term "responsible official" means the Special Agent in Charge (SAC) of the division or his or her designee having the primary responsibility for conducting the investigation.

(5) The term "earliest opportunity" or "earliest possible notice" means one that will not interfere with an investigation or hamper the responsible official in the performance of other law enforcement responsibilities.

(6) The term "multidisciplinary child abuse team" means a professional unit composed of representatives from health, social service, law enforcement, and legal service agencies to coordinate the assistance needed to handle cases of child abuse.

(7) The term "serious crime" (as used in the Victim and Witness Protection Act of 1982 (VWPA)) means a criminal offense that involves personal violence, attempted or threatened personal violence, or significant property loss.

(8) The term "financial" or "pecuniary" harm shall not be defined or limited by a dollar amount, thus the degree of assistance must be determined on a case-by-case basis. For example, since victims' means vary, that which constitutes a minimal financial loss for one might represent a devastating loss for another.

(9) The term "child" means a person who is under the age of 18, who is or is alleged to be:

(a) A victim of a crime of physical abuse, sexual abuse, or exploitation; or

(b) A witness to a crime committed against another person.

(10) The term "child abuse" means the physical or mental injury, sexual abuse or exploitation, or negligent treatment of a child. The term "child abuse" does not include, however, discipline administered by a parent or legal guardian to his or her child provided it is reasonable in manner and moderate in degree and otherwise does not constitute cruelty.

(11) The term "abuse" combined with "physical injury" also means in any case which

(a) a child is dead or exhibits evidence of skin bruising, bleeding, malnutrition, failure to thrive, burns, fracture

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 34 - 3

of any bone, subdural hematoma, soft tissue swelling, internal injuries, or serious bodily harm; and

(b) such condition is not justifiably explained or may not be the product of accidental occurrence; and

(c) any case in which a child is subjected to sexual assault, sexual molestation, sexual exploitation, sexual contact or prostitution.

(12) The term "local child protective services agency" means that agency of the federal government, of a state, or of a local government that has the primary responsibility for child protection on federal land, or federally contracted or operated facilities.

(13) The term "local law enforcement agency" means any federal, state or local law enforcement agency having primary responsibility for the investigation of an instance of alleged child abuse on federal land, or federally contracted or operated facilities.

(14) The term "mental injury" means harm to a child's psychological or intellectual functioning which may be exhibited by severe anxiety, depression, withdrawal, outward aggressive behavior, or a combination of those behaviors, which may be demonstrated by a change in behavior, emotional response, or cognition.

(15) The term "sexual abuse" includes the employment, use, persuasion, inducement, enticement, or coercion of a child to engage in, or assist another person to engage in, sexually explicit conduct; or the rape, molestation, prostitution, or other form of sexual exploitation of children; or incest with children.

(16) The term "sexually explicit conduct" means actual or simulated:

(a) sexual intercourse, including sexual contact in the manner of genital-genital, oral-genital, anal-genital, or oral-anal contact, whether between persons of the same or opposite sex; sexual contact means the intentional touching, either directly or through clothing, of the genitalia, anus, groin, breast, inner thigh, or buttocks of any person with an intent to abuse, humiliate, harass, degrade, arouse or gratify sexual desire of any person;

(b) bestiality;

(c) masturbation;

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 34 - 4

(d) lascivious exhibition of the genitals or pubic area of a person or animal;

(e) sadistic or masochistic abuse.

(17) The term "exploitation" means child pornography or child prostitution.

(18) The term "negligent treatment" means the failure to provide, for reasons other than poverty, adequate food, clothing, shelter, or medical care so as to seriously endanger the physical health of a child.

(19) The term "best efforts" means that, in the spirit of full compliance with VWA legislation, Agents and employees engaged in the investigation or detection of a crime shall make their finest attempt to see that victims of crime are accorded the rights described in the Victims Rights and Restitution Act.

EFFECTIVE: 09/08/94

34-3 VWA STATUTORY BACKGROUND

These guidelines combine the requirements of the Victim and Witness Protection Act of 1982 (VWPA), Public Law (PL) 97-291 (October 12, 1982), and the victims rights statutes contained in the Crime Control Act, PL 101-647 (November 29, 1990), which are Title V, Victims' Rights and Restitution Act of 1990 (VRRRA); and Title II, Subtitles D and E, Victims of Child Abuse Act of 1990 (VCAA). These laws were enacted to protect and enhance the necessary role of crime victims and witnesses in the criminal justice process, and were further interpreted by the 1991 Attorney General Guidelines for Victim and Witness Assistance (Guidelines). The Guidelines require Department of Justice investigative, prosecutorial and correctional components to make their best efforts to ensure that victims of crime are treated with fairness and respect for the victims' dignity and privacy.

The VRRRA sets forth a federal Crime Victims' Bill of Rights which states that a crime victim has the following rights:

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 34 - 5

- (1) The right to be treated with fairness and with respect for the victim's dignity and privacy.
- (2) The right to be reasonably protected from the accused offender.
- (3) The right to be notified of court proceedings.
- (4) The right to be present at all public court proceedings related to the offense, unless the court determines that testimony by the victim would be materially affected if the victim heard other testimony at trial.
- (5) The right to confer with attorney for the Government in the case.
- (6) The right to restitution.
- (7) The right to information about the conviction, sentencing, imprisonment, and release of the offender.

EFFECTIVE: 09/08/94

34-4 ELIGIBILITY FOR VWA

- (1) Witnesses (other than defense witnesses and perpetrators or accomplices of the crime) and victims may be considered for assistance through VWA.
- (2) In cases where the United States or the public are generally the victims (e.g., narcotics trafficking and tax evasion), victim services will be inappropriate; but in virtually ALL cases, there will be witnesses who will be entitled to witness services.
- (3) In Civil Rights cases that allegedly involve police brutality, VWA should not be provided until such time that DOJ assesses the case. In Civil Rights/Inmate cases, VWA will be inappropriate as inmates are already provided medical and mental health services free of charge by the institution in which they are housed.

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 34 - 6

EFFECTIVE: 09/08/94

34-5 OFFICE FOR VICTIMS OF CRIME (OVC), DOJ

The OVC serves as the federal focal point for all crime victim issues. The Federal Crime Victims Division is one of three divisions within the OVC that is responsible for:

(1) Providing and improving services for victims of federal crime;

VWA; (2) Monitoring compliance with legislation pertaining to

(3) Providing training and technical assistance to federal criminal justice personnel on victim assistance issues.

EFFECTIVE: 09/08/94

34-6 COORDINATION OF VWA MATTERS

(1) FBI Headquarters

(a) All matters pertaining to VWA, which involve the FBI, are coordinated through the Criminal Informant Unit (CIU), Intelligence Section, Criminal Investigative Division (CID), FBI Headquarters (FBIHQ).

(b) The CIU acts in a liaison capacity with FBI field offices; with the OVC, DOJ; with other federal agencies which investigate criminal activity; and with U.S. Attorneys' Offices (USAOs). The CIU coordinates VWA matters, as appropriate, with other CID sections and other divisions at FBIHQ.

(2) FBI Field Offices

(a) Each field office shall have a Victim/Witness Coordinator (VWC) designated by the SAC.

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 34 - 7

(b) Each division shall advise the CIU, FBIHQ, by airtel of any changes in the designation of the VWC within 10 working days.

(c) Each field office must establish written office policy determining who will perform the following duties:

At the earliest opportunity after the detection of a crime, each Agent and/or VWC shall make reasonable and diligent efforts to:

1. Identify the victims of a crime and inform them of their right to receive, on request, the services described further in these guidelines and;

2. Present the victim with a printed brochure, entitled "Information for Victims and Witnesses of Crime," which will inform each victim of the name, title, business address, and telephone number of the VWC or the Agent to whom such a request for services should be addressed.

a. In Civil Rights cases a pamphlet should not be provided until DOJ accepts the case indicating contributory conduct was not a factor in the brutality.

3. Upon request, after the victim has reviewed the brochure and requests services, the VWC or the Case Agent shall refer the victim to the place where he/she may receive emergency medical and/or social services; compensation for which the victim may be entitled under this or any other applicable law; and the manner in which such relief may be obtained.

a. The VWC or the Case Agent shall, to the extent deemed necessary and feasible, assist in referring the victim to the specific person or office which will provide the above services.

b. The responsible official or his or her designee shall take appropriate action to ensure that any property of a victim that is being held as evidence is maintained in good condition and returned to the victim as soon as it is no longer needed for evidentiary purposes.

4. The VWC or the Case Agent is required to fill out the Victim/Witness Information form for all cases with victims noting if a pamphlet was provided.

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 34 - 8

5. Consult with and provide the victim or witness with the "earliest possible notice" concerning:

a. the status of the investigation of the crime, to the extent that it is appropriate and will not interfere with the investigation;

b. the arrest of a suspected offender.

6. Upon request by a victim or witness, if cooperation in the investigation of the crime causes his/her absence from work, the VWC or the Case Agent shall notify the employer of the role of the victim or witness in the investigation through verbal or written communication.

7. Upon written request by a victim or witness, if the victim or witness experiences problems with his/her creditors as a result of the victim's or witness' cooperation in the investigation, the VWC or Case Agent shall notify the creditor of the role of the victim or witness in the investigation through verbal or written communication.

EFFECTIVE: 09/08/94

34-7 SECURITY OF COMMUNICATIONS AND FILES

(1) To ensure that appropriate security is afforded communications relating to individuals contacted for VWA purposes, all such communications should be captioned with the individual's true name, followed by the words "VICTIM/WITNESS ASSISTANCE." Bureau regulations regarding the security and release of information is contained in the Manual of Administrative Operations and Procedures (MAOP), Part II, Section 5, 5-1, 5-2; and Section 9, 9-1 through 9-6.

(2) The subclassification number 66F will identify Victim/Witness control files and should be used on all Victim/Witness communications. One copy of each communication should be placed into the control file, one copy in the field office's substantive file, and after the investigation is completed, one copy should be sent to the U.S. Attorney's Office.

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 34 - 9

(3) The FBIHQ control file number 66F-HQ-1043145 should be used on all written communications being forwarded to FBIHQ.

EFFECTIVE: 09/08/94

34-8 REPORTING DATA RELATIVE TO FBI FIELD OFFICES

EFFECTIVE: 09/08/94

34-8.1 Annual Best Efforts Report

(1) FBI field offices MUST provide FBIHQ with statistics regarding their assistance effort as part of the "Best Efforts Questionnaire" by October 15 of each fiscal year and must include:

- (a) The number of criminal cases opened for investigation;
- (b) The number of victims involved in these cases;
- (c) The number of child victims involved in these cases;
- (d) The number of victims assisted by the field office's VWA effort;
- (e) The number of witnesses involved in these cases;
- (f) The number of witnesses assisted by the field office's VWA effort;
- (g) The number of cases in which the VWC was directly involved;
- (h) The number of full-time equivalent professional

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 34 - 10

staff who are dedicated to the VWA effort; and

(i) The types of cases (i.e., white collar, sexual assault, drug-related) that most routinely involve the VWC.

(2) Other issues that concern how well the program is working in the field office should be set forth in the space provided in the "Best Efforts Questionnaire." The information from the "Best Efforts Questionnaire" will be utilized by FBIHQ to prepare the annual "Best Efforts Report" which will be sent to the Attorney General through the OVC. This information will contain all of the aforementioned data for each fiscal year.

(3) In reporting the requirements of the "Best Efforts Questionnaire" to FBIHQ, a letterhead memorandum is to be submitted to the CIU, FBIHQ, by COB October 15 of each fiscal year.

EFFECTIVE: 09/08/94

34-9 FUNDING AND DIRECT SERVICES AVAILABLE TO FEDERAL CRIME VICTIMS

(1) The FBI does not have the authority to provide financial compensation to crime victims but there are various state and local agencies that provide financial and direct assistance to federal crime victims. These services are provided to victims and witnesses by state and local agencies that receive federal crime victim grants from the OVC. The FBI should refer victims and witnesses to all available services. Authority to provide compensation for victims and witnesses rests with each state's compensation board, rather than with the law enforcement departments.

(2) After the victim has reviewed the brochure and if he/she requests services, the VWC or the Case Agent shall refer the victim to the place where he/she may receive emergency medical and/or social services; inform the victim of compensation for which the victim may be entitled under this or any other applicable law; and inform the victim of the manner in which such relief may be obtained.

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 34 - 11

EFFECTIVE: 09/08/94

34-9.1 State Compensation Programs

(1) Crime victims compensation programs, administered by the states, provide reimbursement of out-of-pocket expenses to victims and survivors of victims of violent crime. Payments are made for medical expenses, including expenses for mental health counseling and care, lost wages attributable to a physical injury, and funeral expenses attributable to a death resulting from a compensable crime. Some other compensable expenses include the replacement of eyeglasses or other corrective lenses, dental services and devices, and prosthetic devices.

(2) The Information Resources Division, Executive Agencies, Personnel and Administrative Support Unit, at FBIHQ has signed a Memorandum of Understanding (MOU) regarding the release of information to state compensation boards. The purpose of this MOU is to expedite the release of information to state compensation boards regarding the verification of an incident reported to the FBI by a crime victim. Each field office has a copy of the MOU and the All SACs airtel related to this MOU.

(3) Each state has its own procedures for crime victim compensation including the determination of maximum award amounts, criteria for approving claims, and the application process.

(4) Each VWC should have a "VICTIM/WITNESS RESOURCE MANUAL." Included in this manual is a complete listing of the contact person(s) for each state compensation board. The VWC shall refer the victim to the contact person who can provide him/her with the necessary information needed to apply for compensation. Compensation information should also be listed on the back of each pamphlet. (Entitled Information for Victims and Witnesses of Crime).

EFFECTIVE: 09/08/94

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 34 - 12

34-9.2 Crime Victims Fund

The Victims of Crime Act of 1984 (VOCA) established the Crime Victims Fund (Fund) in the U.S. Treasury to provide financial assistance to victim compensation and victim assistance programs. Fines and penalties from convicted federal defendants - not taxpayers - provide the money for the Fund. The major function of the Fund is to make services available to victims of federal crime by providing grants to direct service providers in addition to state compensation boards.

EFFECTIVE: 09/08/94

34-10 THREAT ASSESSMENT

(1) Consistent with the provisions of Title 18, USC, Sections 3521-3528, the responsible official shall make the necessary and appropriate arrangements to enable victims and witnesses to receive reasonable protection against threat, harm, and intimidation from a suspected offender and persons acting in concert with or at the behest of a suspected offender.

(2) Coordination of services for victims/witnesses requesting protection from intimidation should be coordinated through the field office VWC.

(3) If the victim or witness desires formal protection in the Witness Security Program (WSP), the field office VWC or case Agent should contact the Witness Security Program Coordinator in his/her field office who will then take appropriate actions.

EFFECTIVE: 09/08/94

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 34 - 13

34-11 REPORTING INCIDENTS OF CHILD ABUSE ON FEDERAL LAND AND
FEDERALLY OPERATED OR FEDERALLY CONTRACTED FACILITIES

(1) The VCAA was signed into law as Title II of the CCA. Prior to enacting of this legislation, Congress found that incidents of suspected or actual child abuse on federal land, federally operated or federally contracted facilities was grossly underreported and this underreporting is often the result of the lack of a mandatory federal reporting law.

(2) A major function of this Act is to require persons working on federal land, federally operated or federally contracted facilities where children are cared for or reside, who are mandated reporters to report suspected or actual child abuse to the appropriate local law enforcement agency or local child protective service agency.

(3) Failure to file such a report or inhibiting or preventing someone from filing a report results in criminal penalties.

(4) Bureau regulations regarding the reporting of incidents of child abuse in Indian Country is contained in the MIOG, Part I, Section 198-6 through 198-6.9.

EFFECTIVE: 09/08/94

34-11.1 Mandatory Reporting by Federal Investigators

(1) As law enforcement officers, FBI Agents are included in the category of "mandated reporters" as identified in the VCAA. Therefore, any Agent, working on federal land or in federally operated or contracted facilities, where children are cared for or reside, who has knowledge or reasonable suspicion that a child has been or is going to be abused, must immediately notify the local child protective services agency or law enforcement agency of that knowledge or suspicion. Compliance with this law is a responsibility placed upon each Agent INDIVIDUALLY and not on the FBI as an agency.

(2) Any local law enforcement agency or local child protective service agency that receives notification of child abuse or suspected child abuse from a mandated reporter working on federal land or in federally operated or contracted facilities or other individual

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 34 - 14

must immediately initiate an investigation and take steps to secure the safety and well being of the child (children) involved. This includes the FBI when it has primary investigative responsibility.

(3) When a local law enforcement agency or local child protective services agency receives notification from any person alleging child abuse on federal land or federally operated or contracted facilities outside that agency's primary investigative jurisdiction, the receiving agency must immediately notify the other primary agency and submit a written report within 36 hours as set forth below.

(4) Within 36 hours after receiving notification described above, the receiving agency will prepare a written report that shall include, if available:

(a) the name, address, age and sex of child that is the subject of the report;

(b) the grade and the school in which the child is currently enrolled;

(c) the name and address of the child's parents or other person responsible for the child's care;

(d) the name and address of the alleged offender;

(e) the name and address of the person who made the report to the agency;

(f) a brief narrative as to the nature and extent of the child's injuries, including any previously known or suspected abuse of the child or the child's siblings and the suspected date of the abuse; and

(g) any other information the agency or the person who made the report to the agency believes to be important to the investigation and disposition of the alleged abuse.

(5) Upon completion of their investigation of any allegation of abuse made to a local law enforcement agency or local child protective services agency, such agency shall prepare a final written report on such allegation.

The identity of any person making an initial notification described above shall not be disclosed without consent of that individual to any

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 34 - 15

| person other than a court of law.

EFFECTIVE: 09/08/94

| 34-11.2 Standard Reporting Form (See MIOG, Part II, 34-11.4.)

In every federally operated (or contracted) facility and on all federal lands, a standard written reporting form, with instructions, shall be disseminated to all mandated reporter groups. Use of this form shall be encouraged, but its use shall not take the place of the immediate making of oral reports, telephonically or otherwise, when circumstances dictate.

EFFECTIVE: 09/08/94

| 34-11.3 Penalty

(1) Failure to report suspected child abuse may result in a Class B Misdemeanor. Therefore, each Agent must ensure adherence to the statute. The VCAA also states that a "mandated reporter" who makes a report based upon his/her reasonable belief and which is made in good faith, will be immune from civil or criminal liability for making the report.

(2) Since violation of this statute is a misdemeanor, SACs (or their designees) shall inform each Agent of his/her statutory obligation to report and assist in the identification of abused children and discuss the prosecutive merit of each case with the U. S. Attorney before actively investigating complaints.

EFFECTIVE: 09/08/94

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 34 - 16

34-11.4 Designated Agency to Receive Reports of Child Abuse

(1) The FBI is defined as a "local law enforcement agency" only when it has "primary responsibility for the investigation of an instance of alleged child abuse" on federal land, or federally owned or contracted facilities and must immediately initiate an investigation and take immediate steps to secure the safety and well being of the child (children) involved.

(2) When the FBI receives notification from any person alleging child abuse on federal land, or federally owned or contracted facilities, including Indian country, and the FBI does not have primary investigative jurisdiction as defined by the law, the FBI must immediately notify the appropriate agency and submit a report within 36 hours as set forth in 34-11.2.

EFFECTIVE: 09/08/94

34-11.5 Privacy Protection of Child Witnesses and Child Victims

Stringent procedures for protecting the privacy of a child victim or witness and assuring the confidentiality of information received concerning a child victim or witness, include inter alia: filing under seal all documents which disclose the names of or identifying information concerning child victims and child witnesses, and redacting such names and identifying information from any publicly disclosed documents.

EFFECTIVE: 09/08/94

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 34 - 17

34-12 TRAINING

(1) It shall be mandatory for the Training Division to provide training to all presently employed and new investigators, concerning their responsibilities in carrying out the provisions of the Victim and Witness Protection Act of 1982, Victims Rights and Restitution Act of 1990, and the Victims of Child Abuse Act of 1990, and to provide written instructions to ensure that these laws are implemented.

(2) The VWA Staff at FBIHQ shall be responsible for coordinating a training curriculum, in conjunction with the Training Division at the FBI Academy, Quantico, with respect to the assistance of victims of and witnesses to federal crime, including child witnesses and victims of child abuse.

EFFECTIVE: 09/08/94

34-12.1 The Multidisciplinary Team Approach in Child Abuse Cases

Each SAC, in coordination with the USAOs, shall provide training to all Agents on multidisciplinary methods of interviewing victims of child abuse and child sexual abuse. The responsible official may follow the criteria, set out in Section 212(b), Subtitle A, Victims of Child Abuse Act (VCAA), recommending that state grant recipients develop and implement multidisciplinary child abuse investigation programs, including:

(1) A written agreement between local law enforcement, social service, health, and other related agencies to coordinate child abuse investigations;

(2) Joint initial investigative interviews of child victims by law enforcement, health, and social service agencies;

(3) A requirement that, to the extent practicable, the same agency representative who conducts an initial interview, conduct all subsequent interviews; and

(4) Coordination of each step of the investigation

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 34 - 18

process to minimize the number of the interviews that a child victim must attend.

Where multidisciplinary teams are not yet formally established, federal investigators should coordinate with existing child protective service agencies to reasonably protect children at risk from further abuse. Compliance with this training requirement shall be included in the agency's annual "Best Efforts Report."

EFFECTIVE: 09/08/94

34-13 RELEVANT EXCERPTS OF THE ATTORNEY GENERAL GUIDELINES ON
VICTIM AND WITNESS ASSISTANCE

(1) The following are excerpts relevant to the duties of the FBI regarding VWA as taken from the Attorney General Guidelines for Victim and Witness Assistance. A notation will designate what sections have been skipped.

(2) The Attorney General Guidelines should be interpreted in a positive manner. The advice of FBIHQ should be obtained before the services to victims or witnesses are refused or discontinued if there are any questions regarding the interpretation of these guidelines.

(3) When submitting an inquiry regarding the interpretation of the guidelines or request that the Department of Justice be consulted, provide the necessary information from which a judgment can be made regarding the victim or witness.

ARTICLE I. GENERAL CONSIDERATIONS

A. Statement of Purpose

The purpose of these guidelines is to establish procedures to be followed by the federal criminal justice system in responding to the needs of crime victims and witnesses. These guidelines combine the requirements of the Victim and Witness Protection Act of 1982 (VWPA), PL 97-291 (October 12, 1982), and the victims rights statutes contained in the Crime Control Act of 1990, PL 101-647 (November 29, 1990), "the Act." Consistent with the like purposes of these statutes, the present Guidelines shall provide definitive

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 34 - 19

guidance on implementation of the 1990 Act as well as continued guidance on the protection of witnesses under the VWPA; and shall serve as a single resource for the Department of Justice (investigative, prosecutorial, and correctional) agencies in the treatment and protection of victims and witnesses of federal crimes.

These Guidelines supersede the 1983 Attorney General Guidelines for Victim and Witness Assistance.

B. Background

The Victim and Witness Protection Act of 1982 was enacted "to enhance and protect the necessary role of crime victims and witnesses in the criminal justice process; to ensure that the federal government does all that is possible within limits of available resources to assist victims and witnesses of crime without infringing on the constitutional rights of defendants; and to provide a model for legislation for state and local governments."

Enactment of the Crime Control Act of 1990 demonstrates the continuing national concern for innocent victims of all crimes and reflects the view that the needs and interests of victims and witnesses had not received appropriate consideration in the federal criminal justice system under the VWPA. The victims' rights provisions of this law mandate that officials of the Department of Justice, and other federal agencies, engaged in the detection, investigation, or prosecution of crime, make their best efforts to ensure that victims of crime are treated with fairness and respect for the victim's dignity and privacy.

The 1990 Victims' Rights and Restitution Act (VRRRA) creates, in effect, a federal Victims of Crime Bill of Rights and codifies services that shall henceforth be available to victims of federal crime. This Act does not specifically address the treatment of witnesses; however, it reinforces and augments the VWPA in acknowledging the necessary role of witnesses in the criminal justice process and in ensuring their fair treatment by responsible officials.

The 1990 Victims of Child Abuse Act (VCAA) contains extensive amendments to the criminal code affecting the treatment of child victims and child witnesses by the federal criminal justice system. The 1990 VCAA provides, inter alia, a mandatory requirement for certain professionals working on federal land, or in a federally operated/contracted facility, to report suspected child abuse and child sexual abuse.

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 34 - 20

Thus, the 1990 victims' rights statutes, i.e., Title V, Victims' Rights and Restitution Act, and Title II, Subtitles D and E, Victims of Child Abuse Act, together with the Victim and Witness Protection Act of 1982, provide the federal criminal justice system with enhanced statutory responsibility to assist and protect crime victims and witnesses in a comprehensive and uniform manner.

C. Application

These Guidelines apply to those components of the Department of Justice engaged in the detection, investigation or prosecution of all federal crimes, and in the detention and incarceration of federal defendants. They are intended to apply in all cases in which individual victims are adversely affected by criminal conduct or in which witnesses provide information regarding criminal activity. While special attention shall be paid to victims of serious, violent crime, ALL victims and witnesses of federal crime who have suffered physical, financial, or emotional trauma shall receive the assistance and protection to which they are entitled under the law.

It should be noted that because of the nature of federal criminal cases it will often be difficult to identify the victims of the offense and, in many cases, there will be multiple victims. Sound judgment will, therefore, be required to make appropriate decisions as to the range of victim services and assistance given. However, Department of Justice personnel should err on the side of providing rather than withholding assistance. For example, in a large-scale federal fraud scheme case, it may be possible to extend victim services and assistance to a representative of the many victims of the fraud.

D. Definitions

For purposes of these Guidelines --

(1) The term "victim" means a person that has suffered direct or threatened, physical, emotional, or pecuniary harm as a result of the commission of a crime, including:

(a) in the case of a victim that is an institutional entity, an authorized representative of the entity; and

(b) in the case of a victim who is under 18 years of age, incompetent, incapacitated, or deceased, one of the following (in order of preference): a spouse; a legal guardian; a parent; a child;

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 34 - 21

a sibling; another family member; or another person designated by the court.

(2) Federal departments and state and local agencies, as entities, shall not be considered "victims" for the purposes of Articles III and IV of these Guidelines.

(3) The term "witness" means a person who has information or evidence concerning a crime and provides information regarding his/her knowledge to a law enforcement agency. Where the witness is a minor, the term "witness" includes an appropriate family member or legal guardian. The term "witness" does not include a defense witness or an individual involved in the crime as a perpetrator or accomplice.

(4) The term "serious crime" (as used in the VWPA of 1982) means a criminal offense that involves personal violence, attempted or threatened personal violence, or significant property loss.

(5) The term "financial" or "pecuniary" harm shall not be defined or limited by a dollar amount, thus the degree of assistance must be determined on a case-by-case basis. For example, since victims' means vary, that which constitutes a minimal financial loss for one might represent a devastating loss for another.

SKIP D(6), p. 3.

(7) The term "child" means a person who is under the age of 18, who is alleged to be --

(a) a victim of a crime of physical abuse, sexual abuse, or exploitation; or

(b) a witness to a crime committed against another person.

(8) The term "child abuse" means the physical or mental injury, sexual abuse or exploitation, or negligent treatment of a child. The term "child abuse" does not include, however, discipline administered by a parent or legal guardian to his or her child provided it is reasonable in manner and moderate in degree and otherwise does not constitute cruelty.

(9) The term "physical injury" includes lacerations, fractured bones, burns, internal injuries, severe bruising, or serious bodily harm.

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 34 - 22

(10) The term "mental injury" means harm to a child's psychological or intellectual functioning which may be exhibited by severe anxiety, depression, withdrawal or outward aggressive behavior, or a combination of those behaviors, which may be demonstrated by a change in behavior, emotional response, or cognition.

(11) The term "sexual abuse" includes the employment, use, persuasion, inducement, enticement, or coercion of a child to engage in, or assist another person to engage in, sexually explicit conduct; or the rape, molestation, prostitution, or other form of sexual exploitation of children; or incest with children.

(12) The term "sexually explicit conduct" means actual or simulated--(A) sexual intercourse, including sexual contact in the manner of genital-genital, oral-genital, anal-genital, or oral-anal contact, whether between persons of the same or of opposite sex; sexual contact means the intentional touching, either directly or through clothing, of the genitalia, anus, groin, breast, inner thigh, or buttocks of any person with an intent to abuse, humiliate, harass, degrade, or arouse or gratify sexual desire of any person; (B) bestiality; (C) masturbation; (D) lascivious exhibition of the genitals or pubic area of a person or animal; or (E) sadistic or masochistic abuse.

(13) The term "exploitation" means child pornography or child prostitution.

(14) The term "negligent treatment" means the failure to provide, for reasons other than poverty, adequate food, clothing, shelter, or medical care so as to seriously endanger the physical health of a child.

(15) The term "multidisciplinary child abuse team" means a professional unit composed of representatives from health, social service, law enforcement, and legal service agencies to coordinate the assistance needed to handle cases of child abuse.

ARTICLE II. CRIME VICTIMS' BILL OF RIGHTS

A. Victims' Rights (Sec. 502(a))

BEST EFFORTS TO ACCORD RIGHTS. The Act provides that officers and employees of the Department of Justice and other departments and agencies of the United States engaged in the

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 34 - 23

detection, investigation, or prosecution of crime shall make their best efforts to see that victims of crime are accorded the rights described in the Act.

B. BILL OF RIGHTS OF CRIME VICTIMS (Sec. 502(b))

A crime victim has the following rights:

- (1) The right to be treated with fairness and with respect for the victim's dignity and privacy.
- (2) The right to be reasonably protected from the accused offender.
- (3) The right to be notified of court proceedings.
- (4) The right to be present at all public court proceedings related to the offense, unless the court determines that testimony by the victim would be materially affected if the victim heard other testimony at trial.
- (5) The right to confer with attorney for the Government in the case.
- (6) The right to restitution.
- (7) The right to information about the conviction, sentencing, imprisonment, and release of the offender.

B. Mandatory Reporting of "Best Efforts"

In the spirit of full compliance with these Guidelines, each United States Attorney, Department Chief of Litigation, FBI Special Agent in Charge (through the Director, FBI) as well as each responsible official of the Department's investigating field offices and correctional facilities, shall report annually to the Attorney General, through the Director, Office for Victims of Crime, by November 1st of each year, on the "Best Efforts" they have made during the preceding fiscal year, in ensuring that victims of crime are accorded the rights set out in the Act.

The responsible official, in preparing the annual "Best Efforts" Report, shall include an account of practices and procedures which have been adopted (and are in actual use in each of their respective offices) during the preceding fiscal year, to provide the services to victims mandated under the Act.

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 34 - 24

C. Performance Appraisal

The Attorney General strongly recommends that the annual performance appraisal of each federal law enforcement officer, investigator, prosecutor, and corrections officer (and appropriate staff of those agencies) include, as a required activity, implementation of and compliance with the victims' rights and victims and witnesses services provisions set forth in these Guidelines. Institution of this recommendation should be included in the annual "Best Efforts" Report.

ARTICLE III. SERVICES TO VICTIMS AND WITNESSES

As a general rule, for purposes of this Article, Investigative components will be responsible for C(1), (2), and (3), D(1), (2), (3)(a)(b), (5) and (6); prosecutorial components will be responsible for D(3)(c)-(h), and (4); and correctional components will be responsible for D(7) and (8).

Accordingly, at each stage in the performance of services, the transition of responsibility from one component of the Department of Justice to the next must, of necessity, include a sharing of information (in many cases PRIOR to the actual turning over of responsibility). In this way, gaps in notification and other services are eliminated and crime victims receive uniform rather than fragmented treatment, starting from the initial investigation and continuing throughout their entire involvement with the federal criminal justice system.

A. Designation of Responsible Officials (Sec. 503(a))

For purposes of these Guidelines, the Attorney General makes the following designations of persons who will be responsible for identifying the victims of crime and performing the services described in the VRRRA, section 503(c), at each stage of a criminal case;

INVESTIGATION

For cases under investigation, and in which no charges have yet been instituted, application of this section will be the responsibility of the following officials:

- (1) With respect to offenses under investigation by the Federal Bureau of Investigation, the responsible official shall be

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 34 - 25

the Special Agent in Charge of the division having primary responsibility for conducting the investigation;

SKIP A. Investigation (2)-(4), Prosecution, Custodial and Corrections, p.7-8.

B. Delegation and Coordination

In order to implement the requirements of the Act, there must be one individual who shall be designated specifically to carry out victim-witness services in each Department of Justice investigating field office and correctional facility, U. S. Attorney's Office, and Justice Department litigating division. This person shall be delegated authority by the responsible official to carry out the activities enumerated in these Guidelines.

It is incumbent upon responsible officials to ensure that all components of the Department of Justice cooperate with each other to the maximum extent possible in providing victims the services to which they are legally entitled. In many instances where certain duties and responsibilities overlap, the responsible officials must take all steps necessary to require coordination and interagency teamwork.

Moreover, all components shall work with appropriate components of other federal agencies that investigate and prosecute violations of federal law to assist them in providing these services to victims; and shall coordinate their victim-witness service efforts with state and local law enforcement officials, including tribal police officials in Indian Country and victim assistance and compensation service providers.

C. Identification of Victims (Sec. 503 (b))

"At the earliest opportunity after the detection of a crime," the responsible official of the investigative agency shall make reasonable and diligent efforts to:

- (1) identify the victims of a crime;
- (2) inform the victims of their right to receive, on request, the services described in the Act; and
- (3) inform each victim of the name, title, business address, and telephone number of the responsible official to whom such

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 34 - 26

a request for services should be addressed.

Within the meaning of this Article, "the earliest opportunity" means one that will not interfere with an investigation or hamper the responsible official in the performance of other law enforcement responsibilities.

In order to comply with the above informational requirements, it is recommended that a printed brochure, containing general information, brief description of rights and available services as well as the names and phone numbers of key officials and Victim-Witness Coordinator, be given to victims as soon as identified. Whenever possible, personal contact should be initiated with victims. Institution of this recommendation should be included in the annual "Best Efforts" Report.

D. Description of Services (Sec. 503 (c))

(1) "At the earliest opportunity after detection of a crime," the responsible official of the investigative agency shall make reasonable and diligent efforts to inform crime victims concerning:

(a) the place where the victim may receive emergency medical and/or social services;

(b) compensation or restitution for which the victim may be entitled under this or any other applicable law; and the manner in which such relief may be obtained. (see article VI, "Restitution"; see also Appendix, under "Compensation"); and

(c) the availability of public and private programs which provide counseling, treatment and other support to the victim.

(d) The responsible official shall, to the extent deemed necessary and feasible, assist the victim in contacting the specific person or office which will provide the above services.

(2) Consistent with the provisions of Title 18, USC, Sections 3521-3528, the responsible official shall make the necessary and appropriate arrangements to enable victims and witnesses to receive reasonable protection against threat, harm and intimidation from a suspected offender and persons acting in concert with or at the behest of a suspected offender.

Moreover, information on the prohibition against

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 34 - 27

intimidation and harassment and the remedies therefor shall routinely be made available to victims and witnesses. The responsible official shall, if warranted, advise the component of the Justice Department having the enforcement responsibilities (e.g., the U.S. Marshals Service) of instances involving intimidation or harassment of any victim or witness.

(3) During the investigation and prosecution of a crime, (IF the victim or witness has provided a current address or telephone number) a responsible official shall make diligent and reasonable efforts to consult with and provide the victim or witness "the earliest possible notice" concerning:

(a) the status of investigation of the crime, to the extent it is appropriate and will not interfere with the investigation, including the decision not to seek an indictment or otherwise commence a prosecution;

(b) the arrest of a suspected offender;

SKIP D(3) c-h & D(4), p.10-11.

(5) At all times, the responsible official shall take appropriate action to ensure that any property of a victim that is being held as evidence is maintained in good condition and returned to the victim as soon as it is no longer needed for evidentiary purposes.

(6) The Department of Justice-designated responsible official, or the head of another department or agency that conducts an investigation of a sexual assault shall pay, either directly or by reimbursement of payment by the victim, the cost of a physical examination of a victim and the costs of materials used to obtain evidence.

SKIP D(7)-(8), p.11.

ARTICLE IV. OTHER SERVICES

In addition to the services described above, other appropriate assistance should be extended to victims and witnesses, to the extent feasible, as follows:

A. Federal prosecutors shall resist attempts by the defense to obtain discovery of the names, addresses and phone numbers of victims and witnesses. Responsible officials and employees should

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 34 - 28

also avoid disclosing the names, addresses and phone numbers of victims and witnesses.

In cases involving a witness who has been promised anonymity or who operated in an undercover capacity, federal prosecutors should consult with such witness, and the primary law enforcement agency involved in the case, before disclosing the identity, address, or location of any such witness, and shall not make such disclosure without the consent of the witness and the law enforcement agency.

B. Upon request by a victim or witness, the responsible official should assist in notifying:

- the employer of the victim or witness if cooperation in the investigation or prosecution causes his/her absence from work; and
- the creditors of the victim or witness, where appropriate, if the crime or cooperation in its investigation or prosecution affects his/her ability to make timely payments.

C. Responsible officials should establish programs to assist Department of Justice employees who are victims of crime.

D. Victims and witnesses should be provided information or assistance with respect to transportation, parking, translator services and related services.

SKIP ARTICLE V. Victim Impact Statement, p. 12-13.

SKIP ARTICLE VI. Restitution, p. 13-14.

ARTICLE VII. CHILD VICTIMS' AND CHILD WITNESSES' RIGHTS

A. Statement of Purpose

The Victims of Child Abuse Act of 1990 (VCAA) was enacted in response to the alarming increase of suspected child abuse cases made each year (over 2 million reports each year). In such cases, because the investigation and prosecution of child abuse is extremely complex, too often the system had not paid sufficient attention to the needs and welfare of the child victim, thus aggravating the trauma that the child had already experienced. Therefore, in order to address this nationwide emergency, the 1990 VCAA provides, inter alia, authorization for training and technical assistance to judges, attorneys and others involved in state and federal court child abuse

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 34 - 29

cases; requires certain professionals to report suspected cases of child abuse under federal jurisdiction; and amends the United States criminal code to ensure protection of children's rights in court and throughout the criminal justice system.

The new landmark procedures codify specific "rights" for children, never before legally recognized in federal court, and allow other important accommodations for children, including: the right of a child to have an adult attendant accompany the child during court testimony; allowance of the use of closed-circuit television and videotaped depositions of children, as alternatives to live, in-court testimony; stringent procedures which protect a child witness' privacy as well as sanctions for violating such procedures; and a requirement disallowing routine competency examinations, except upon written motion that compelling reasons exist, and ruling out age as a compelling reason. The goal of this Article is intended to assist every federal law enforcement officer, investigator, and prosecutor to take necessary and valid action to reduce the trauma to the child victim caused by the criminal justice system while at the same time increasing the successful prosecution of child abuse offenders.

These Guidelines shall serve to ensure full implementation of the VCAA by all investigative, prosecutorial and correctional components of the Department of Justice.

B. Investigation/Interviewing of Child Victims

(1) Reporting and Investigation of Suspected Cases of Child Abuse.

(a) Pursuant to Sec. 226, Subtitle D, VCAA, certain professionals working on federal land, or in a federally operated or contracted facility, in which children are cared for or reside, are required to report suspected child abuse to an investigative agency designated to receive and investigate such reports. The statute provides further that the Attorney General shall designate the agency to receive and investigate these reports of suspected child abuse. By formal written agreement, the designated agency may be a nonfederal agency.

STANDARD REPORTING FORM. In every federally operated (or contracted) facility and on all federal lands, a standard written reporting form, with instructions, shall be disseminated to all mandated reporter groups. Use of this form shall be encouraged, but its use shall not take the place of the immediate making of oral reports, telephonically or otherwise, when circumstances dictate.

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 34 - 30

REFERRAL TO LAW ENFORCEMENT. When such reports are received by social services or health care agencies, and involve allegations of sexual abuse, serious physical injury, or life-threatening neglect of a child, there shall be an immediate referral of the report to a law enforcement agency with authority to take emergency action to protect the child. All reports received shall be promptly investigated, and whenever appropriate, investigations shall be conducted jointly by law enforcement and social services personnel (or multidisciplinary team) with a view toward avoiding multiple interviews with the child. In addition, it is important that a child victim be referred for a medical examination, if warranted, by a physician with expertise in forensic examinations.

REPORTING IN INDIAN COUNTRY. As noted earlier, a separate statute, the Indian Child Protection and Family Violence Prevention Act, PL 101-630 (November 28, 1990), governs reporting of child abuse in Indian Country. Pursuant to its provisions, certain professionals are required to report suspected child abuse to the "local law enforcement agency." Title 18, USC, Section 1169. These terms are defined in section 1169 to mean the federal, state or tribal agency that has the primary responsibility for child protection or the investigation of child abuse within the portion of Indian Country involved. Furthermore, where the report indicates the victim or abuser is an Indian and a preliminary inquiry indicates a criminal violation has occurred, the local enforcement agency, if other than the Federal Bureau of Investigation, must report the occurrence immediately to the Federal Bureau of Investigation.

(2) Mandatory Training for all Reporter Groups.

(a) The responsible official of the designated investigative agency shall provide to all mandated reporter groups of covered professionals training in their statutory obligation to report and in the identification of abused children.

(b) Sanctions for Failure to Report. The statute also provides that a covered professional who, while working on federal land or in a federally operated (or contracted) facility, in which children are cared for or reside, learns of facts that give reason to suspect that a child has suffered an incident of child abuse, but fails to report, shall be guilty of a Class B misdemeanor. Title 18, USC, Section 2258.

(3) Interviewing Procedures to Reduce Trauma to Child.

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 34 - 31

The responsible official, in coordination with the U. S. Attorney, shall provide training to all federal investigators on multidisciplinary methods of interviewing victims of child abuse and sexual child abuse. The responsible official may follow the criteria, set out in Sec. 212(b), Subtitle A, VCAA, recommended for state grant recipients to develop and implement multidisciplinary child abuse investigation programs including:

- a written agreement between local law enforcement, social service, health, and other related agencies to coordinate child abuse investigation;

- joint initial investigative interviews of child victims by law enforcement, health, and social service agencies;

- a requirement that, to the extent practicable, the same agency representative who conducts and initial interview conduct all subsequent interviews; and

- coordination of each step of the investigation process to minimize the number of interviews that a child victim must attend.

Where multidisciplinary teams are not yet formally established, federal investigators should coordinate with existing child protective service agencies to reasonably protect children at risk from further abuse.

C. Prosecution of Child Abuse Cases

SKIP C(1) - C(3), p.17-21.

(4) Privacy Protection of Child Witnesses and Child Victims.

Stringent procedures for protecting the privacy of a child victim or witness and ensuring the confidentiality of information received concerning a child victim or witness, include inter alia: filing under seal all documents which disclose the names of or identifying information concerning child victims and child witnesses, and redacting such names and identifying information from any publicly disclosed documents.

SANCTIONS FOR VIOLATIONS OF RULE REGARDING DISCLOSURE.

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 34 - 32

A knowing or intentional violation of the privacy protection accorded children pursuant to Section 3509 of Title 18, USC, is a CRIMINAL CONTEMPT punishable by not more than one year's imprisonment, or fine, or both. Title 18, USC, Section 403.

SKIP C(5) - C(11), p. 22-24

ARTICLE VIII. MANDATORY TRAINING - VICTIMS'/CHILD VICTIMS' AND WITNESSES' RIGHTS

It shall be mandatory for all components of the Department of Justice covered by these Guidelines to provide training to all presently employed and new attorneys, investigators, law enforcement, and corrections officers concerning their responsibilities in carrying out the provisions of the Victim and Witness Protection Act of 1982, Victims Rights and Restitution Act of 1990, and the Victims of Child Abuse Act of 1990, and to provide written instructions to appropriate subcomponents to ensure that these laws are implemented.

In addition, all training units conducted or supported by the Department of Justice shall develop programs which address victim assistance from the perspective of the personnel they train. These units include the FBI Academy at Quantico, the Attorney General's Advocacy Institute, the Federal Law Enforcement Training Center at Glynco, Georgia (through agreement with the U.S. Department of Treasury), and field training conducted by the FBI and DEA.

Compliance with this training requirement shall be included in the agency's annual "Best Efforts" Report.

The Office for Victims of Crime shall be responsible for coordinating training programs, in conjunction with all components of the Department of Justice, with respect to victims and witnesses of federal crime, including child witnesses and victims of child abuse.

ARTICLE IX. NONLITIGABILITY

These Guidelines provide only internal Department of Justice guidance. They are not intended to, do not, and may not be relied upon to create any rights, substantive or procedural, enforceable at law by any person in any matter civil or criminal. These Guidelines shall not be construed to create, enlarge, or imply any duty or obligation to any victim, witness or other person for which the United States or its employees could be held liable in damages. Nor are any limitations hereby placed on otherwise lawful litigative prerogatives of the Department of Justice.

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 34 - 33

| Signed August 6, 1991, by Dick Thornburg, Attorney General. |

EFFECTIVE: 09/08/94

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 35 - 1

SECTION 35. FBI AUTOMATED DATA PROCESSING AND
TELECOMMUNICATIONS (ADPT) SECURITY POLICY

35-1 PURPOSE (See MIOG, Part I, 261-2.)

The purpose of this document is to establish uniform policy, responsibilities, and authorities for the implementation of the FBI's Automated Data Processing and Telecommunications (ADPT) Security Program.

EFFECTIVE: 07/26/95

35-2 ADPT SECURITY PROGRAM REFERENCES

References to various regulations/laws applicable to the responsibilities of ADPT security-related personnel are located in Section 35-11.

EFFECTIVE: 07/26/95

35-3 DEFINITION OF TERMS

A glossary of terms is included as Section 35-12.

EFFECTIVE: 07/26/95

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 35 - 2

35-4 SCOPE

(1) The provisions of this policy apply to all FBI personnel, all FBI ADPT systems, networks and support facilities, and to contractors acting on behalf of the FBI. This policy also applies to any outside organizations, or their representatives, who are granted access to the FBI's ADPT system resources, such as other federal agencies and Joint Task Force members.

(2) Microprocessors which are embedded in and dedicated strictly to production/process control, such as laboratory equipment, are excepted.

(3) The Information Systems Security Unit (ISSU), Security Countermeasures Section, National Security Division, is the point-of-contact for questions concerning this policy document.

EFFECTIVE: 07/26/95

35-5 BACKGROUND

(1) The FBI develops a strategic plan each year which represents a commitment to carry out its mission with increasing effectiveness and efficiency. Information technology is an essential supporting element to the FBI's mission. Employees worldwide use ADPT systems for all facets of the Bureau's operations. These ADPT services also support law enforcement personnel and agencies outside the FBI.

(2) In keeping with the FBI's mission, the goal of the FBI's ADPT security program is to establish and maintain effective security countermeasures to ensure the data confidentiality, integrity, and operational availability of all FBI ADPT systems that process, store, or transmit classified and sensitive but unclassified (hereafter referred to as sensitive) information. In essence, this policy applies to all FBI Systems, given that all Bureau information is treated as at least sensitive. Moreover, Bureau information is not releasable except through the Freedom of Information/Privacy Acts (FOI/PA) process.

(a) The Bureau's ADPT security program has been

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 35 - 3

designed to address the compromise of information processed in ADPT systems: (a) through penetration by hostile intelligence services and/or criminal elements; (b) by otherwise legitimate users who gain access to data or processes for which they are not authorized; or (c) as a result of inadequate security design, implementation, or operation.

(b) The security countermeasures must preserve the integrity of the information processing to ensure the data is accurate and relevant to achieve the FBI's investigative, law enforcement, and administrative support requirements. Inaccurate data could lead to uninformed decisions and adversely impact the FBI's mission.

(c) Required ADPT services should be available to authorized users within their operational time constraints. The security controls should also make the services unavailable to unauthorized users.

(3) The scope of this policy document is ADPT security, including applicable life cycle security requirements. Several related programs should be taken into consideration when establishing and reviewing ADPT security requirements. Policies and procedures covering the related programs listed below are in this policy by reference (see Section 35-11) and should be obtained by contacting the appropriate program manager.

(a) The Security Countermeasures Section (SCMS), National Security Division (NSD) prescribes policy, procedures, and specifications for maintaining facility security for the FBI. The SCMS is also responsible for the FBI's information security, personnel security, and industrial security programs.

(b) The FBI Central Office of Record (FBICOR) is responsible for setting policy for handling FBI communications security (COMSEC) materials and equipment and for establishing standards and procedures for granting authorization to FBI employees for access or use of those materials and equipment. The FBICOR also evaluates and approves cryptography and communications security measures to be used in ADPT systems.

(c) The Freedom of Information-Privacy Acts (FOIPA) Section, Information Resources Division sets policy for the FBI's FOIPA programs.

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 35 4

EFFECTIVE: 07/26/95

35-6 GENERAL POLICY

(1) Classified and sensitive information in FBI ADPT systems must be safeguarded against unauthorized disclosure, modification, access, use, destruction, or delay in service. An FBI ADPT system is a telecommunications or automated information system that is owned, leased, or operated by or on behalf of the FBI.

(2) The minimum security requirements identified in this policy shall be implemented to protect classified and sensitive information processed, stored, or transmitted by FBI ADPT systems and to protect FBI ADPT system resources.

(3) All ADPT systems processing, storing, or transmitting classified or sensitive information must be submitted for accreditation. Prior to processing, storing, or transmitting classified information, ADPT systems must be accredited. (See Section 35-8.2.) ADPT systems used to process, store, or transmit sensitive information must be accredited as expeditiously as possible.

(4) Connectivity is prohibited between internal FBI ADPT systems and all other systems or networks not covered under the FBI's management authority without approval of the appropriate FBI accrediting authority.

(5) All FBI ADPT systems are for official business only. System users have no expectation of privacy while utilizing these resources.

EFFECTIVE: 07/26/95

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 35 - 5

35-7 ROLES AND RESPONSIBILITIES

(1) The Director, FBI, is responsible for the security of all ADPT systems under his purview and authorizes the implementation of ADPT security countermeasures based on national policy and guidance. The Director is also responsible for:

(a) Certifying annually to the Department Security Officer (DSO) the adequacy of ADPT systems security in the FBI.

(b) Ensuring a computer security education, training, and awareness program is established in the FBI.

(c) Ensuring all ADPT system security plan documentation is maintained as defined in Section 35-8.1.2.

(d) Designating senior executive service personnel accreditation authority for sensitive and classified computer systems in the FBI. (See (3)(g).)

1. The Assistant Director, NSD, per Director of Central Intelligence Director (DCID) 1/16, has been designated as the accreditation authority for all systems processing, storing, or transmitting sensitive compartmented information (SCI).

2. The Security Programs Manager (SPM), SCMS, NSD, has been designated as the accreditation authority for all classified systems other than those processing, storing, or transmitting SCI, and for all sensitive systems.

(2) The FBI's SPM, SCMS, NSD is responsible for the day-to-day administration of all security programs for the FBI, including the ADPT security program as follows:

(a) Accrediting all classified systems other than those processing, storing, or transmitting SCI and all sensitive systems.

(b) Implementing the FBI's ADPT security education, training, and awareness program on behalf of the Director, FBI.

(c) Submitting security violation reports to the DSO, which include a damage assessment and any actions taken to prevent future violations.

(3) The FBI's ADPT Security Officer, ISSU, SCMS, NSD, has

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 35 - 6

been appointed by the Director, FBI, to facilitate the implementation of the FBI's ADPT security program, and has the following responsibilities:

(a) Ensuring an operational ADPT security program is in place that asserts a centrally administered security policy. The ADPT security program must comply with the minimum security requirements defined in federal and departmentwide mandates while preserving the flexibility of operations inherent in the Bureau's mission.

(b) Developing and promulgating ADPT security program policy for the FBI. Interpreting policy relating to the FBI ADPT security functions and developing FBI unique guidance as required. Assisting FBI components and their representatives with their efforts to comply with these policies during the performance of their duties, by providing explanation or clarification of ADPT security-related questions that may have an impact on mission performance.

(c) Ensuring the appointment of Computer Systems Security Officers (CSSOs) for classified and sensitive FBI ADPT systems and providing the CSSOs with assistance.

(d) Reviewing and approving acquisitions, in coordination with the CSSO and certifying that the appropriate ADPT security requirements defined in this document are included in the specifications for the operation of an ADPT installation facility, equipment, application system, or acquisition of ADPT hardware, software or related services.

(e) Providing the CSSO with direction and guidance in defining and approving security requirements prior to the start of formal development of software.

(f) Approving the security requirements prior to the start of formal development of software.

(g) Ensuring accreditation packages are prepared for all ADPT systems under FBI authority that process, store, or transmit sensitive or classified information. The contents of an accreditation package are described in Section 35-8.2.

1. Providing guidance on the scope and contents of the system security plans.

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 35 - 7

2. Reviewing system security plans prepared by or on behalf of the System CSSOs.

3. Preparing statements of residual risk and summary statements of compliance to complete each accreditation package.

4. Submitting the accreditation package to the appropriate accreditation authority, as defined in Section 35-7(1)(d), for accreditation.

5. Acting as a liaison to the DSO and the Department's Justice Management Division, Information Resources Management, Security Programs Manager (IRM-SPM) for all ADPT security matters.

(h) Maintaining a record system containing the status of all accreditation documentation required in this policy document.

(i) Administering the Bureau's security incident reporting program, on behalf of the SPM, to include establishing reporting criteria and coordinating with DOJ.

(j) Coordinating the FBI's virus prevention program, to include: recommending virus prevention solutions; providing guidance in defining the requirements; and selecting the approach.

(k) Conducting ADPT security policy compliance review and oversight activities, as discussed in Section 35-8.4.

(l) Establishing and maintaining a program for conducting periodic facility risk analyses.

(m) Establishing standards and guidance for the preparation of ADPT Installation Disaster and Continuity Plans. Conducting Bureauwide analyses and establishing and verifying Bureau strategies for business recovery and alternate processing. Coordinating the development of ADPT Installation Disaster and Continuity Plans for FBI ADPT facilities.

(n) Establishing standards and guidance for preparing End-User ADPT Contingency Plans.

(o) Identifying areas or issues requiring ADPT security-related research and development effort.

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 35 - 8

(4) The head of each FBI Division (the Legal Attaches for each Legal Attache office) is responsible for all aspects of ADPT security under his/her jurisdiction. These responsibilities shall be delegated to the Security Countermeasures Program Manager (SCMPM), as set forth in MIOG, Part I, Section 261. In addition, the sponsor of each FBI ADPT system or major application shall ensure that a CSSO is appointed and that this appointment is documented in the system security plan.

(5) The SCMPM shall assume the responsibility for the implementation of ADPT security for a division or Legal Attache. The SCMPM may delegate the day-to-day implementation of the security responsibilities to other members of the division, but will remain the primary point-of-contact for ADPT security matters for the division. Responsibilities include:

(a) Implementing ADPT security policy for ADPT resources that are under the direct operational responsibility of the division.

(b) Enforcing the security policy and ADPT security countermeasures on all personnel who develop, manage, operate, maintain, or use a division's ADPT resources.

(c) Acting as the point-of-contact for security discussions with the FBI's ADPT Security Officer.

(d) Ensuring all employees under his/her jurisdiction receive computer security awareness training, as discussed in Section 35-8.3, following the guidance of the SPM. Promoting general operational ADPT security awareness within his/her organization.

(e) Reporting immediately to the ADPT Security Officer any security incidents, such as any attempt to gain unauthorized access to information, virus infection, or other event affecting the systems security.

(f) Ensuring End User ADPT Contingency Plans are developed, in accordance with Section 35-8.1.4, to ensure continued operations of essential functions within the division in the event that ADPT support is interrupted.

(g) Advising his/her management on implementation of provisions of this policy and applicable references.

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 35 - 9

(h) Ensuring all ADPT operations are conducted as accredited or that accreditation packages are prepared for operations not covered under existing accreditations. Accreditation is discussed in Section 35-8.2.

(i) Maintaining a list of non-Bureau individuals with access to FBI systems and ensuring whenever a change in SAC occurs, the incoming SAC reevaluates access granted to non-Bureau individuals.

(j) Establish a program that will check on a monthly basis with squads hosting non-Bureau individuals the need for continued access to FBI systems.

(6) A Computer Systems Security Officer (CSSO) shall be assigned for each FBI ADPT system. The CSSO is responsible for:

(a) Ensuring that new ADPT systems, whether acquired or developed, are implemented with appropriate security features and meet the minimum requirements defined in this policy.

1. Defining security requirements prior to starting formal development of a new ADPT system, in coordination with the ADPT Security Officer.

2. Reviewing acquisitions in coordination with the ADPT Security Officer, to ensure that the appropriate ADPT security requirements defined in this policy are included in the specifications of an ADPT installation facility, equipment, application system or acquisition of ADPT hardware, software or related services.

3. Reviewing ADPT systems whenever changes occur, or at least every three years, to ensure changes have not occurred which affect the accreditation status. Conducting design reviews and system tests, and certifying the results recorded, for all new software and for existing software when significant modifications are made. Section 35-8.2 discusses the types of changes that may affect the accreditation status of an ADPT system.

4. Identifying and recommending to management security improvements for the ADPT system.

5. Ensuring that configuration control mechanisms are used and maintained to protect the security-related

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 35 - 10

features of an ADPT system.

(b) Preparing or overseeing the preparation of system security plans, as discussed in Section 35-8.1, and maintaining the documentation for each ADPT system under his/her assigned responsibility.

(c) Coordinating the preparation and review of the system security plan with the ADPT Security Officer. The required steps in the approval process are discussed in Section 35-8.1.1.

(d) Ensuring the distribution of standard security procedures tailored for end users and operators of computer systems. Advising users of the security features and procedures used on the ADPT system.

(e) Coordinating with the appropriate CSSOs of other systems and/or the FBI's ADPT Security Officer to ensure that planning for shared resources adequately addresses the security requirements that are relevant to each system.

(f) Establishing access control criteria and administrative procedures, which are discussed in Section 35-9.4.1, consistent with Bureau policy, by which only authorized persons can gain access to the ADPT system. The criteria will identify authorized users and identify responsibility for approving all access to the system. The procedures will identify the access control mechanisms and assign responsibility for administering the mechanisms.

(g) Ensuring the review of audit trails and the thorough investigation of audit trail discrepancies, in accordance with the review cycle defined in the system security plan.

(h) Reporting immediately to the Security Countermeasures Program Manager any security incident, such as an attempt to gain unauthorized access to information, virus infection, or other event affecting the system's security.

(7) The Section Chief of the Technical Operations Section, Information Resources Division is responsible for providing policy and guidance on Technical Surveillance Countermeasures (TSCM), intrusion detection, and emanations security.

(8) The Unit Chief of the Network and Information Systems Support Unit (NISSU), Operations Management Section, Information Resources Division is responsible for providing policy and guidance on

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 35 - 11

the telecommunication-related construction of facilities to meet national standards for emanations security.

(9) All persons who use, manage, operate, maintain, or develop classified or sensitive FBI ADPT systems must comply with this policy.

EFFECTIVE: 11/28/97

35-8 ADPT SYSTEMS SECURITY LIFE CYCLE

(1) This section of the ADPT security policy documents activities relating to ADPT system acquisition and development. Whereas activities pertaining to system development and acquisition have traditionally been centrally conducted by Headquarters elements, the FBI's existing and planned ADPT system technology affords the opportunity for decentralized system development activities. It is imperative that all personnel are aware that, whereas this policy does not discourage systems development, it provides guidance to ensure that ADPT systems that are developed, acquired, and documented are in compliance with this policy.

(2) The topics in this Section are applied as follows:

(a) Security Planning. Security planning activities are the responsibility of the sponsor of an ADPT system, the SCMPM, the CSSO, the ADPT Security Officer, and the SPM. These activities pertain to the development or acquisition of new FBI ADPT systems or modifications to existing systems.

(b) Accreditation. Accreditation activities are the responsibility of the CSSO, the ADPT Security Officer, the SPM, and the accrediting authority.

(c) Security Education, Training, and Awareness. These activities apply to all personnel who manage, use, or operate an FBI ADPT system, whether they are FBI employees or not. These activities are ongoing.

(d) Security Oversight. Security oversight activities related to this policy are conducted by the ADPT Security Officer, the SCMPM, the CSSO, the SPM, and the Inspection Division.

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 35 - 12

| These activities are ongoing.

EFFECTIVE: 07/26/95

| 35-8.1 Security Planning (See MIOG, Part II, 35-7.)

Security planning activities support the accreditation of all classified and sensitive ADPT systems. This section describes the activities and documentation required to achieve accreditation of a classified or sensitive FBI ADPT system and includes discussion of system security plans, risk management, contingency planning, certification, and system security procedures. The ADPT Security Officer should be consulted prior to the development or acquisition of a classified or sensitive system to establish the scope of the security-related activities and documentation required to achieve accreditation.

EFFECTIVE: 07/26/95

| 35-8.1.1 Approvals (See MIOG, Part II, 35-7.)

(1) Several steps in the security planning process require the CSSO to seek approvals to proceed with system planning activities.

(2) Security requirements shall be defined and approved by the CSSO and the ADPT Security Officer prior to the start of development or as part of the acquisition process.

(3) The ADPT Security Officer shall approve the system design based on the security reviews prior to the start of system development.

(4) The ADPT Security Officer shall approve the certification test plan and shall approve the results of the certification testing.

(5) DOJ approval of the system security planning

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 35 - 13

documentation is required prior to accreditation, as discussed in Section 35-8.2.

EFFECTIVE: 07/26/95

35-8.1.2 System Security Plan (See MIOG, Part II, 35-7 & 35-8.2.)

(1) The objective of system security planning is to improve protection of information and information processing resources. The managers most directly affected by and interested in the information or processing capabilities must show that their information and processing capabilities are adequately protected from loss, misuse, unauthorized access or modification, unavailability, or undetected activities.

(2) The boundaries of the computer system must be clearly defined by the CSSO. When a network is used by only the FBI, the FBI ADPT Security Officer will determine the boundaries. Comparable systems, operating in similar environments, may be included in a single system security plan. If additional security measures are required for a particular operating environment, they will be added as a supplement to the system security plan. While generic security plans lessen the administrative burden, CSSOs are responsible for ensuring the ADPT systems under their purview are operating in accordance with the approved system security plan. Local area networks (LANs), hosts with terminals, groups of stand-alone personal computers, workstations, and office automation systems located in the same general area and performing the same general functions, require only one system security plan.

(3) System security plan documentation is required for every classified and sensitive FBI ADPT system. The system security plan documents ADPT security requirements from development or acquisition, implementation, and operation to secure disposal. The system security plan is to be developed and maintained by the CSSO assigned to the ADPT system. The FBI ADPT Security Officer shall define the scope and contents of a system security plan for the FBI ADPT systems to ensure a standardized approach and to ensure compliance with applicable regulations. The system security plan should provide FBI management with sufficient information to make an assessment about the security posture of the ADPT system. The components of a system security plan are:

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 35 - 14

b2
(a) A security plan which includes the information described in Office of Management and Budget (OMB) Bulletin 90-08 or its successor and is implemented in forms provided by DOJ or using the guidelines for preparing an FBI system security plan. Any questions should be directed to the FBI ADPT Security Officer (ADPTSO), ISSU, SCMS, NSD, [REDACTED] Room 4282, FBIHQ. The ADPTSO can assist in identifying the mode of operation of the system, assessing the threats and vulnerabilities, estimating the risk involved in the operation, and identifying specific critical countermeasures and/or safeguards. A system security plan form is available in WordPerfect from the ADPTSO.

(b) Documented risk management actions pertaining to the ADPT system. Section 35-8.1.3 discusses the risk management process.

(c) Certification statement that reflects the results of certification tests of the security features applicable to the system. Section 35-8.1.5 discusses the certification process.

(d) Contingency plan which consists of an emergency response plan, backup operations plan, and post-disaster recovery plan. Section 35-8.1.4 discusses the contingency planning process.

(e) Standard security procedures for users and operators of the system. Section 35-8.1.6 discusses standard security procedures.

EFFECTIVE: 07/26/95

35-8.1.3 Risk Management (See MIOG, Part II, 35-8.1.2.)

(1) Risk management is the total process of identifying, controlling, and eliminating or minimizing uncertain risks that may affect system resources. Management must identify the resources to be protected and analyze the risks to determine the appropriate level of protection needed. The risk management process includes: risk analysis, as derived from an analysis of threats and vulnerabilities; management decision to implement security countermeasures and to accept residual risk; implementation and test of selected security countermeasures; and effectiveness reviews.

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 35 - 15

(2) A risk is derived from the analysis of threats and vulnerabilities. Formal risk analysis requires determining relativity among risks and assessing associated damage or loss. This relativity forms the basis for selecting effective security countermeasures. The FBI does not currently have a standardized methodology for conducting a risk analysis. The DOJ Simplified Risk Analysis Guideline, FIPS PUB 65, and the National Institute of Standards and Technology (NIST) PUB 500-174 provide guidance. The FBI ADPT Security Officer shall be consulted, prior to the start of the risk analysis process, for guidance on the scope of the analysis and the recommended approach to be taken.

(a) Risk analysis will be conducted/sponsored by the ADPT Security Officer for each FBI ADPT mainframe/network facility. The risk analysis procedure will be conducted when a new or substantially modified ADPT facility design is approved and will be conducted:

1. Prior to the approval of design specifications for new general support systems and their supporting installations.

2. Whenever a significant change occurs to the general support system (e.g., adding a local area network; changing from batch to on-line processing; adding dial-up capability). Criteria for defining significant change shall be commensurate with the sensitivity of the data processed by the general support system.

3. At periodic intervals established by the ADPT Security Officer commensurate with the sensitivity of the data processed, but not to exceed every three years if no risk analysis has been performed during that period.

(b) The CSSO shall conduct a risk analysis which focuses on the technical and administrative security control techniques associated specifically with the system under review, including the interface between the operating systems and the application and/or the communications environment and the application and the threats inherent in processing in a specific environment. The results of a facility risk analysis are taken into account when defining and approving security specification for the application systems or network systems.

(3) Responsibility for implementation of the recommendations of a risk analysis rests with the manager of the ADPT

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 35 - 16

system or facility under review. Response to the recommendations contained in the risk analysis shall include implementation time lines or rationale for nonimplementation of recommended security countermeasures. ADPT system managers must evaluate the recommendations made regarding the systems under review and determine whether to implement the recommendations based on technical and operational feasibility and cost. The FBI's accreditation authority will consider the effects of the reviewer's actions in making accreditation decisions.

EFFECTIVE: 07/26/95

35-8.1.4 Contingency Planning (See MIOG, Part II, 35-7(5), 35-8.1.2.)

(1) Each ADPT system or grouping of like systems must be supported by a logical contingency plan. Well-written contingency plans, routinely reviewed, tested and updated, will enable vital operations and resources to be restored as quickly as possible and keep system downtime to an absolute minimum, providing reasonable continuity of ADPT support if events occur that prevent normal operations.

(2) The elements to be addressed as part of contingency planning for all ADPT systems are:

(a) Emergency response procedures appropriate to fire, flood, civil disorder, natural disaster, bomb threat or any other incident or activity which may endanger lives, property or the capability to perform essential functions.

(b) Backup arrangements, procedures and responsibilities, to ensure that essential (critical) operations can be continued if normal processing or data communications are interrupted for any reason for an unacceptable period of time. The minimally acceptable level of degraded operation of the essential (critical) systems or functions will be identified and prioritized so that the contingency plan accomplishes the priorities.

(c) Post-disaster recovery procedures and responsibilities, to facilitate the rapid restoration of normal

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 35 - 17

operations at the primary site, or if necessary, at a new facility, following the destruction, major damage or other interruptions at the primary site.

(3) Facility Disaster Recovery Plans address the protection of FBI ADPT general support system security and resources and will ensure the availability of critical Bureau resources, facilitating the continuity of operations during the emergency. The objective of an ADPT Installation Disaster and Continuity Plan is to provide reasonable continuity of computer center/telecommunication information technology support should events occur which prevent normal operations. The ADPT Security Officer is responsible for developing ADPT Installation Disaster and Continuity Plans and defining the testing requirements which will be implemented by the CSSO.

(4) The CSSO shall develop and maintain in a current state, a contingency plan for each ADPT system, which will provide reasonable assurance that critical data processing support can be continued, or resumed quickly, if normal operations of the system are interrupted. The contingency planning activities for an application system are conducted in concert with facility disaster recovery planning and/or end-user contingency planning, when such plans exist. It should be noted that, depending on the results of the criticality assessment, the CSSO for a system may determine that the system is not critical enough to the division or user community to warrant developing and maintaining continuity of operations strategies for interim system processing until normal operations are resumed. In this event, the contingency plan will consist of a continuity of operations statement to that effect. This is subject to the approval of the accrediting authority.

(5) The Security Countermeasures Program Manager for a division is responsible for ensuring that End-User ADPT Contingency Plans are in place for his/her division's microcomputer ADPT resources. The plans also address the division's business continuity requirements for interfacing with applications supported by application contingency plans. The ADPT Security Officer provides guidance for the formulation of the plans. End-User ADPT Contingency Plans are to be developed and/or reviewed and updated periodically or whenever a major change occurs in the processing environment, which includes the physical site, hardware, software, and/or operating systems.

(6) All plans must be operationally tested at a frequency commensurate with the risk and magnitude of loss or harm that could

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 35 - 18

result from disruption of information processing support.

EFFECTIVE: 07/26/95

35-8.1.5 Certification (See MIOG, Part II, 35-8.1.2, 35-8.4, 35-9.3.2.)

(1) Certification is the comprehensive security test and evaluation of the technical and nontechnical security features of a computer system and other safeguards, made in support of the accreditation process, that establishes the extent to which a particular design and implementation meet a specified set of security requirements. Certification primarily addresses software and hardware security countermeasures, but must also consider procedural, physical, personnel, and emanations security to the extent that these measures are employed to enforce security policy.

(a) Custom developed software - Design reviews and systems tests will be performed, and a certification of the results recorded, for all newly developed software and for existing software when significant modifications are made.

(b) Commercial off-the-shelf software (COTS) - Commercially procured software shall be examined to assure that the software contains no features which might be detrimental to the security of the ADPT system. Security-related software shall be examined to ensure that the security features function as specified.

(2) The CSSO shall oversee or conduct certification tests of the computer system. If resources are available, individuals who conduct the certification testing should be independent of the system's developers. The results of the tests shall be documented in a format such that the tests can be repeated, if required, to achieve the results reflected in the certification report.

(3) The system security countermeasures should be modified to reflect the results of the certification testing, as appropriate.

(4) The extent of certification testing will vary with the security mode of operation of the system.

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 35 - 19

(a) For dedicated security mode of operation, the certification will focus on the physical, procedural, and personnel security measures that ensure all users have the appropriate clearance, access approval, and need-to-know for all data on the system. Since the system is not required to separate users and data with technical security measures, the certification effort will not be extensive.

(b) For the system high-security modes of operation, the certification must cover the same factors as for the dedicated security mode. In addition, testing must establish that the hardware and software security features reliably separate users from any data for which they do not have a need-to-know.

(c) For compartmented and multilevel security modes of operation, specific certification tests will be designed pending DOJ approval (as discussed in Section 35-8.2(1)(b)).

(5) Guidance on conducting these tests shall be provided by the ADPTSO.

EFFECTIVE: 07/26/95

35-8.1.6 Standard Security Practices (See MIOG, Part II, 35-8.1.2.)

System security procedures shall be developed and provided to all users and operators. The procedures shall explain how the security mechanisms in a specific ADPT system work, so that the users and operators are able to consistently and effectively protect their information. The procedures should also be addressed in user training.

EFFECTIVE: 07/26/95

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 35 - 20

35-8.2 Accreditation (See MIOG, Part II, 35-6, 35-7, 35-8.1.1, 35-9.4, 35-9.4.17.)

(1) Accreditation is an official management authorization to operate an ADPT system: in a particular mode of operation; with a prescribed set of security countermeasures; against a defined threat and with stated vulnerabilities and countermeasures; in a given operational environment; under a stated operational concept; with stated interconnection to other ADPT systems; and, at an acceptable level of risk for which the accrediting authority has formally assumed responsibility. The accrediting authority accepts security responsibility for the operation of an ADPT system and officially declares that a specified system will adequately protect information.

(a) The security processing mode of an ADPT system will be determined based on the classification or sensitivity and formal categories of data and the clearance, access approval, and need-to-know of the users of the system. Formal categories of data are those for which a written approval must be issued before access (for example, SCI compartments or special access programs). The available or proposed security features of the system are not relevant in determining the actual security mode. All ADPT systems will be accredited to operate in one of the following security modes of operation wherein the following statements are satisfied concerning users with direct or indirect access to the ADPT system, its peripherals, remote terminals, or remote hosts:

1. Dedicated Security Mode - all users possess the required personnel security clearance or authorization, formal access approval (if required), and need-to-know for all data handled by the ADPT system.

2. System High-Security Mode - all users possess the required personnel security clearances or authorization, but not necessarily a need-to-know, for all data handled by the ADPT system. If the ADPT system processes classified information, all users must have formal access approval and signed nondisclosure agreements for all the information stored and/or processed (including all compartments, subcompartments, and/or special access programs).

3. Compartmented Security Mode - all users possess a valid personnel security clearance for the most restricted information processed in the computers system; formal access approval for, and have signed nondisclosure agreements for that information to which they are to have access; and a valid need-to-know for that

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 35 - 21

information to which they are to have access.

4. Multilevel Security Mode - some users do not have a valid personnel security clearance for all the information processed in the ADPT system; all users have the proper clearance and have the appropriate formal access approval for that information to which they have access; and all users have a valid need-to-know for that information to which they are to have access.

(b) The dedicated security mode and the system high-security mode are the only modes of operation authorized by the Department for the processing of classified and sensitive information on ADPT systems. Exceptions to allow the operation of ADPT systems in the compartmented and multilevel security modes may be requested in writing from the DSO by the SPM. (See MIOG, Part II, 35-8.1.5(4).)

(2) All ADPT systems processing, storing, or transmitting classified or sensitive information must be submitted for accreditation. Prior to processing, storing, or transmitting classified information, ADPT systems must be accredited. ADPT systems used to process, store, or transmit sensitive information must be accredited as expeditiously as possible.

(3) The system security plan documentation discussed in Section 35-8.1.2 shall be submitted by the CSSO to the FBI ADPT Security Officer for review. The FBI ADPT Security Officer will develop a summary of compliance with security requirements and a statement of residual risk.

(4) The system security plan, summary of compliance, and statement of residual risk for classified systems must be reviewed by the DSO representative prior to accreditation. For sensitive systems, this documentation will be reviewed by the DOJ IRM-SPM representative prior to accreditation.

(5) The appropriate FBI accreditation authority, i.e., the Assistant Director, NSD, for SCI systems and the SPM for all other systems, makes the accreditation decision based on the summary of compliance, statement of risk, and approved system security plan. The accreditation process results in a decision that the ADPT system is:

(a) accredited to operate, or

(b) given an interim approval to operate for a specific time pending satisfaction of specified requirements, or

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 35 - 22

(c) denied permission to operate until the identified deficiencies or inadequacies are corrected.

(6) Every FBI ADPT system covered by this policy must be reaccredited every three years. The accreditation status and supporting accreditation documentation shall also be reviewed and revised as appropriate under the following circumstances:

(a) Significant changes in the hardware, software, or data communications configuration that impact security countermeasures defined in the original accreditation package. A significant change constitutes a change that needs to be brought to the attention of the accrediting authority.

(b) Changes in the sensitivity of the information processed.

(c) Changes in the security mode of operation.

(d) Relocation or structural modifications of the computer facility or remote terminal areas.

(e) A breach of security, reported violation of security, or unusual situation that appears to invalidate the accreditation.

(7) The accreditation package revision and review process will include:

(a) Accomplishment of the same steps required for the original accreditation package. Those portions of the package that are still valid need not be redone.

(b) The system security plan, summary of compliance, and statement of residual risk will have to be reviewed and approved by the DOJ IRM-SPM representative or DSO representative, as appropriate.

(c) The appropriate FBI accrediting authority will review and reaccredit the ADPT system.

(8) The FBI ADPT Security Officer shall maintain a record system containing the status of all of the documents in the accreditation packages for the FBI's systems.

(9) The accrediting authority for a system is the only

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 35 - 23

person authorized to exempt an operation from the security requirements specified in the accreditation statement. This exemption shall be formally documented and shall be retained with the original accreditation package.

EFFECTIVE: 07/26/95

35-8.3 Security Education, Training, and Awareness (See MIOG, Part II, 35-7(5), 35-9.2.)

(1) The ISSU, SCMS, NSD established an ADPT Security Education, Training, and Awareness Program for the FBI. This training shall be extended to all personnel who manage, use, or operate an FBI ADPT system, whether they are employed by the FBI or not. This includes Joint Task Force (JTF) members utilizing any FBI ADPT system (e.g., other federal, state, or local police personnel utilizing FBI microcomputers in an off-site), members of other federal agencies in non-JTF capacity, and any contractor personnel utilizing FBI ADPT systems. The goal of the training program is to ensure that these personnel are made aware of: threats, vulnerabilities, and risks associated with the ADPT systems; what requires protection; information accessibility, handling, marking, and storage considerations; physical and environmental considerations necessary to protect the ADPT system; system, data and access controls; contingency plan procedures; secure configuration control requirements; responsibility to promptly report security violations to the CSSO; and, responsibility to report to the SPM if the security training appears inadequate.

(2) All new employees will receive a security awareness briefing within 60 days of their appointment, as part of their orientation. Continuing training shall be provided whenever there is a significant change in the agency information systems security environment or procedures or when an employee enters a new position which deals with sensitive information. Refresher training shall be given as frequently as determined by the SCMPM, based on the sensitivity of the information that the employee uses or processes. All FBI employees will be provided with refresher awareness material or briefings at least annually.

(3) Each person receiving training shall complete a Notice of Responsibility and Computer Security Awareness Certification

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 35-24

upon completion of each training course which will be retained by the SCMPM. (See Section 35-13.1.) Guidance on the tracking of these training activities will be provided by ISSU, SCMS, NSD.

(4) ADPT security training above the awareness level shall be provided to all personnel who design, implement, or maintain systems regarding the types of security and internal control techniques that should be incorporated into system development, operation and maintenance. The division should consult with the ISSU, SCMS, NSD for guidance on achieving these training objectives.

EFFECTIVE: 07/26/95

35-8.4 Security Oversight (See MIOG, Part II, 35-7(3)(k).)

(1) The ADPT security program is implemented through several policy actions: appointment of CSSOs, acquisition reviews, review and approval of security requirements to support system development; preparation and approval of accreditation documentation; and security incident reporting.

(2) Given the global nature and participation of the FBI ADPT resources, the appointment of CSSOs to assist in ensuring adherence to and to provide a point-of-contact for accomplishing ADPT security activities has been established. CSSOs shall be appointed for all ADPT systems.

(3) The FBI's Inspection Division reviews ADPT security as part of a division's periodic inspection. The FBI ADPT Security Officer will coordinate with the Inspection Division on the status of ADPT security within a division upon completion of the inspection.

(4) Whenever an office makes a major move, e.g., relocates to a new building, the division's Security Countermeasures Program Manager should conduct a compliance review to determine whether the change in physical location has had an impact on the ADPT security posture. The Division's Security Countermeasures Program Manager should consult with the Security Countermeasures Section and should retain the results of the security review as part of the division's security documentation.

(5) As is current practice, the FBI shall continue to

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 35 - 25

enforce ADPT security as part of the acquisition process. The Information Systems Security Unit must approve ADPT-related acquisitions, as discussed in Section 35-8.1.5. The ISSU should maintain formal records of acquisition activities to ensure that security plans are either developed or modified to reflect the acquisitions. The ADPT Security Officer reviews and approves all ADPT-related acquisitions to certify that the appropriate ADPT security requirements are included in the specification for the operation of an ADPT installation facility, equipment, application system, or acquisition of ADPT hardware, software, or related services. COTRs for a contract action should ensure that the ADPT security-related requirements are adhered to by the contractors throughout the life cycle of the contract.

(6) The ADPT Security Officer shall ensure that periodic system security reviews are conducted. Even if there are no changes to the security posture of a system or division, ADPT systems will be reviewed and reaccredited if three years have elapsed since the date of certification of the security posture. The ADPT Security Officer shall develop, with the assistance of the SPM and the SCMPMs, a list of ADPT systems requiring accreditation. This list should include the recommended priority and the accrediting authority for each ADPT system to be accredited. This list shall be verified annually.

EFFECTIVE: 07/26/95

35-9 MINIMUM SECURITY REQUIREMENTS (See MIOG, Part I, 261-2.)

(1) The goal of ADPT security is to develop a functionally secure, efficient, cost-effective environment based on an assessment of security risks and safeguards. All ADPT systems processing, storing or transmitting classified or sensitive information shall meet the requirements of this policy through automated or manual means. More stringent requirements may be imposed based on a risk analysis. Classified and SCI systems will also conform to the provisions of DCID 1/16, "Security Policy for Uniform Protection of Intelligence Processed in Automated Information Systems and Networks (U)," 19 July 1988.

(2) This section documents the minimum security requirements for all FBI ADPT systems with respect to facility security, personnel security, administrative security, technical

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 35 - 26

security features, emanations security, and communications security. Related security disciplines are referenced where appropriate.

EFFECTIVE: 07/26/95

35-9.1 Facility Security

(1) Facility security addresses the requirement to provide physical and environmental security controls commensurate with the level of risk to the ADPT systems supported in a facility, as identified by a risk analysis. The security controls must not be less than the minimum requirements discussed in this section unless a written waiver has been granted by the accrediting authority, i.e., the SPM for non-SCI systems and the Assistant Director, NSD for SCI systems.

(2) For the purposes of this policy, an ADPT facility includes any space housing ADPT equipment such as terminals, microcomputers, mainframe systems, communications equipment and/or supporting environmental control utilities. Facilities also include data storage libraries and ADPT system documentation libraries.

EFFECTIVE: 07/26/95

35-9.1.1 Physical Security

(1) Physical security is that part of the FBI's facility security program which is concerned with the physical measures designed to prevent unauthorized physical access to equipment, facilities, material, information, and documents, and to safeguard them against espionage, sabotage, damage, tampering, theft and other covert or overt acts. ADPT hardware, software, documentation, and all classified and sensitive information handled by the ADPT system shall be protected to prevent unauthorized disclosure, modification, or destruction. ADPT system hardware, software, or documentation shall be protected if access to such resources reveals information that may be used to eliminate, circumvent, or otherwise render ineffective the security countermeasures for classified or sensitive information.

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 35 - 27

(2) Classified or sensitive FBI information must be processed, stored, or transmitted in spaces which are under exclusive FBI control while operational. When not in operation or under the direct personal control of an authorized person, FBI ADPT systems and information must be protected by storage areas, storage equipment, and/or systems or measures which are consistent with the FBI's facility security program.

(3) The SPM prescribes policies, procedures, and standards for the FBI's facility security program. ADPT security planning must take into consideration the facility security program prior to conducting ADPT operations, at any location, as part of the accreditation process for an ADPT system that processes, stores, or transmits classified or sensitive FBI information.

(4) More stringent physical security controls are required to support the processing, storage, and transmission of SCI. This activity will be subject to the provisions of DCID 1/16 which states the processing of SCI data must be restricted to an accredited SCI Facility (SCIF) and SCI may not be stored on nonremovable storage media except in accredited SCIFs approved for the open storage of SCI. DCID 1/21 provides SCIF physical security criteria. There are instances where other facility security-related rules and requirements apply, too (e.g., the Legal Attaches must comply with Department of State standards in addition to the FBI requirements).

Network and Information Systems Support Unit (NISSU), OMS, IRD conducts surveys and develops the specifications for SCIFs and for the field offices and Legal Attaches. These activities are coordinated by the SPM, who is also the accrediting authority for the FBI's SCIFs.

(5) For all types of facilities where classified or sensitive information is stored, processed, or transmitted, physical access will be restricted to those individuals who are cleared and authorized in accordance with the personnel security requirements discussed in Section 35-9.2 and who are necessary to complete job functions and related duties. All uncleared personnel granted facility access must be properly escorted and restricted to those areas necessary to complete their tasks. Classified and sensitive FBI information must be protected from unauthorized disclosure to such persons.

EFFECTIVE: 11/28/97

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 35 - 28

35-9.1.2 Environmental

(1) Environmental controls address the requirement to provide appropriate temperature and humidity controls, fire protection, power, and natural disaster protection necessary to ensure the continuity of ADPT facilities, equipment, and operations.

(2) An office area that supports desktop ADPT equipment, such as microcomputers, does not require additional environmental controls beyond the requirements specified for human safety and comfort.

(3) ADPT facilities supporting large-scale ADPT operations, such as mainframe computer and telecommunication facilities, require consideration of additional environmental controls as determined by a facility risk analysis. The following additional environmental controls shall be considered.

(a) Fire prevention, detection, suppression and protection measures.

(b) Controls that reduce the risk of water damage, provide water detection, and corrective measures, and water hazard prevention devices.

(c) Electric power supply protection.

(d) Temperature and humidity control.

(e) Natural disaster protection from earthquake, lightning, windstorm, and other natural disasters.

(f) Housekeeping protection from dirt and dust.

(g) Personnel safety features.

EFFECTIVE: 07/26/95

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 35 - 29

35-9.2 Personnel (See MIOG, Part II, 35-9.1.1, 35-9.4.1, 35-9.4.5.)

(1) All personnel who have been entrusted with the management, operation, maintenance, or use of an FBI ADPT system processing, storing, or transmitting sensitive and/or classified information require the appropriate personnel security approval. The SCMS, NSD, sets policy and provides procedures and guidance in support of the FBI's personnel security program. ADPT security planning must take into consideration the personnel security program prior to conducting ADPT operations as part of the accreditation process for an FBI ADPT system.

(2) All FBI personnel hold Top Secret security clearances. MIOG, Part I, Section 67-7 through 67-7.11, provides policies and procedures for personnel security clearances for Bureau employees.

(3) Non-Bureau personnel who have been entrusted with the management, operation, maintenance, or use of classified FBI ADPT systems require Top Secret security clearances. See MIOG, Part I, Sections 259 and 260. Personnel security approvals for nonclassified FBI ADPT systems are documented in the System Security Plans for these systems.

(4) Non-Bureau personnel who are required to perform maintenance on FBI ADPT systems within FBI controlled space and who do not require access to classified systems may be approved for escorted access based on an FBI-conducted Limited Background Investigation. This activity shall be coordinated by the SPM. Refer to MIOG, Part I, Section 260, "Industrial Security Program," particularly 260-4.1.1.

(5) Personnel must be indoctrinated, as required, prior to being granted access to FBI ADPT systems that support special access programs. The provisions for special access programs are discussed in MIOG, Part II, Section 26-10.2.

(6) ADPT security training must be provided to all personnel who manage, operate, develop or use ADPT systems. Refer to Section 35-8.3.

(7) The SCMPM shall ensure that debriefings are conducted, as required by MIOG, Part I, Section 261-2.

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 35 - 30

EFFECTIVE: 07/26/95

35-9.3 Technical Security Features (See MIOG, Part II, 35-9.4.2, 35-9.4.6.)

The purpose of this section is to establish near-term requirements and long-term goals to improve the security of the Bureau's ADPT systems through increasing reliance on technical security features. The minimum technical security requirements addressed in Sections 35-9.3.1 and 35-9.3.2 are technically feasible in the Bureau's current ADPT environment and shall be addressed. As technology evolves, the desirable technical security features identified in Section 35-9.3.3 should be addressed during the system planning process.

EFFECTIVE: 07/26/95

35-9.3.1 Minimum Technical Security Requirements (See MIOG, Part II, 35-9.3, 35-9.4.2.)

(1) ADPT systems used for the processing of classified or sensitive information in the System High Security Mode of Operation must have the functionality of the C2 level of trust defined in the Department of Defense (DoD) 5200.28-STD, "Department of Defense Trusted Computer System Evaluation Criteria." The Trusted Network Interpretation of the Trusted Computer System Evaluation Criteria, National Computer Security Center Technical Guide 005 (NSC-TG-005), provides guidance on achieving C2 functionality in a network. Other safeguards which maintain the level of system security commensurate with the sensitivity of the data may be substituted in cases where C2 requirements are time-consuming, technically unsound, or adversely affect operations to an unacceptable degree. The Department Security Officer must approve exceptions to C2 for classified systems. The IRM-SPM must approve such exceptions for sensitive systems.

(2) Systems operated in the Compartmented or Multilevel Security Mode of Operation require additional security controls and will be addressed on a case-by-case basis. The ADPT Security Officer shall be consulted to ensure that the technical security requirements

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 35 - 31

are adequately addressed. These modes of operation require approval by the Department Security Officer.

(3) FBI ADPT operations involving classified information and SCI must be conducted in accordance with the provisions of Director of Central Intelligence Directive 1/16, "Security Policy for Uniform Protection of Intelligence Processed in Automated Information Systems and Networks." The ADPT Security Officer shall be consulted prior to defining the security requirements for classified and SCI systems to ensure that the technical security requirements defined in DCID 1/16 are adequately addressed.

(4) The design of ADPT systems that process, store, or transmit classified or sensitive information must include, at a minimum, the technical security features discussed in this section. Security countermeasures shall be in place to ensure each person having access to a computer system is individually accountable for his/her actions on the system.

(a) User Identification - The ADPT system shall control and limit user access based on identification and authentication of the user. The identity of each user will be established positively before authorizing access. User identification and password systems support the minimum requirements of access control, least privilege, and system integrity.

(b) Authentication - For ADPT system requiring authentication controls, the ADPT system shall ensure that each user of the ADPT system is authenticated before access is permitted. Currently, use of a password system is the preferred method for authenticating users of FBI ADPT systems. Passwords will be authenticated each time they are used. FIPS PUB 83 provides standards for authentication. More sophisticated authentication techniques, such as retina scanners or voice recognition systems, must be cost-justified through the risk analysis process.

(c) Audit Records - All systems transactions are subject to recording and routine review for inappropriate or illegal activity. Audit trails should be sufficient in detail to facilitate reconstruction of events if compromise or malfunction occurs. Audit trails should be reviewed at least once weekly, or as specified in the system security plan. The audit trail should contain at least the following information:

1. The identity of each user and device having access to the system or attempting to access the system.

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 35 - 32

2. The time and date of the access, time and date of log-off.

3. Activities that might modify, bypass, or negate security safeguards controlled by the computer system.

4. Security-relevant actions associated with processing.

(d) Object Reuse - All classified and sensitive ADPT systems shall clear memory and storage before reallocation to a different user. This prevents one user from obtaining another user's residual data.

(e) Access Control - For systems operating in the System High Security Mode of Operation, this may be implemented through discretionary access control techniques through measures such as file passwords, access control lists, disk encryption or other techniques, as defined in the approved system security plan. For ADPT systems operating in the compartmented or multilevel security mode, mandatory access control (MAC) is required. MAC is a means of restricting access to information based on labels. A user's label indicates what information the user is permitted to access and the type of access (e.g., read or write) that the user is allowed to perform. An object's label indicates the sensitivity of the information that the object contains. A user's label must meet specific criteria defined by MAC policy in order for the user to be permitted access to a labeled object. This type of access control is always enforced above any discretionary controls implemented by users.

(5) The following additional technical security control requirements apply to FBI ADPT systems:

(a) Internal Labeling - By definition, compartmented mode and multilevel secure modes of operation require internal labeling. In addition, for systems operating in other modes and processing multiple classifications of information (e.g., Sensitive and Secret), security classification labels shall be associated with all data within the system.

(b) Standard Warning Banner - This banner addresses the concerns that those individuals who are using ADPT systems without or in excess of their authority, and those authorized users who are subject to monitoring, be told expressly that by using the system they are consenting to such monitoring. It also provides a basis for

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 35 - 33

establishing the "knowingly" and "with intent" provisions of Title 18, USC, Section 1030, should prosecution become necessary. The following banner shall be displayed on all FBI ADPT systems at a point prior to the user signing onto the system:

"This FBI system is for the sole use of authorized users for official business only. You have no expectation of privacy in its use. To protect the system from unauthorized use and to insure that the system is functioning properly, individuals using this computer system are subject to having all of their activities on this system monitored and recorded by system personnel. Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals evidence of possible abuse or criminal activity, system personnel may provide the results of such monitoring to the appropriate officials."

(c) Inactivity Time Out - The ADPT system shall lock out an interactive session after an interval of user inactivity not to exceed thirty minutes. The time interval and restart requirements shall be specified in the system security plan.

(6) Interconnections between sensitive and classified FBI ADPT systems and non-FBI ADPT systems must be established through Controlled Interfaces. The ADPT Security Officer must be consulted for guidance on establishing controlled interfaces. The controlled interfaces used in an ADPT system implemented as a network shall be accredited at the highest classification level and most restrictive classification category of information on the network. The controlled interface function of an ADPT system is composed of a combination of gateway and guard functions. Gateways provide a secure point of interconnection between networks, connected peripheral devices, remote terminals, or remote hosts, and provide a reliable exchange of security information to allow secure interconnections between components. Automated guard processors and security filters (hereafter referred to as guards) are software or hardware/software techniques or specialized equipment that filter information in a data stream based on associated security labels and/or data content. For example, a guard might accept an input data stream of information of mixed classifications up to SECRET, but permit only data classified up to CONFIDENTIAL to pass.

EFFECTIVE: 07/26/95

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 35 - 34

35-9.3.2 Security Assurances (See MIOG, Part II, 35-9.3 & 35-9.4.2.)

(1) ADPT systems shall be examined when received from the vendor and before being placed into use.

(a) Hardware - an examination shall result in assurance that the equipment appears to be in good working order and have no "parts" that might be detrimental to the secure operation of the resource when placed under FBI control and cognizance. Subsequent changes and developments which affect security may require additional examination. The emanations security requirements stated in Section 35-9.5 also apply.

(b) Commercial Software - Commercially procured software shall be examined to ensure that the software contains no features which might be detrimental to the security of the ADPT system. Security-related software shall be examined to assure that the security features function as specified.

(c) Software Developed In-house - New or significantly changed software and hardware developed by or specifically for the FBI shall be subject to testing and review at all stages of the development.

(2) The FBI endorses the use of products from the Evaluated Products List (EPL) which is maintained by the National Computer Security Center. Products on the EPL are computer systems, software or components that protect information while it is being stored or processed. They have been evaluated by the government as to the degree of trust that can be placed in them. In order to assess this, the DoD Trusted Computer System Evaluation Criteria was written and products were evaluated against this criteria and given a level of trustworthiness. When certified to be properly implemented through the process discussed in Section 35-8.1.5, these products shall be accepted as meeting the security requirements for the portion of the ADPT system where they are used.

(3) If products from the EPL are not specified or used, a functionality statement is required to discuss how the trusted computing base functionality will be achieved and a time frame for full implementation to the appropriate level of trust will be included. The functionality statement will become part of the accreditation decision. The areas to be addressed in the system security planning phase include:

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 35 - 35

(a) Confidence in Software Source - In acquiring resources to be used as part of an ADPT system, consideration shall be given to the level of confidence placed in the vendor to provide a quality product, to support the security features of the product, and to assist in the correction of any flaws.

(b) Security Performance Testing - Security performance testing includes both certification testing that is performed before the ADPT system is accredited and ongoing performance testing that is performed on a regular basis.

(c) Flaw Discovery - For ADPT systems operating in the compartmented security mode or multilevel security mode, the vendor shall provide a method for ensuring the discovery of flaws in the system (hardware, firmware, or software) that may have an effect on the security of the ADPT system.

(d) Security Penetration Testing - In addition to testing the performance of the ADPT system operating in the compartmented security mode or multilevel security mode, there shall be testing to attempt to penetrate the security countermeasures of the system. The test procedures shall be documented in the test plan for certification and also in the test plan for ongoing testing.

(e) Description of Trusted Computing Base Protection - The protection and provisions of the trusted computing base shall be documented in such a manner to show the underlying planning for the security of an ADPT system operating in the compartmented security mode or multilevel security mode of operation. The trusted computing base shall be isolated and protected from any user or unauthorized process interference or modification. Hardware and software features shall be provided that can be used to periodically validate the correct operation of the elements of the trusted computing base.

(f) Flaw Tracking and Remediation - For ADPT systems operating in the multilevel security mode of operation, the vendor shall provide evidence that all discovered flaws have been tracked and remedied.

(g) Life-Cycle Assurance - The development of hardware, firmware, and software shall be conducted under life-cycle control and management.

(4) Configuration Management - At a minimum, a configuration management system shall be in place that maintains

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 35 - 36

control of changes of any of the system's technical features that may alter the accreditation status. Examples include security-related hardware or changes of any line of source or object code of the security-related software. The system will record by whom, for what reason, and when the change is made. Up-to-date documentation of the security-related hardware and/or software design will be maintained. This is a requirement to preserve the integrity of accreditation.

EFFECTIVE: 07/26/95

35-9.3.3 Desirable Technical Security Features (See MIOG, Part II, 35-9.3.)

(1) As technology evolves, system planning should address the achievement of the technical security features addressed in this section. The goal is to achieve a multilevel security mode of operation for all FBI ADPT systems and to provide a trusted path from the workstation forward. A multilevel secure environment allows the FBI to expand the efficiency of information processing. The planning process shall be documented and approved through the system security plan.

(2) Interoperability With External Systems - Support for digital signature standards, nonrepudiation in messaging systems, and data encryption issues should be provided as they relate to interagency communications or interoperability.

(3) Continuous On-Line Automated Monitoring and Warning - The ADPT system shall provide for continuous, real-time monitoring (audit) of use and real-time warning to the CSSO of suspected misuse.

(4) Network Access Control Features - The following areas shall be addressed to achieve a trusted communications path:

(a) Identification and Authentication Forwarding - Reliable forwarding of the identification shall be used between ADPT systems when users are connecting through a network. When identification forwarding cannot be verified, a request for access from a remote ADPT system shall require authentication before permitting access to the system.

(b) Protection of Authenticator Data - In forwarding

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 35 - 37

the authenticator information and any tables (e.g., password tables) associated with it, the data shall be protected from access by unauthorized users (e.g., by encryption) and its integrity shall be ensured.

(c) Methods of Continuous, On-line Monitoring - Monitoring of network activities shall be included in each network operating in a multilevel security mode. This monitoring shall also include real-time notification to the CSSO of any system anomalies.

(5) Secure Message Traffic - The communications methodology for the network shall ensure the detection of errors in traffic across the network links and the retransmission of erroneous traffic.

(6) Security Label Integrity - For an ADPT system accredited to operate in the compartmented security mode or multilevel security mode, the communications methodology shall ensure: integrity of the security labels; the association of a security label with the transmitted data; and enforcement of the control features of the security labels.

(7) Device Labels - For an ADPT system accredited to operate at the compartmented security mode or multilevel security mode, the communications methodology shall ensure that the originating and destination device labels are a part of each message header and enforce the control features of the data flow between originator and destination.

EFFECTIVE: 07/26/95

35-9.4 Administrative Security and Accountability

(1) Administrative security is the administrative controls and operational procedures used in conjunction with or in place of technical security features to achieve a level of security consistent with the sensitivity of the information processed, stored, or transmitted by FBI ADPT systems. The applicable administrative security controls are documented in the system security plan for a system.

(2) The CSSO shall establish access control criteria and

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 35 - 38

administrative procedures to control access to information processed, stored, or transmitted by FBI ADPT systems. Access is defined as the ability and the means to approach, communicate with (input to or receive output from), or otherwise make use of any material or component in an ADPT system. These activities are documented through the system security planning process, approved by the ADPT Security Officer and accredited as discussed in Section 35-8.2.

EFFECTIVE: 07/26/95

35-9.4.1 Access Control Criteria (See MIOG, Part II, 35-7(6), 35-9.4.4.)

(1) The access control criteria shall identify who is authorized to access the system, and identify responsibility for approving all access to the system. The individual who requires access must possess the appropriate security clearance and have the need to know, i.e., access to the information is an operational necessity. Moreover, the system security features must have the technical ability to restrict the user's access to only that information which is necessary for operations and for which the user has clearance.

(2) Bureau personnel accessing internal FBI ADPT systems must have Top Secret security clearances (as discussed in Section 35-9.2). Personnel must only be granted access to systems for which they have a valid need to know based on their operational necessity (e.g., an individual working in the Personnel Division would not require access to case information).

(3) Non-Bureau individuals operating in Joint Task Forces (JTF), other federal agencies in non-JTF capacity, and/or private contractors to support particular operations will be granted limited access to FBI systems. Access will be limited to the privileges assigned to nonsupervisory Special Agent personnel with access to unrestricted case classifications and cases. In limited circumstances, SACs may request supervisory access for non-Bureau individuals who serve as task force supervisors.

(a) Each request for access must be individually reviewed. The review criteria are:

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 35 - 39

1. The individual must possess a Top Secret security clearance.
2. The individual must have the need to know, i.e., access to the information is an operational necessity; SAC/AD recommendation and the sponsoring division of the application must concur.
3. The system security features must have the technical ability to restrict the user's access to only that information which is necessary for operations and for which the user has clearance.

(b) All requests must be submitted in writing to: the sponsoring division of the application, for need-to-know criteria; the SPM, for personnel security clearance status; and, the ADPT Security Officer, for evaluation of the technical security features.

(c) The SPM will be the final adjudicator of all access authorization and will maintain a list of non-Bureau personnel who have been authorized access to FBI ADPT systems.

(4) The non-Bureau individual must receive Computer Security Awareness Training, Application Training and execute an FBI nondisclosure agreement (FD-868) defined in MIOG, Part II, 35-13.2.

(5) The FBI also operates systems designed for the support of the criminal justice community, (e.g., NCIC). Because these systems have not been designed for internal FBI use, personnel accountability requirements are defined for each system and are documented in the System Security Plans for these systems. Certain provisions of Section 35-9.4.1 may not apply to these systems.

EFFECTIVE: 08/19/97

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 35 - 40

35-9.4.2 Administrative Procedures (See MIOG, Part II, 35-13.)

(1) Administrative procedures support the access control mechanisms (i.e., the applicable technical security features discussed in Section 35-9.3) and assign responsibility for administering the mechanisms.

(2) Access control mechanisms provide identification and authentication features as discussed in Section 35-9.3. These features are administered as follows:

(a) Each user of an FBI ADPT system must be uniquely identified. User identification (ID) will not be shared.

(b) Users of FBI ADPT systems will be restricted to only those privileges necessary to perform assigned tasks.

(c) Super-user or system programmer privileges will be granted on a selective basis and will identify any constraints applicable to privileged users.

(d) User accounts that have been inactive for over 90 days will be suspended. The person responsible for administering the access control mechanism is authorized to reinstate such accounts up to 180 days overall. User accounts that have been inactive for 180 days will be deleted and may only be reissued by the person authorized to approve access who is identified in the access control criteria and only to an individual who has been authorized access.

(e) If passwords are selected as the authentication mechanism for a system, password usage shall meet the standards which are set forth in FIPS PUB 112:

1. Passwords shall be changed at least every 90 days.

2. Passwords shall be changed when a security violation is suspected or known.

3. All vendor or default passwords shall be changed prior to system implementation.

4. A password shall be protected commensurate with the information to which it provides access. Password distribution methods shall be provided protection equivalent to the

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 35 - 41

level of information the passwords protect.

(f) At the time of password issuance, users must be briefed on the following:

1. Password classification and exclusiveness.
2. Measures to safeguard "classified" and "sensitive" passwords.
3. Prohibitions against disclosing passwords to other personnel.
4. Responsibilities for notifying the CSSO of password misuse.
5. Password change procedures.

(3) All systems transactions are subject to recording and routine review for inappropriate or illegal activity. Audit logs should be reviewed as specified in the system security plan. Audit logs should be retained according to the retention period specified in the system security plan. Evidence of security violations must be reported to the ADPT Security Officer. The contents of audit logs are described in Section 35-9.3.1.

(4) When an individual who has been granted access to an FBI ADPT system no longer requires access privileges, the CSSO shall ensure that the individual's identification (ID), passwords, and other access codes are immediately removed from all ADPT systems.

EFFECTIVE: 07/26/95

35-9.4.3 Internal Controls

(1) Office of Management and Budget (OMB) Circular A-123, "Internal Control Systems," prescribes the policies and procedures to be followed by departments and agencies in establishing, maintaining, evaluating and reporting on internal controls in their program and administrative activities. OMB Circular A-123 requires that an organization establish and maintain a cost-effective system of internal controls to provide reasonable assurance that government

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 35 - 42

resources are protected against fraud, waste, mismanagement, and misappropriation.

(2) Control techniques that support of the internal control objectives for FBI ADPT systems include, but are not limited to the following:

(a) Key duties and responsibilities in authorizing, processing, recording, and reviewing system-related activities should be separated among individuals to the extent practical in the organizational structure. For example, system security-related and general system operational duties should be performed by separate individuals.

(b) Individuals assigned primary responsibility for performing critical functions in support of the ADPT system (e.g., system administration, security administration, system operations, programming, etc.) should have trained alternates who can perform these functions in the event the individual who is assigned primary responsibility is unavailable.

(c) System life cycle documentation should exist to reflect the current state of the ADPT system as it is being operated. The documentation must be sufficient to ensure effective operation by users and system maintenance by programmers.

(3) The risk assessment for the ADPT system should include a review of the susceptibility of the system to waste, loss, unauthorized use, or misappropriation.

EFFECTIVE: 07/26/95

35-9.4.4 Software and Data Security (See MIOG, Part II, 35-13.)

(1) All software used on FBI ADPT systems should be obtained through authorized procurement channels. Use of software acquired through other than appropriate procurement channels (e.g., public domain software, bulletin board services, personally owned software (developed or purchased)) is restricted, must be approved in writing by the SAC as an operational necessity, and must adhere to the applicable software licensing restrictions. Even if the software is approved by the SAC, software acquired through other than the

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 35 - 43

appropriate procurement channels must be scanned for malicious code and used on a standalone microcomputer to maintain the accreditation of FBI ADPT systems.

(2) FBI microcomputers and associated ADPT storage media which have processed, stored or transmitted other than appropriately acquired software must be cleared prior to processing FBI information. When the software is no longer required, the software should be cleared from the system. Non-FBI microcomputers and associated storage media which have processed, stored, or transmitted non-FBI software and/or information must be sanitized prior to processing, storing, or transmitting any FBI information (e.g., personally owned computer must be sanitized before it is used to process FBI information). The clearing and sanitization processes are discussed in Section 35-9.4.14.

(3) Safeguards must be in place to detect and minimize inadvertent or malicious modification or destruction of an ADPT system's application software, operating system software, and critical data files. The safeguards should achieve the integrity objectives and should be documented in the system security plan. Executable software authorized to run on an FBI ADPT system shall be identified in the system security plan. The level of protection must be commensurate with the sensitivity of the information processed. At a minimum, such media should be backed-up and stored physically separated from the system or at an off-site location.

(4) Virus prevention measures commensurate with the level of risk identified in the risk analysis shall be employed to protect the integrity of the software/data. The ADPT Security Officer manages the virus protection program for the FBI and should be contacted for approved virus scanning and cleanup techniques and/or procedures if there is a suspected or known malicious software threat. Whenever a virus infection is detected, it should be reported to the ADPT Security Officer. All media shall be scanned as follows:

(a) All seized machines and media, prior to introduction to or use by any FBI ADPT system.

(b) All removable magnetic media (such as floppy disks) entering the operational environment regardless of source, prior to use.

(c) All fixed storage devices, on a periodic basis.

(5) Use of software shall comply with copyright laws.

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 35 - 44

(6) To facilitate compliance with MIOG, Part II, Section 2-9, "Grand Jury (Rule 6)," access to Rule 6(e) information via electronic means must be tracked by user name, date, time, what was accessed, and what actions were taken. All existing Rule 6(e) information readily identifiable as such, and all Rule 6(e) information added to the system must be labeled, as discussed in Section 35-9.4.10, and access to it restricted and tracked, as discussed in Section 35-9.4.1.

(7) Access to SCI information must be restricted to appropriately indoctrinated individuals. Access to TOP SECRET and/or SCI information must be tracked by user name, date, time, what was accessed, what actions were taken. All existing TOP SECRET and/or SCI readily identifiable as such and all TOP SECRET and/or SCI added to the system, must be labeled and access to it restricted. The FBI ADPT Security Officer shall be contacted prior to development or operation of any system processing SCI.

(8) Introduction of data from sources and/or in formats other than those specified in the system security plan (e.g., financial data received from banking institutions) must be approved in writing by the SAC as an operational necessity. These activities must be in conformance with the accreditation of the ADPT system.

(9) In order to maintain software integrity, proper configuration management and change controls must be used to monitor updates to and the installation of software. This process will help to ensure that the software functions as expected and that a historical record of software changes is maintained. Such controls also help to ensure that only authorized software is permitted on the system. These controls may include a software configuration policy that grants managerial approval prior to software modification, then documents the changes.

EFFECTIVE: 07/26/95

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 35 - 45

35-9.4.5 Maintenance Activities (See MIOG, Part II, 35-13.)

(1) Hardware and software maintenance activity may affect the integrity of existing protection measures or permit the introduction of security exposures into a system (e.g., computer viruses, trojan horses, logic bombs, implant devices, etc.).

(2) All electronic storage and memory devices associated with FBI ADPT systems may not be returned to the vendor for "trade-in" or credit purposes. Exceptions must be approved by the ADPT Security Officer.

(3) Dial-up diagnostic maintenance examination of FBI ADPT equipment via remote communication between vendors and FBI facilities is prohibited.

(4) All maintenance work performed on-site must be supervised by FBI personnel knowledgeable in the operation of the ADPT system regardless of the classification of the system or its associated media. On-site maintenance personnel must meet the personnel security requirements discussed in Section 35-9.2. Vendor diagnostic software used on any FBI microcomputer may not be removed from FBI control. Vendor diagnostic software must be scanned, write-protected, and retained by the Computer Specialist. Only this copy of the software may be used on FBI ADPT systems.

(5) Storage media and microcomputers with nonremovable ADPT storage media must only be transferred through maintenance channels approved by FBIHQ. Only ADPT storage media and microcomputers which have been sanitized and declassified, as discussed in Section 35-9.4.14, can be released from FBI control for maintenance.

EFFECTIVE: 08/04/97

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 35 - 46

35-9.4.6 Portable Microcomputers (See MIOG, Part II, 35-9.4.17
& 35-13.)

(1) Portable microcomputers (e.g., laptops, notebooks) support the Bureau's mission but require extra attention due to the vulnerability that their portability creates.

(2) As is the case with all FBI equipment, portable microcomputers are considered nonexpendable FBI property. An FD-281 (or FD-281a), "RECEIPT FOR GOVERNMENT PROPERTY," must be executed for portable microcomputers issued to an individual for an extended period of time. Portable microcomputers charged out for shorter periods of time may be accounted for by O-96, "FBI Property Pass," or an FD-79, "CHARGE-OUT RECORD OF NONEXPENDABLE PROPERTY." See Manual of Administrative Operations and Procedures (MAOP), Part I, 1-3, "GOVERNMENT PROPERTY," for details.

(3) To the extent possible, portable microcomputers should be kept in the possession of the individual to whom they are issued or charged out.

(4) FBI portable microcomputers are authorized to process classified information up to and including Secret/Collateral within the U.S. and its territories and can be connected to the FBI Secure Network (FBINET). The processing of Top Secret and SCI information is not authorized on portable microcomputers without written authorization by the FBI's SPM. Like classified documents, portable microcomputers used to process classified information must be secured in locked storage when not under direct personal control. Portable microcomputers should be kept in the possession of the individual to whom they are issued or charged out. Removable hard drives must always remain in the direct personal control of the individual to whom they are issued or maintained in a secured locked container within FBI-controlled space. The hard drive cannot be left unattended.

(5) All FBI portable microcomputers are to have security subsystems installed which provide specific security features, including individual identification, authentication and access control, and disk encryption, as discussed in Section 35-9.3.

(6) Use of portable ADPT systems outside U.S. territories must be coordinated with the ADPTSO.

(7) Removable hard drive devices used to process, store, or transmit National Security Information (NSI) (this includes all hard drives connected to the FBINET) and/or FBI sensitive information

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 35 - 47

cannot have communications software that supports the connection to a modem or any other network (LEO, Internet, etc.) without written authorization from the FBI ADPTSO.

(8) Storage of FBI sensitive and/or classified information on removable hard drives must be kept to a minimum. The individual to whom they are issued or charged to will be responsible for ensuring information processed and stored on the removable hard drive is uploaded to the FBI's central record system or transferred to another file storage media which will be retained in controlled FBI space and then deleted from the hard drive. This will reduce the amount of information contained on the hard drive if the drive is lost or stolen.

(9) Portable microcomputers and docking stations are not authorized within the Criminal Informant Management System (CIMS) program.

(10) Connections to non-FBI networks, and the purchase of FAX/MODEMS will be approved, on a case-by-case basis, by the ADPTSO. Portable microcomputers connected to non-FBI networks must operate as DEDICATED microcomputers. These portable microcomputers should not process any FBI sensitive information and MUST NOT process any National Security Information. Additional hard drives can be procured to support the use of FAX/MODEMS.

EFFECTIVE: 08/18/97

35-9.4.7 Inventory of ADPT Systems Processing Classified Information

Computer Specialists must be able to identify all equipment processing, storing, or transmitting classified information, whether operating as part of a network or in a standalone mode of operation. This requirement is in addition to the hardware and software inventory requirements stated in MIOG, Part II, Section 16-18.9.

EFFECTIVE: 08/04/97

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 35 - 48

35-9.4.8 Telecommunications (See MIOG, Part II, 35-9.4.15 & 35-13.)

(1) Unencrypted dial-up access to FBI ADPT systems is prohibited.

(2) Connections between FBI ADPT systems and non-FBI ADPT systems, public or private, may only be authorized under the following conditions:

(a) Connections to non-FBI ADPT systems for law enforcement-related inquiries (e.g., Department of Motor Vehicles, state or local police departments, and credit bureaus) are authorized. Microcomputers connected to non-FBI networks must operate as dedicated microcomputers. These connections should be documented locally. Documentation should include technical description of the connection and administrative approvals.

(b) All other connections to non-FBI networks will be approved, on a case-by-case basis, by the ADPT Security Officer. For example, FBIHQ is working to provide access from FBINET to U.S. Customs Service, Drug Enforcement Administration, and the National Information Infrastructure (NII). In order to ensure the security of FBINET, these interconnections will require special security measures such as trusted guard processors or multilevel secure systems. As part of the approval process, the ADPT Security Officer will ensure that the appropriate documentation, such as memoranda of understanding, interconnection agreements, etc., is executed on behalf of the FBI.

(3) Because electronic bulletin boards may have constitutional expectations of privacy, a comprehensive program of monitoring electronic bulletin boards for criminal or intelligence purposes is prohibited.

EFFECTIVE: 07/26/95

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 35 - 49

35-9.4.9 Classification and Controls (See MIOG, Part II, 35-13.)

(1) ADPT systems are classified at the highest level of information that has been entered into, stored on, or processed by the system unless the system can be appropriately declassified. The ADPT system must be labeled, secured and operated commensurate with its classification level. An exception is microcomputers with nonremovable ADPT storage media may only store classified information when the SPM has granted a written waiver for fixed drive open storage and the system is protected with a security system that prevents writing to the fixed drive, forcing use of removable media.

(2) All ADPT storage media containing classified information must be labeled and secured in accordance with the policies for the storage of classified material stated in MIOG, Part II, Section 26-5 through 26-5.3.

(3) FBI ADPT systems that store, process, or transmit sensitive or classified information must be operated only in space that is under exclusive Bureau control and under the personal control of authorized persons. ADPT systems, such as microcomputers, operated under FBI control must be adequately protected to ensure that access to FBI information is available only while FBI personnel are on-site.

(4) When not under the personal control of an authorized person either during or outside regular working hours, FBI microcomputers must be secured as follows:

(a) Microcomputers must be turned off. Exceptions must be approved as part of the accreditation statement.

(b) Diskettes, tapes, removable storage devices and printer ribbons must be labeled and secured commensurate with the highest level of information ever stored on the device.

(5) All FBI ADPT systems connected to FBINET, IISNET, and SAMNET are considered classified and must be appropriately labeled and controlled at the level of those networks.

(6) The FBINET subnetwork is authorized to process up to and including SECRET/collateral data. Under no circumstances may TOP SECRET (TS) or Sensitive Compartmented Information (SCI) be processed by FBINET or introduced by any means into any ADPT system that is connected to the FBINET. To facilitate compliance with this restriction, all correspondence containing TS or SCI levels of data or

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 35 - 50

information will be "portion marked" to show specific classification levels (i.e., title, paragraph). Portion marking will allow for that information which is classified as SECRET/collateral or below to be entered into ADPT systems accessed by the FBINET network. Under no circumstances may SCI, regardless of classification level, be processed on the FBINET. (See MIOG, Part II, 26-2.6.3.)

EFFECTIVE: 07/26/95

35-9.4.10 External Labels (See MIOG, Part II, 35-9.4.4 & 35-13.)

(1) All ADPT storage media must be marked with a classification and a data descriptor label. Portable microcomputers are exempt from this provision.

(a) All systems with nonremovable ADPT storage devices must conspicuously display classification and data descriptor labels on the unit that contains the magnetic ADPT storage device. The monitor may also be labeled.

(b) Removable media must be labeled with external markings. An exception to this policy is granted for computer center operations supporting a computerized tape management system that provides internal classification and data descriptor designations, as long as the media remains in FBI-controlled spaces. However, all magnetic media leaving FBI-controlled spaces must be labeled with the external classification and data descriptor labels.

(2) Classification Labels are color-coded labels used to indicate the highest level of classification of information ever stored on ADPT storage media. The classification labels used by the FBI are: CLASSIFIED SCI yellow label, SF-712; TOP SECRET orange label, SF-706; SECRET red label, SF-707; CONFIDENTIAL blue label, SF-708; and UNCLASSIFIED green label, SF-710.

(3) Data Descriptor Labels are used to identify additional safeguarding controls related to information stored on ADPT storage media. They should indicate, at a minimum, the appropriate dissemination and control channels. These labels should also contain information necessary to retrieve archived data. The data descriptor label is SF-711 (or equivalent). The following illustrates information to be inserted on the data descriptor label, as applicable:

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 35 - 51

(a) Classification - This space should contain either one of the three classification levels: TOP SECRET, SECRET, CONFIDENTIAL; or a statement that the media is either SENSITIVE or UNCLASSIFIED. TOP SECRET, SECRET, or CONFIDENTIAL, and UNCLASSIFIED are defined in MIOG, Part II, Section 26-2.4.

(b) Dissemination - Dissemination restrictions or handling caveats are used in conjunction with certain information to indicate that the information has special access or handling requirements. They are not classification levels. Examples include:

1. Rule 6(e) Material: Rule 6(e) of the Rules of Criminal Procedure, "Secrecy of Proceedings and Disclosure."

2. ORCON: Dissemination and Extraction of Information Controlled by Originator - May not be disseminated outside of the Headquarters of the receiving agency in any form, even extracted or paraphrased, without permission of the originator.

3. NOFORN: Not Releasable to Foreign Nationals - May not be released in any form to foreign governments, foreign nations or non-U.S. citizens without permission of the originator.

(c) Control - Control Channels are formal systems of restricted access established to protect the sensitive aspects of sources and methods and analytical procedures of foreign intelligence programs. Examples of Control Channels are: COMINT Channels (HVCCO) and TK Channels.

(d) Compartments/Code words - A Compartment is one of the divisions into which Sensitive Compartmented Information (SCI) is separated in order to control access, distribution, and protection. SCI is information requiring special Intelligence Community controls indicating restricted handling within present and future Community intelligence collection programs and their end products. A special access authorization is required for each compartment. Examples of Compartments are: SI, G, and TK. Multiple Compartments may be handled within a single Control Channel. Generally, each compartment has one or more unique code words associated with it to identify the information as belonging to that compartment. Code words are generally classified and/or handled within specific Control Channels; therefore, no examples are given here.

(e) Agency/Office, Phone, Content, and Comments - The balance of the items on the data descriptor label may be used to

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 35 - 52

record information pertinent to each division's environment.

EFFECTIVE: 08/18/97

35-9.4.11 Manual Security Classification Reviews

Printouts must be reviewed manually (even if the system initially prints the classification level) to ensure they are appropriately marked with classification and control caveats.

EFFECTIVE: 07/26/95

35-9.4.12 Processing Sensitive Compartmented Information

FBI ADPT operations involving SCI must be conducted in accordance with the provisions of Director of Central Intelligence Directive (DCID) No. 1/16 "Security Policy for Uniform Protection of Intelligence Processed in Automated Systems and Networks." ADPT systems used to process SCI must be housed in accredited Sensitive Compartmented Information Facilities (SCIFs). A list of currently accredited SCIFs is maintained by the SPM. SCI must not be stored on nonremovable ADPT storage media, except in accredited SCIFs approved for the open storage of SCI. The FBI ADPT Security Officer must be contacted prior to the development or operation of any system that will process SCI.

EFFECTIVE: 07/26/95

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 35 - 53

35-9.4.13 Reuse of Computer System Media

(1) ADPT equipment and storage media that has processed FBI information may only be reused (e.g., transferred to another unit) within FBI control systems (i.e., formal access programs, SCIF, and TEMPEST) after they have been cleared by FBI employees.

(2) The following conditions must be met:

(a) The microcomputer or ADPT storage media remains labeled and secured to the highest level of information ever entered into, stored on, or processed by the device.

(b) When equipment or media is reused by a new user group (e.g., transfer between squads), the ADPT storage media and nonvolatile memory devices must be cleared by the Computer Specialist.

(c) ADPT storage media (removable and nonremovable) may be cleared in the field by FBIHQ approved means as defined by the ADPTSO and approved by the SPM.

(3) Regardless of the clearing process, a microcomputer which has been used to process classified information may not be removed from its operational environment without the written approval of the ADPTSO or the SPM. The microcomputer must continue to be secured commensurate with the highest classification level of information ever entered into, stored on, or processed by the system until the system has been sanitized and declassified.

EFFECTIVE: 08/04/97

35-9.4.14 Disposal of Computer System Media (See MIOG, Part II, 35-9.4.4, 35-9.4.5, 35-9.4.18 & 35-13.)

(1) If the equipment is to be released from the classified control system or disposed of by the FBI, it must first be declassified. Microcomputer equipment which has processed sensitive or classified information may not be released from FBI control until the equipment is declassified (downgraded to UNCLASSIFIED). If the SCMPM cannot formally declassify the microcomputer, release or disposal of the equipment must be through FBIHQ. The following conditions must be met:

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 35 - 54

(a) Generally, there are two ways to sanitize magnetic media - overwrite or degauss. Overwrite procedures designed to declassify media are stricter than the clearing process designed for use where the media will remain within FBI control systems. Both methods require verification that they were successful. In addition, technological advances in magnetic media may render certain techniques/procedures ineffective. Therefore, the sanitization method must be approved in writing by the SPM.

(b) A microcomputer system may be formally declassified by an original classification authority of the Division after review by the Division Security Countermeasures Program Manager only if all the following conditions are met:

1. The microcomputer system does not contain nonvolatile memory or nonremovable ADPT storage devices.
2. All volatile memory is sanitized by turning off the microcomputer.
3. All removable ADPT storage devices and printer ribbons are removed.
4. The microcomputer is not connected to any FBI network.

(c) When inoperable, diskettes, tape cartridges, printouts, ribbons and similar items used to process sensitive or classified information must be destroyed in accordance with MIOG, Part II, Section 26-15.

(d) When inoperable, hard disks used to process sensitive or classified information must be sent to FBIHQ for proper disposal following procedures provided in MIOG, Part II, Section 26-7.2, pertaining to mail services.

(3) The use of and return of any demonstration systems from vendors must be coordinated with the ADPT Security Officer and the Chief, Property Procurement and Management Section, Finance Division.

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 35 - 55

EFFECTIVE: 07/26/95

35-9.4.15 Facsimile

(1) Sensitive and classified information should only be transmitted via a secure facsimile system.

(2) Use of facsimile modems on any FBI ADPT system must follow the approval process defined for modems as discussed in Section 35-9.4.8.

EFFECTIVE: 07/26/95

35-9.4.16 Voice Mail Systems

Because there are no recognized standards for voice mail systems, these systems have not been built to meet standard security specifications and are not considered to be secure systems. These systems are, in fact, susceptible to unauthorized access. Therefore, any message left on a voice mail system should contain the minimal amount of information possible. Do not leave any information on a voice mail system that, if compromised, could damage the mission of the FBI or endanger lives. All suspected unauthorized access attempts shall be reported to the SCMPM.

EFFECTIVE: 07/26/95

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 35 - 56

35-9.4.17 Bureau Work Performed at Home

(1) Use of an FBI portable computer (e.g., laptop, notebook) at home is authorized if usage is in keeping with the policy stated in Section 35-9.4.6.

(2) Use of other ADPT equipment (whether Bureau equipment or personally owned equipment) at home must meet the requirements for all FBI ADPT systems that are discussed in this policy, to include the system security plan, risk analysis, contingency plan, certification, standard security procedures, and accreditation as discussed in Section 35-8.2. Although it is technically feasible to address these requirements, it is generally cost prohibitive to conduct these activities for individual systems. Therefore, use of ADPT equipment to process Bureau work at home is actively discouraged unless it is an operational necessity.

(3) Under the following conditions, the STU-III, Type 1, a secure telephone unit designed specifically for the secure transmission of Sensitive but Unclassified and National Security Information, may be approved by the ADPT Security Staff, NSD, for the installation in an FBI employee's private residence located in the United States only. An electronic communication should be directed to the ADPT Security Officer, NSD, requesting approval.

(a) The Assistant Director in Charge, Assistant Director, or SAC must approve, in writing, the operational need for the installation of a STU-III, Type 1, in the employee's residence.

(b) STU-III, Type 1, installation is approved for the transmission of conversations (voice) up to, and including, Top Secret. No Sensitive Compartmented Information will be approved for transmission from a private residence. This policy does not apply to the transmission of data.

(c) When the STU-III is in an unkeyed state, the equipment must be protected in a manner that is sufficient to preclude any reasonable chance of theft, sabotage, or tampering. When not in use, the Crypto-Ignition Key (CIK) must be locked up or retained in the custody of the authorized FBI employee. The room in which the equipment is installed must prevent eavesdropping. In addition, Sensitive but Unclassified and NSI conversations must be held in the presence of authorized personnel only, that is, personnel with appropriate clearances and need to know. The STU-III must be installed in a room that can meet these requirements.

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 35 - 57

EFFECTIVE: 08/28/97

35-9.4.18 Use of Non-Bureau-Owned ADPT Systems

(1) Use of personally owned, leased, or loaned equipment (e.g., equipment provided by a local police department as part of a JTF) to support the processing of Bureau information must meet all provisions of this policy. The following additional restrictions apply:

(a) Under no circumstances will personally owned, leased, or loaner equipment or media be used to process classified information.

(b) To the extent possible, information should be stored on FBI-owned storage media. Provisions should be made which allow for FBI retention of nonremovable, nonvolatile storage device (e.g., microcomputer hard drives) if the device cannot be successfully sanitized as discussed in Section 35-9.4.14.

(2) For security reasons, placement and removal of microcomputers and related media to operational environments where classified information is processed must be approved by the responsible Security Countermeasures Program Manager or the FBI Security Programs Manager.

EFFECTIVE: 07/26/95

35-9.5 Emanations Security (See MIOG, Part II, 35-9.3.2.)

(1) ADPT systems, including but not restricted to microcomputers and communications switches, used to process classified information must meet national TEMPEST standards for the specific operational and physical environment in which they are operated. In many instances, these standards may be met with commercial equipment.

(2) The Section Chief of the Technical Operations Section, IRD, provides policy and guidance on Technical Surveillance Countermeasures (TSCM) and emanations security. The Technical

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 35 - 58

Programs Unit conducts TEMPEST certifications.

(3) Network and Information Systems Support Unit (NISSU), OMS, IRD is responsible for ensuring the provisions of NACSIM 5203, "Guidelines for Facility Design and Red/Black Installation (U)," June 30, 1982 and Appendix B to NACSIM 5204, "NSA Specifications for RF Shielded Enclosures for Communications Equipment General Specifications," are met with respect to addressing the telecommunications aspects of this program. (NISSU) defines the requirements, develops the specifications and conducts inspections. These activities are coordinated with the SPM.

EFFECTIVE: 11/28/97

35-9.6 Communications Security

The FBI's ADPT security program relies on a related program, the communications security program, to protect telecommunications systems. Communications security (COMSEC) is defined as all measures which are taken to prevent recovery of information while it is being transmitted by telecommunications equipment. All communications circuits used to interconnect remotely located components of FBI ADPT systems which process, store or transmit classified or sensitive information require consideration of COMSEC measures.

EFFECTIVE: 07/26/95

35-10 SECURITY INCIDENTS AND VIOLATIONS

(1) A security incident is a condition that has the potential to impact the security of an ADPT system, such as any attempt to gain unauthorized access to information, virus infection, or loss or theft of computer media. Security incidents may result from intentional or unintentional activities. ADPT security-related incidents should be reported to the FBI ADPT Security Officer by the CSSO or SCMPM, as appropriate. The FBI ADPT Security Officer will address the impact of the security incidents on the system's

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 35 - 59

accreditation status and recommend additional security countermeasures to reduce generic risks. In addition, DOJ requires that all malicious software incidents of DOJ automated information systems, including mainframes, microcomputers, networks, or personal computers, be documented and reported. For reporting purposes, malicious software incidents include any detection of malicious software, whether detected on magnetic media prior to entry into an FBI ADPT system or after infection of the system, and any actual execution of malicious software. The ADPT Security Officer will maintain the appropriate records and fulfill the DOJ reporting requirements on behalf of the SPM. DOJ will use this information to determine the extent of problems in the Department.

(2) FBI employees are subject to disciplinary action for violation of FBI ADPT security policy. Such violations may invoke FBI disciplinary action even if they are not criminally pursued. Reportable ADPT security-related violations are addressed in the MAOP, Part I, Section 13-13, "Schedule of Disciplinary Offenses and Penalties for FBI Employees," and should be reported as specified in the MAOP. Sanctions for noncompliance are also provided in the MAOP. It should be noted that reporting violations to the ADPT Security Officer does not relieve the responsibility for reporting to ASU or OPR, as defined in the MAOP.

(3) Any person who knowingly, willfully, or negligently discloses information to unauthorized persons will be subject to the appropriate penalties and sanctions under the law (i.e., Privacy Act, Computer Fraud and Abuse Act, National Security Act, or appropriate espionage statutes).

(4) Non-FBI employees who violate this policy are subject to having their access to FBI ADPT systems and facilities terminated.

EFFECTIVE: 07/26/95

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 35 - 60

35-11 REGULATIONS/LAWS GOVERNING ADPT SECURITY (See MIOG, Part II, 35-2, 35-5.)

(1) Title 5, U.S. Code, 552a, "Privacy Act of 1974," (Public Law 93-579), December 31, 1974

(2) Title 5, Code of Federal Regulations (CFR), Part 930, Subpart C, "Employees Responsible for the Management of Use of Federal Computer Systems"

(3) Title 31, U.S. Code, 1105, 1113, 3512, "Federal Managers' Financial Integrity Act of 1982," (Public Law 97-255), September 8, 1982 (FMFIA)

(4) Title 18, U.S. Code, 1030, "Computer Fraud and Abuse Act of 1986," (Public Law 99-474), October 16, 1986

(5) Title 18, U.S. Code, 2701, "Electronic Communications Privacy Act of 1986," (Public Law 99-508), October 21, 1986

(6) Title 40, U.S. Code, 759, "Computer Security Act of 1987" (Public Law 100-235), January 8, 1988

(7) Title 41, CFR, 201, Federal Information Resources Management Regulation (FIRM)

(8) Title 44, U.S. Code, 3501-3520, "The Paperwork Reduction Act of 1980" (Public Law 96-511), December 11, 1980

(9) Department of Justice (DOJ) Order 2640.2C, "Telecommunications and Automated Information Systems Security," June 25, 1993

(10) Department of Justice (DOJ) Order 2830.1D, "Automated Information Systems Policies," October 3, 1986

(11) Department of Justice, "Simplified Risk Analysis Guidelines (SRAG)," May 18, 1990

(12) Director of Central Intelligence Directive (DCID) No. 1/14, "Minimum Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information," January 22, 1992

(13) Director of Central Intelligence Directive (DCID) No.

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 35 - 61

1/16, "Security Policy for Uniform Protection of Intelligence Processed in Automated Information Systems and Networks," July 19, 1988

(14) Director of Central Intelligence Directive (DCID) No. 1/21, "Manual for Physical Security Standards for Sensitive Compartmented Information Facilities (SCIFs)," January 30, 1994

(15) Executive Order 12958 (E.O. 12958), "National Security Information," April 20, 1995

(16) Federal Information Processing Standards Publication, FIPS PUB 65, "Guidelines for Automatic Data Processing Risk Analysis"

(17) Federal Information Processing Standards Publication, FIPS PUB 87, "Guidelines for ADP Contingency Planning"

(18) Federal Information Processing Standards Publication, FIPS PUB 112, "Password Usage"

(19) Government Accounting Office (GAO) "Policy and Procedures Manual for Guidance of Federal Agencies - Title II - Accounting"

(20) National Security Council/Policy Coordinating Committee, National Security Directive 42 (NSD 42), "National Policy for the Security of National Security Telecommunications and Information Systems," July 5, 1990

(21) National Telecommunications and Information Systems Security Directive (NTISSD) No. 500, "Information Systems Security (INFOSEC) Education, Training, and Awareness," February 25, 1993

(22) National Telecommunications and Information Systems Security Instruction (NTISSI) No. 7000, "Tempest Countermeasures for Facilities," November 29, 1993

(23) National Telecommunications and Information Systems Security Policy (NTISSP) No. 200, "National Policy on Controlled Access Protection," July 15, 1987

(24) National Telecommunications and Information Systems Security Policy (NTISSP) No. 300, "National Policy on Control of Compromising Emanations," November 29, 1993

(25) NIST Special Publication 500-174, "Guide for

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 35 - 62

Selecting Automated Risk Analysis Tools," October 1989

(26) Office of Management and Budget (OMB) Circular A-123,
"Internal Control Systems," August 4, 1986

(27) Office of Management and Budget (OMB) Circular A-127,
"Financial Management Systems," December 19, 1984

(28) Office of Management and Budget (OMB) Circular A-130,
"Management of Federal Information Sources," June 25, 1993

(29) Office of Management and Budget (OMB) Bulletin
90-08, "Guidance for Preparation of Security Plans for Federal
Computer Systems that Contain Sensitive Information"

(30) Department of Defense (DoD) 5200.28-STD, "Department
of Defense Trusted Computer System Evaluation Criteria"

(31) National Computer Security Center Technical Guide 005
(NSC-TG-005), "Trusted Network Interpretation of the Trusted Computer
System Evaluation Criteria"

(32) National Computer Security Information Memorandum
(NACSIM) 5203, "Guidelines for Facility Design and Red/Black
Installation (U)," June 30, 1982

(33) Appendix B to NACSIM 5204, "NSA Specifications for RF
Shielded Enclosures for Communications Equipment General
Specifications (U)"

EFFECTIVE: 07/26/95

35-12 GLOSSARY OF TERMS (See MIOG, Part II, 35-3.)

(1) Access - the capability and opportunity to gain
knowledge of, or to alter information or materials, including the
ability and means to communicate with (i.e., input or receive output),
or otherwise make use of any information, resource, or component in a
computer system.

(2) Access Control - the process of limiting access to
the resources of a system to only authorized persons, programs,

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 35 - 63

processes, or other systems. Synonymous with controlled access and limited access.

(3) Accreditation - the official management authorization for operation of an ADPT system which provides a formal declaration by an accrediting authority that a computer system is approved to operate in a particular security mode using a prescribed set of safeguards. Accreditation is based on the certification process, as well as other management considerations. An accreditation statement affixes security responsibility with the accrediting authority and shows that proper care has been taken for security.

(4) Accrediting Authority - the official who has the authority to decide on accepting the security safeguards prescribed for a computer system or that official who may be responsible for issuing an accreditation statement that records the decision to accept those safeguards. The Senior Executive Service personnel designated by the Director, FBI, are the authorized accrediting authorities.

(5) Automated Data Processing Telecommunications (ADPT) System - an assembly of hardware, software, and/or firmware configured to collect, create, communicate, compute, disseminate, process, store, and/or control information in an automated fashion. An ADPT system must be under the same direct management control with essentially the same function, reside in the same environment and have the same characteristics and security needs. Examples of ADPT systems include, but are not limited to: mainframe, minicomputer, microcomputer, local and wide area networks, connectivity and control hardware/firmware and application systems.

(6) ADPT Security - measures or controls that safeguard or protect an ADPT system against unauthorized (accidental or intentional) disclosure, modification, destruction of ADPT system and data, or denial of service. ADPT system security includes consideration of all hardware and/or software functions, characteristics, and/or features; operational procedures, accountability procedures, and access controls at all computer facilities; management constraints; physical structures and devices; and personnel and communication controls needed to provide an acceptable level of risk for the ADPT and for the data contained in the system.

(7) Authorization - the privileges and permissions granted to an individual by a designated official to access or use a program, process, information, or system. These privileges are based on the individual's clearance and need-to-know.

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 35 - 64

(8) Authorized Person - a person who has the need-to-know for classified or sensitive information in the performance of official duties and who has been granted a personnel security clearance or authorized access at the required level. The responsibility for determining whether a prospective recipient is an AUTHORIZED PERSON rests with the person who has possession, knowledge, or control of the classified or sensitive information involved, and not with the prospective recipient.

(9) Audit Trail - a chronological record of system activities that enables the reconstruction and examination of the sequences of events and/or changes in an event.

(10) Authenticate - the process to verify the identity of a user, device, or other entity in a computer system, often as a prerequisite to allowing access to resources in a system.

(11) Availability - the property of being accessible and usable upon demand by an authorized entity. Required ADPT services must remain available to authorized users operating within the same security constraints that make these services unavailable to unauthorized users.

(12) Certification - the comprehensive security test and evaluation of the technical and nontechnical security features of a computer system and other safeguards, made in support of the accreditation process, that establishes the extent to which a particular design and implementation meet a specified set of security requirements.

(13) Classified - any information that has been determined, pursuant to Executive Order 12958 or any predecessor order, to require protection against unauthorized disclosure and is so designated.

(14) Clearing - the process of removing information recorded on an ADPT storage media and nonvolatile memory devices. Clearing cannot be used to downgrade/declassify ADPT storage media or nonvolatile memory. Clearing can be performed in the field using FBIHQ-approved means and is used when the microcomputer and ADP storage media remain in FBI control.

(15) Compartmented Security Mode - an operational method where each user with direct or indirect individual access to a computer system, its peripherals, and remote terminals or hosts meets

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 35 - 65

all the following criteria:

- (a) a valid personnel security clearance for the most restricted information in the computer system.
- (b) formal access approval, and has signed nondisclosure agreements, for that information to which that user is to have access.
- (c) a valid need-to-know for that information to which that user is to have access.

(16) Communications Security (COMSEC) - the protective measures taken to deny unauthorized persons information derived from telecommunications and ensure the authenticity of such communication. Communications security includes crypto security, transmission security, and physical security of COMSEC material.

(17) Compromise - the disclosure of classified or sensitive information to persons not authorized access or having a need-to-know.

(18) Compromising Emanations - unintentional signals that, if intercepted and analyzed, would disclose the information transmitted, received, handled, or otherwise processed by telecommunications or automated information systems equipment.

(19) Confidentiality - sensitive data that are held in confidence and are protected from unauthorized disclosure. FBI ADPT systems support a range of unclassified, sensitive and classified National Security Information, up to and including TOP SECRET code word material.

(20) Configuration Management (CM) - an approach for specifying, documenting, controlling, and maintaining the visibility and accountability of all appropriate hardware, software, firmware, communications interfaces, operating procedures, installation structures, and all changes thereto.

(21) Contingency Plan - an emergency response plan, backup operations plan, and post-disaster recovery plan, maintained by an activity as a part of its security program, that will ensure the availability of critical resources and facilitate the continuity of operations in an emergency situation. Synonymous with disaster plan and emergency plan.

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 35 - 66

(22) Declassification - a formal statement that a microcomputer system or its media is UNCLASSIFIED.

(23) Dedicated Security Mode - an operational method when each user with direct or indirect individual access to a computer system, its peripherals, and remote terminals or hosts meets all the following criteria:

(a) a valid personnel security clearance for all information on the system.

(b) a valid need-to-know for all information contained within the system.

(c) for classified systems, formal access approval, and signed nondisclosure agreements for all the information stored and/or processed (to include all compartments, subcompartments, and/or special access programs).

(24) Dedicated System - a system that is specifically and exclusively dedicated to and controlled for a specific mission, either for full-time operation or a specified period of time.

(25) Denial of Service (DOS) - the prevention of authorized access to resources or the delaying of time-critical operations. DOS refers to the inability of an ADPT system or any essential part to perform its designated mission, either by loss of, or degradation of operational capability.

(26) Department of Defense (DoD) Trusted Computer System Evaluation Criteria - a document published by the National Computer Security Center containing a uniform set of basic requirements and evaluation classes for assessing degrees of assurance in the effectiveness of hardware and software security controls built in the design and evaluation of systems. These criteria are intended for use in the design and evaluation of systems that will process and/or store sensitive or classified data. This document is also referred to as the "Orange Book."

(27) Encryption - the process of transforming data to an unintelligible form to conceal its meaning in such a way that the original data cannot be obtained without using the inverse decryption process.

(28) Environment - the aggregate of external procedures, conditions, and objects that affect the development, operation, and

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 35 - 67

maintenance of a system.

(29) FBINET - The FBI Network that provides secure communications for the FBI Data Network supporting classified automated applications up to the SECRET noncode word level.

(30) Identification - the process that enables recognition of an entity by a system, generally by the use of unique machine readable user names.

(31) IISNET - the Intelligence Information System Network that provides secure communications for the FBI Data Network supporting classified automated applications to include TOP SECRET code word material.

(32) Individual Accountability - the ability to associate positively the identity of a user with the time, method, and degree of access to a system.

(33) Industrial Security - the management, control and safeguard of FBI information entrusted to contractors.

(34) Information Security - the protection of information systems against unauthorized access to or modification of information, whether in storage, processing or transit, and against the denial of service to authorized users or the provision of service to unauthorized users, including those measures necessary to detect, document, and counter such threats.

(35) Integrity - computerized data that is the same as those in the source documents and has not been exposed to accidental or malicious alteration or destruction. The information processing must ensure the data is accurate, timely, and complete to support the FBI's investigative, law enforcement, and administrative support requirements. Inaccurate data could lead to uninformed decisions and adversely impact investigations.

(36) Interconnected System - an approach in which the network is treated as an interconnection of separately created, managed, and accredited computer systems.

(37) Label - the marking of an item of information that reflects its security classification. An internal label is the marking of an item of information that reflects the classification of that item within the confines of the medium containing the information. An external label is a visible or readable marking on

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 35 - 68

the outside of the medium or its cover that reflects the classification of the information resident within that particular medium.

(38) Least Privilege - the principle that requires each subject be granted the most restrictive set of privileges needed for the performance of authorized tasks. The application of this principle limits the damage that can result from accident, error, or unauthorized use.

(39) Microprocessor - a semiconductor central processing unit contained on a single integrated circuit chip.

(40) Mode of Operation - a description of the conditions under which a computer system functions, based on the sensitivity of data processed and the clearance levels and authorizations of the users.

(41) Multilevel Security Mode - an operational method where each user with direct or indirect individual access to a computer system, its peripherals, and remote terminals or hosts meets all the following criteria:

(a) some users do not have a valid personnel security clearance for all the information processed in the computer system.

(b) all users have the proper clearance and have the appropriate formal access approval for that information to which they have access.

(c) all users have a valid need-to-know for that information to which they have access.

(42) Need-to-Know - a determination by the owner of sensitive and/or classified information that a prospective recipient has a requirement for access to, knowledge of, or possession of the information in order to perform tasks or services essential to carry out official duties.

(43) Nonvolatile Memory Units - devices which continue to retain their contents when power to the unit is turned off (e.g., bubble memory, Read Only Memory - ROM).

(44) Overwrite Procedure - process which removes or destroys data recorded on a computer storage medium by writing

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 35 - 69

patterns of data over, or on top of, the data stored on the medium.

(45) Password - a protected and private character string used to authenticate.

(46) Personnel Security Clearance - an administrative determination, in compliance with Executive Order 10450, that an individual is eligible from a security point of view for access to classified information of the same or lower category as the level of the personnel clearance being granted.

(47) Personnel Security - the procedures established to ensure that all personnel who have access to any sensitive information have all required authorities as well as all appropriate clearances.

(48) Physical Security - the application of physical barriers and control procedures as preventative measures or countermeasures against threats to resources and information.

(49) Purge - the removal of data from computer system storage devices in such a way that there is assurance, proportional to the sensitivity of the data, that the data cannot be reconstructed.

(50) Residual Risk - the portion of risk that remains after security measures have been applied.

(51) Risk Analysis - the process of identifying security risks, determining their magnitude, and identifying areas needing safeguards. Risk analysis is a part of the risk management process.

(52) Risk Management - the total process of identifying, controlling, and eliminating or minimizing uncertain events that may affect system resources. It includes risk analysis, cost benefit analysis, and effectiveness reviews.

(53) SAMNET - the SAMNET is the FBI's Command and Control Network which provides for distribution between FBI divisions of classified administrative narrative traffic to include the TOP SECRET code word material.

(54) Sanitization - the technical elimination of all information from ADPT storage media and nonvolatile memory devices so they can be formally certified as declassified by appropriate authorities.

(55) Secure Configuration Control - the set of procedures

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 35 - 70

appropriate for controlling changes to a system's hardware and software structure for the purpose of ensuring that changes will not lead to violations of the system's security policy.

(56) Security Countermeasures - the protective measures and controls that are prescribed to meet the security requirements specified for a system. Those safeguards may include, but are not necessarily limited to: hardware and software security features; operating procedures; accountability procedures; access and distribution controls; management constraints; personnel security; and physical structures, areas, and devices. Also called safeguards or security controls.

(57) Security Requirements - types and levels of protection necessary for equipment, data, information, applications, and facilities to meet security policies.

(58) Security Specifications - a detailed description of the security countermeasures/safeguards required to protect a system.

(59) Security Violation - an event which may result in disclosure of sensitive or classified information to unauthorized individuals, or that results in unauthorized modification or destruction of system data, loss of computer system processing capability, or loss or theft of any computer system media.

(60) Sensitive but Unclassified Information - refer to Sensitive Information.

(61) Sensitive Compartmented Information (SCI) - classified information about or derived from intelligence sources, methods, or analytical processes that is required to be handled exclusively within formal access control systems established by the Director, Central Intelligence (DCI).

(62) Sensitive Compartmented Information Facility (SCIF) - an accredited area, room, group of rooms or installation where SCI may be stored, used, discussed, and/or electronically processed.

(63) Sensitive Information - information that requires protection due to the risk or magnitude of loss or harm that could result from inadvertent or deliberate disclosure, modification and/or destruction of the information. The term includes information, the improper use or disclosure of which could adversely affect the ability of the FBI to accomplish its mission; information that is investigative in nature; grand jury information subject to the Federal

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 35 - 71

Rules of Criminal Procedure, Rule 6(e), Grand Jury Secrecy of Proceedings and Disclosure; proprietary information; records about individuals requiring protection under the Privacy Act; information not releasable under the Freedom of Information Act; and information which could be manipulated for personal profit or to hide the unauthorized use of money, equipment, or privileges. Also referred to as Sensitive but Unclassified Information and Limited Official Use Information.

(64) Standard Security Procedures - step-by-step security instructions tailored to users and operators of computer systems which process sensitive or classified information.

(65) Standalone System - a single user system not connected to any other systems.

(66) System High Security Mode - an operational method where each user with direct or indirect individual access to a computer system, its peripherals, and remote terminals or hosts meets all the following criteria:

(a) a valid personnel security clearance for all information on the computer system.

(b) a valid need-to-know for some of the information contained within the system.

(c) for classified systems, formal access approval, and signed nondisclosure agreements for all the information stored and/or processed (to include all compartments, subcompartments, and/or special access programs).

(67) System Integrity - the quality that a system has when it performs its intended functions in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.

(68) Telecommunications - the preparation, transmission, communication, or related processing of information (i.e., writing, images, sounds or other data) by electrical, electromagnetic, electromechanical, electrooptical, or electronic means.

(69) TEMPEST - short name referring to investigation, study, and control of compromising emanations from telecommunications and automated information systems equipment. (See Compromising Emanations.)

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 35 - 72

(70) Threat - the means through which a weakness can be exploited to adversely affect an ADPT system, facility, network, or operation. Threats can be categorized as human or environmental in origin and include sabotage, espionage, natural disasters, data disclosure, data destruction, hardware/software failure, etc.

(71) Trusted Computing Base (TCB) - totality of protection mechanisms within a computer system, including hardware, firmware, and software, the combination of which is responsible for enforcing a security policy. The ability of a trusted computing base to enforce correctly a unified security policy depends on the correctness of the mechanisms within the trusted computing base, the protection of those mechanisms to ensure their correctness, and the correct input of parameters related to the security policy.

(72) Volatile Memory Units - devices which do not retain their contents when the power to the unit is turned off (e.g., Random Access Memory - RAM). Volatile memory units become UNCLASSIFIED when the system is turned off.

(73) Vulnerability - a potential weakness in an existing or planned security control environment whose exploitation may impact the confidentiality, integrity, and/or availability of a specific resource or mission.

EFFECTIVE: 07/26/95

35-13

COMPUTER SECURITY AWARENESS CHECKLIST

OFFICIAL BUSINESS ONLY - FBI computer systems, both mainframes and microcomputers, are for official business only. You have NO EXPECTATION OF PRIVACY in their use.

AUDIT OF USER ACTIVITIES - All systems transactions are subject to recording and routine review for inappropriate or illegal activity conducted.

SANCTIONS - A violation of security requirements could result in termination of system access privileges and serious disciplinary action, possibly removal. In addition, Title 18, USC, Section 1030 provides criminal penalties for any person illegally accessing a government-owned or -operated computer.

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 35 - 73

CLASSIFICATION - A microcomputer and associated magnetic media is classified at the highest level of information that has been entered into, stored on, or produced by the system unless the system can be appropriately declassified. The microcomputer must be labeled, secured, and operated commensurate with its classification level. FBI PORTABLE microcomputers are authorized to process classified information up to and including Secret/Collateral within the U.S. and its territories and can be connected to the FBI Secure Network (FBINET). The processing of Top Secret and SCI information is not authorized on portable microcomputers without written authorization by the FBI's Security Programs Manager (SPM). (See MIOG, Part II, 35-9.4.9.)

LABELS - Removable ADPT storage media must be marked with a classification and a data descriptor label. Microcomputers with nonremovable ADPT storage devices must conspicuously display a classification and a data descriptor label on the unit that contains the magnetic ADPT storage device. Portable microcomputers are exempt from this provision. (See MIOG, Part II, 35-9.4.10.)

STORAGE - All ADPT storage media must be labeled and secured in accordance with existing policies.

PROTECT AGAINST DISASTER - Back up all your data files on a regular basis, according to your division's "END-USER AUTOMATED DATA PROCESSING CONTINGENCY PLAN."

DOWNGRADING/DECLASSIFYING - ADPT storage media (operative and inoperative, removable and nonremovable) and nonvolatile memory devices may NEVER be downgraded or declassified in the field.

EQUIPMENT AND MEDIA DISPOSAL - Microcomputer equipment which has processed sensitive or classified information may not be released from FBI control until the equipment is sanitized and declassified. When inoperable, diskettes, tape cartridges, printouts, ribbons, and similar items used to process sensitive or classified information must be destroyed as classified trash. When inoperable, hard disks used to process sensitive or classified information must be sent to FBIHQ for proper disposal. (See MIOG, Part II, 35-9.4.14.)

MAINTENANCE - All maintenance must be performed only by properly cleared persons and must be supervised by FBI personnel knowledgeable in the operation of microcomputers. Vendor diagnostic software used on any FBI microcomputer may not be removed from FBI-controlled environment. All electronic, storage, and memory devices associated with FBI microcomputers must remain in FBI-controlled space and may

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 35 - 74

never be returned to the vendor for "trade-in" or credit purposes.

[ADPT] storage media and microcomputers with nonremovable [ADPT] storage media must be transferred for off-site maintenance only through FBIHQ control channels. (See MIOG, Part II, 35-9.4.5.)

PHYSICAL CONTROL - FBI microcomputers which process sensitive or classified information must be operated only in FBI-controlled space and under the direct supervision of authorized persons. When not under the direct supervision of an authorized person either during or outside regular working hours, FBI microcomputers must be: turned off; diskettes, tapes, removable hard disks, and printer ribbons must be labeled, removed, and secured. Microcomputers with nonremovable

[ADPT] storage media and nonvolatile memory devices operated in areas that are not staffed 24 hours a day (e.g., resident agencies, off-sites) must not be used to process or store classified information. To the extent possible, PORTABLE microcomputers should be kept in the possession of the individual to whom they are issued or charged out. PORTABLE computers which must be left unattended for any amount of time must be properly secured. (See MIOG, Part II, 35-9.4.6.)

SOFTWARE CONTROLS - All software used on FBI microcomputers must be obtained through either: the Operations Management Section, Information Resources Division, FBIHQ, or appropriate FBI procurement channels.

INTRODUCTION OF NON-FBI DATA - Introduction of non-FBI data (e.g., transcripts from United States Attorneys, information from Joint Task Force agencies) must be approved in writing by the SAC as an operational necessity, and all magnetic media must be scanned for viruses prior to use. (See MIOG, Part II, 35-9.4.4.)

SENSITIVE COMPARTMENTED INFORMATION (SCI) - FBI ADPT operations involving SCI must be conducted in accordance with the provisions of Director of Central Intelligence Directive (DCID) No. 1/16, "Security Policy for Uniform Protection of Intelligence Processed in Automated Systems and Networks."

TEMPEST - A microcomputer used to process classified information must meet national TEMPEST standards. FBIHQ provides TEMPEST certifications. Any change to the approved configuration, including internal components or external devices, or relocation of the microcomputer invalidates the TEMPEST certification.

TELECOMMUNICATIONS - Unencrypted dial-up access to FBI information systems or networks is prohibited. FBI microcomputers must not be connected to any non-FBI network, public or private. All

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 35 - 75

microcomputers connected to the Integrated Digital Communications System (IDCS) (formerly the Computer Applications Communications Network (CACN)), are considered classified and must be appropriately labeled. Exceptions may only be granted by the FBIHQ ADPT Security Officer. (See MIOG, Part II, 35-9.4.8.)

BULLETIN BOARDS - A comprehensive program of monitoring electronic bulletin boards for criminal or intelligence purposes is prohibited. Any access to non-FBI electronic bulletin boards is severely restricted. (See MIOG, Part II, 35-9.4.8.)

MAINFRAME ACCESSOR IDs AND PASSWORDS - Each user is assigned a unique accessor ID for identification and a unique password to be used for authentication. Accessor IDs may be publicly known, passwords must be kept secret. It is your responsibility to protect your password. Passwords serve as an "electronic signature" on all system transactions for which they are used. You will be held responsible if someone else uses your password in connection with a system transaction.

Your password is for your use only. Lending it to someone else is a security violation and may result in disciplinary action against both parties.

Never disclose your password to anyone. Memorize it; do not put it in writing. Safeguard it. Your password is the key to one of the FBI's most valuable resources.

If you forget your password, notify your Computer Specialist. Your old password will be deleted from the system and a new one issued.

Immediately following a suspected or known compromise of a system password, a new password will be issued and the compromised password deleted from the system.

When a system user no longer needs access, the password will be removed from the system.

If you leave the terminal unattended for any reason, log off. An unattended terminal is vulnerable to masquerading. Any user signed on to a terminal which has been inactive for a period of 30 minutes will be automatically signed off. You must reidentify yourself by reestablishing the session. (See MIOG, Part II, 35-9.4.2.)

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 35 - 76

REPORT SECURITY VIOLATIONS - If you become aware of any violation of these requirements or suspect that your password may have been used by someone else, it is your responsibility to report that information immediately to your respective Division Security Officer, field office or FBIHQ Computer Specialist.

If you have any questions about the proper operation or security of computer systems entrusted to you, contact a field office or FBIHQ Computer Specialist or Division Security Officer.

EFFECTIVE: 08/18/97

35-13.1 Notice of Responsibilities and Computer Security Awareness Certification (See MIOG, Part II, 35-8.3)

You have been entrusted with the management, operation, or use of a Federal Bureau of Investigation (FBI) computer system processing sensitive and/or classified information. Both you and the FBI have responsibility pursuant to the Computer Security Act of 1987 to protect sensitive information and under 28 CFR, Part 17, to protect classified information. Specific responsibilities are set forth in Manual of Investigative Operations and Guidelines (MIOG), Part II, Section 16-18, "FBI MICROCOMPUTER POLICY;" MIOG, Part II, Section 35, "FBI AUTOMATED DATA PROCESSING AND TELECOMMUNICATIONS SECURITY POLICY;" and in MIOG, Part II, Section 26, "CLASSIFIED NATIONAL SECURITY INFORMATION AND MATERIAL." At a minimum, you must follow the attached security awareness checklist as a basic guide and reminder of your responsibilities to protect the information processed and/or stored in the computer system(s) entrusted to you. For additional information about computer security, contact the field office or FBIHQ Computer Specialist or Division Security Officer.

I certify that I have read, understand, and shall comply with the practices and requirements of the preceding notice and the attached FBI Computer Security Awareness Checklist.

Signature

Date

Sensitive
PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 35 - 77

Official Bureau Name SSAN

EFFECTIVE: 08/04/97

35-13.2 Nondisclosure Agreement for Joint Task Force/Contractor
Members (FD-868) (See MIOG, Part II, 35-9.4.1.)

FD-868 (8-19-97)

(FBI SEAL)

U.S. Department of Justice

Federal Bureau of Investigation

Washington, D.C. 20535

NONDISCLOSURE AGREEMENT FOR JOINT TASK FORCE/CONTRACTOR MEMBERS
AN AGREEMENT BETWEEN _____ AND THE FBI
(Name of Individual-Printed or Typed)

As consideration for assignment in the Federal Bureau of Investigation (FBI), United States Department of Justice, and as a condition for continued assignment, I hereby declare that I intend to be governed by and I will comply with the following provisions:

1. That I am hereby advised and I understand Federal Law, including statutes, regulations issued by the Attorney General and Orders of the President of the United States, prohibit loss, misuse or unauthorized disclosure or production of information in the files of the FBI.
2. I understand that unauthorized disclosure of information in the files of the FBI or information I may acquire as a Task Force/Contractor employee of the FBI could result in impairment of national security, place human life in jeopardy, or result in denial of due process to a person or persons who are subjects of an FBI investigation, or prevent the FBI from effectively discharging its responsibilities. I understand the need for this secrecy agreement; therefore, as consideration for assignment, I agree that I will never divulge, publish, or reveal either by word or conduct, or by other means of disclosure to any unauthorized recipient without official

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 35 - 78

written authorization by the Director of the FBI or his delegate, any information from the investigatory files of the FBI or any information relating to material contained in the files, or disclose any information or produce any material acquired as a part of the performance of my official duties or because of my official status. The burden is on me to determine, prior to disclosure, whether information may be disclosed and in this regard I agree to request approval of the Director of the FBI in each such instance by presenting the full text of my proposed disclosure in writing to the Director of the FBI at least thirty (30) days prior to disclosure. I understand that this agreement is not intended to apply to information which has been placed in the public domain or to prevent me from writing or speaking about the FBI, but it is intended to prevent disclosure of information where disclosure would be contrary to the law, regulation, or public policy. I agree the Director of the FBI is in a better position than I to make that determination.

3. I agree that all information acquired by me in connection with my duties while on assignment with the FBI and all official material to which I have access remains the property of the United States of America, and I will surrender upon demand by the Director of the FBI or his delegate, or upon separation from the FBI, any material relating to such information or property in my possession. I also agree assignment to the United States of any profits resulting from the publication of information in breach of this agreement.

4. I understand that obtaining information under false pretenses or any unauthorized disclosure may be a violation of Federal law and prosecuted as a criminal offense and, in addition to this agreement, may be enforced by means of an injunction or other civil remedy. I also understand that the use of the FBI network and its automated information systems, i.e., the Automated Case Support (ACS) System, to access records other than in furtherance of authorized responsibilities will be viewed as obtaining information under false pretenses and may be in violation of the Privacy Act.

5. I agree that all the information that I will access will be for the sole purpose of authorized and lawful purposes in furtherance of the responsibilities of the particular Joint Task Force or contract under which the user is being provided access. (JTF/Contract _____)

I accept the above provisions as conditions for my assignment and continued assignment in the FBI. I agree to comply with these provisions both during my assignment in the FBI and following termination of such assignment. I have read this Agreement carefully

Sensitive

PRINTED: 02/18/98

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 35 -- 79

and my questions, if any, have been answered.

(Signature)

(Type or Print Name)

Witnessed and accepted in behalf of the Director FBI on

_____, _____, by _____
(Date) (Year) (Signature)

EFFECTIVE: 08/19/97

Sensitive
PRINTED: 02/18/98