

**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
PRINTED: 02/18/98

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
PRINTED: 02/18/98

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
PRINTED: 02/18/98

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

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

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

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]

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

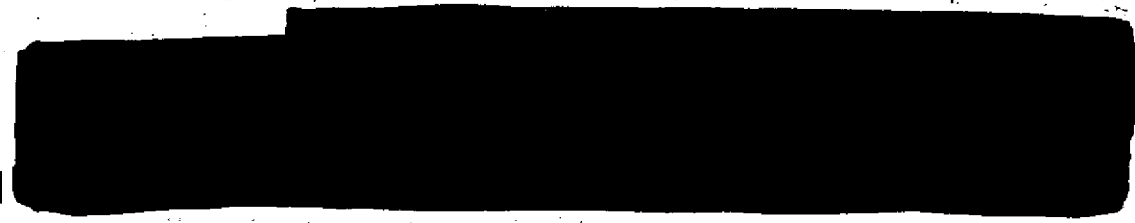

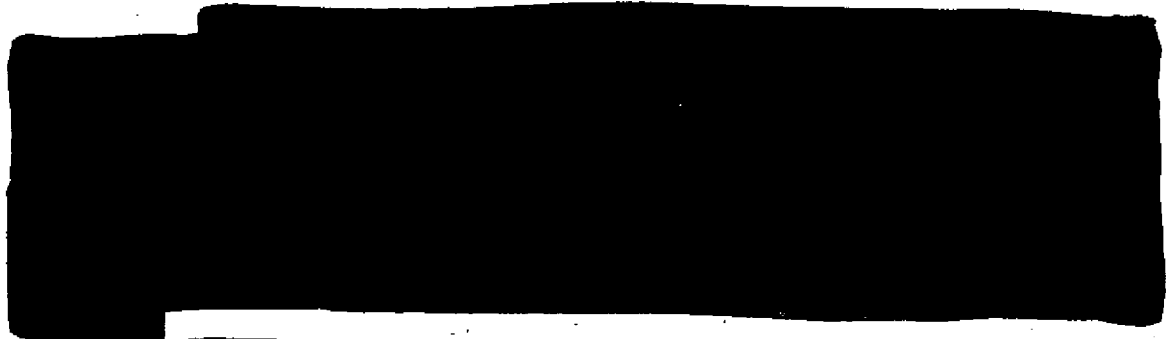

PAGE 16 - 42

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

Sensitive

PRINTED: 02/18/98

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

PAGE 16 - 52

(5) Computer Specialist Management Program

This program is responsible for the overall management of the CS Program. These responsibilities include maintenance of CS Program staffing levels; CS temporary duty staffing for major case investigations or crisis response incidents; evaluations of field CS Programs, and overseeing the recruitment, evaluation, hiring, promotion, and other related personnel actions for CSs in the field and at FBIHQ. This program also oversees the activities of the Computer Specialist Advisory Group, and coordinates the annual Technical Automation Conference.

(6) Computer Specialist Training Program

This program is responsible for the training of field and FBIHQ CSs. These responsibilities include the continued development and implementation of CS training curricula which will empower CSs with the ability to operate and maintain the FBI's existing and emerging computer hardware and software systems.

(7)

b2
b7E

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

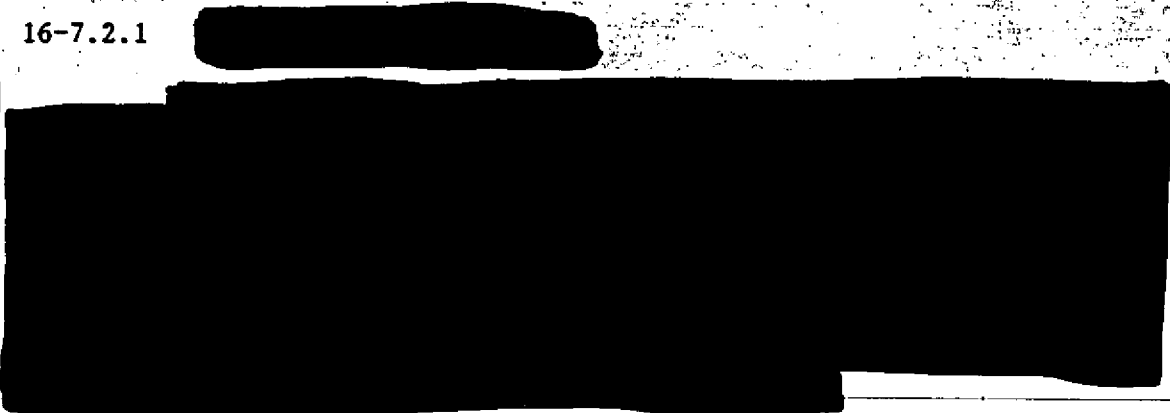
XXXXXXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X for this page X
XXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXX
XXXXXX

Sensitive

Manual of Investigative Operations and Guidelines
Part II

PAGE 16 - 54

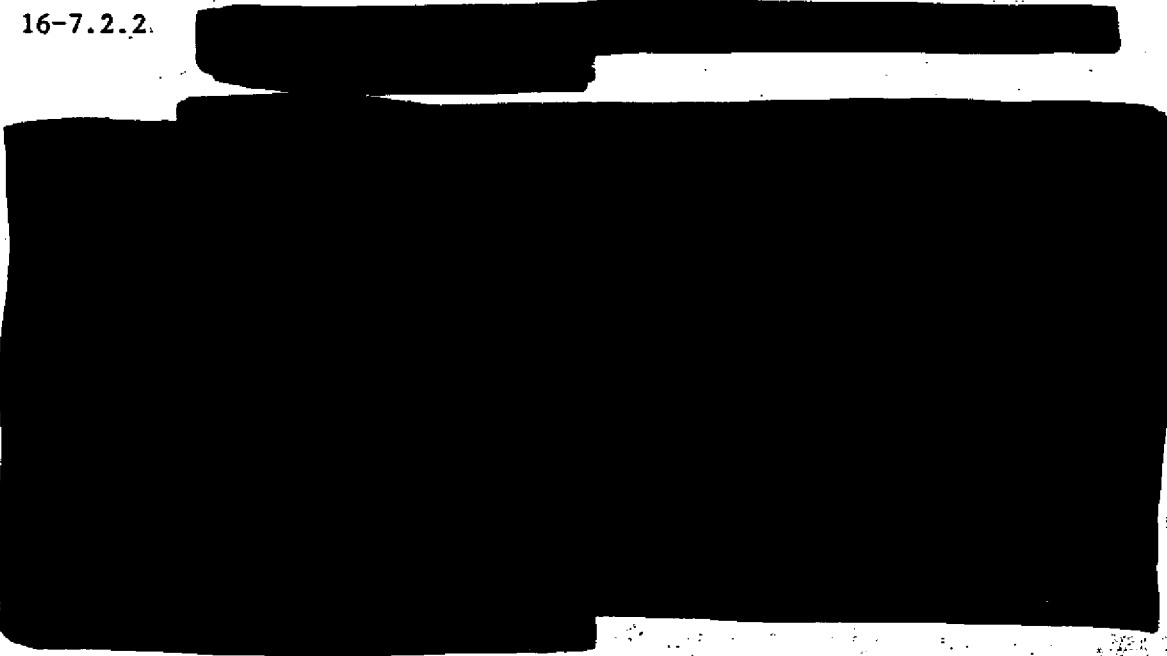
16-7.2.1



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]

b2
b7E

[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 reproduc- tion 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

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]

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.

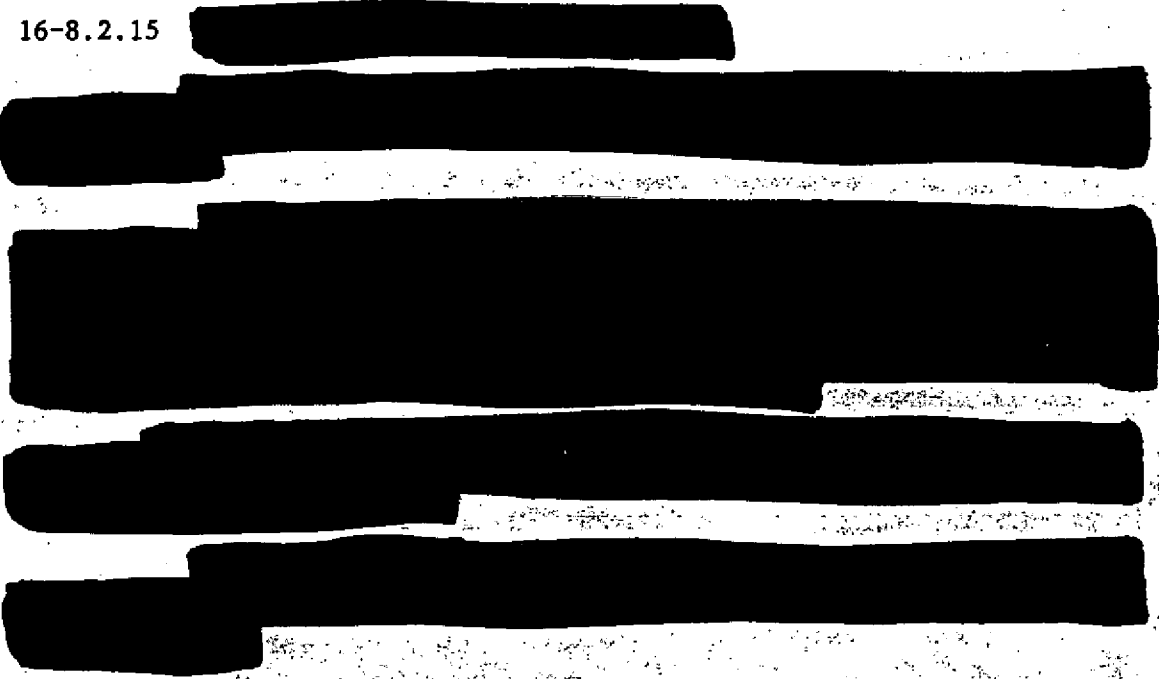
(2) An authorized copy of the copyrighted sound recording should be obtained from the manufacturer and submitted at the same time the questioned sound recording is submitted to Technical Services Division for examination.

(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
PRINTED: 02/18/98

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

PRINTED: 02/18/98

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

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.

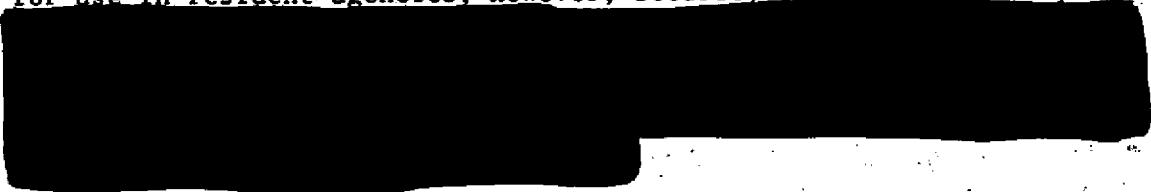
EFFECTIVE: 09/21/93

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

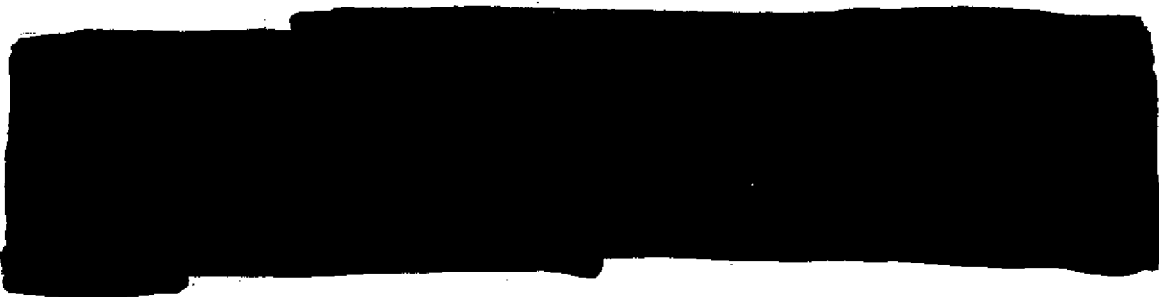
use of NLETS to the acquisition and dissemination of nonsensitive information. The following guidelines are set forth regarding the use of NLETS by the FBI:

(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.

62
b7E

EFFECTIVE: 08/18/94

Sensitive
PRINTED: 02/18/98

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

b2
b7E



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

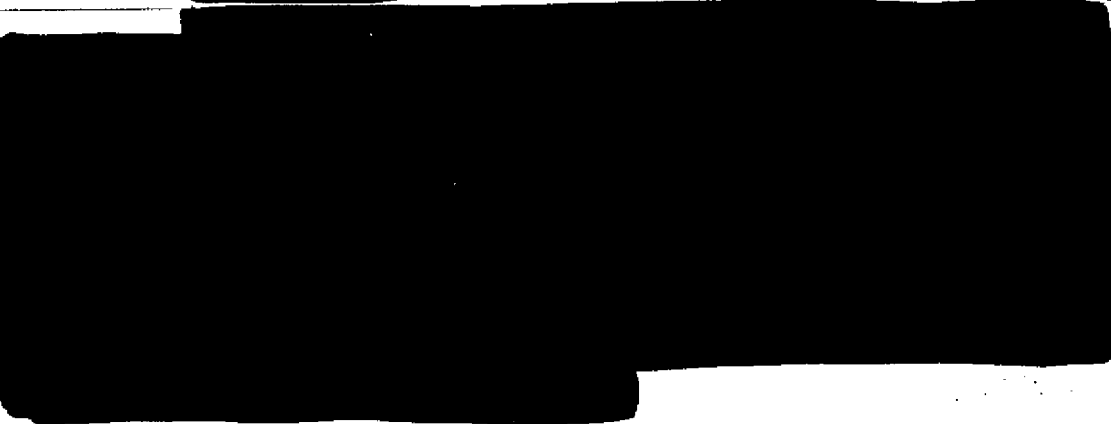
EFFECTIVE: 11/24/97

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.)

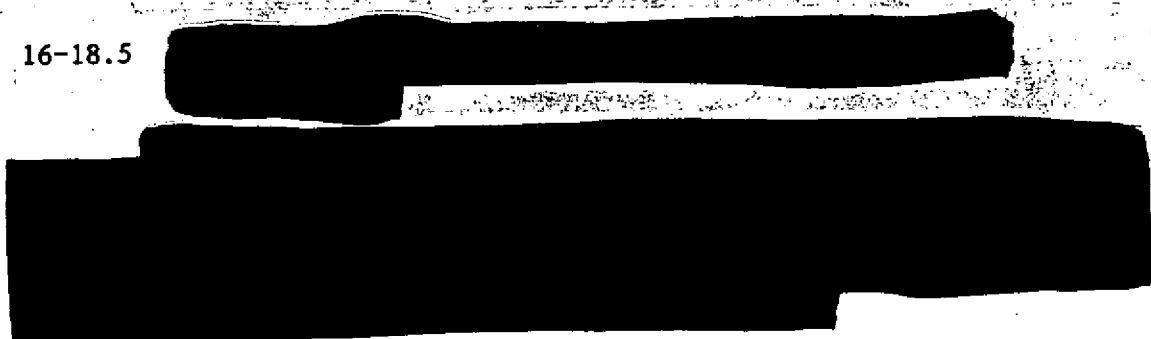
EFFECTIVE: 08/04/97

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
PRINTED: 02/18/98

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

PRINTED: 02/18/98

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

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

PRINTED: 02/18/98

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