# SECTION 259. SECURITY CLEARANCE INVESTIGATIONS

259-1 PURPOSE (See MIOG, Part I, 67-18 (3); II, 35-9.2.)

(1) All individuals who require access to National Security Information (NSI) must undergo a security clearance background investigation (BI). Individuals who are under contract to the FBI are discussed under Part I, Section 260 of the MIOG. This section deals with individuals who are not FBI contractors and require access to NSI.

(2) Deleted

(3) The other classifications in the FBI Security Program are 67E, 260, and 261 and are explained in those sections of the MIOG, Part I.

EFFECTIVE: 10/18/95

259-2 259A - CLASSIFIED INFORMATION PROCEDURES ACT (CIPA) (See MIOG, Part II, 17-2 (6) & 23-9; MAOP, Part II, 3-1.1 & 3-1.2.)

(1) The CIPA legislation was enacted in 1980 by Congress to provide for the introduction of NSI within the context of a federal CRIMINAL proceeding in order to prevent a defendant from claiming an inability to provide adequate defense because of a need to have access to NSI. Prior to CIPA, this claim could result in the government requesting a dismissal of the criminal charges rather than compromise national security.

(2) Persons needing a security clearance are identified by the court, e.g., attorneys and their staffs and court personnel. The request for a BI originates with the court and is coordinated with the Department of Justice (DOJ). Subsequently, DOJ directs FBIHQ Security Programs Manager to conduct a BI and provide the results to DOJ for clearance adjudication.

(3) Procedurally, at FBIHQ the cases are managed by the |Industrial/Facility|Security Unit|(I/FSU),|Security Countermeasures Section (SCMS), National Security Division (NSD), and any questions and/or consultation may be directed accordingly. |I/FSU|sets out investigation for the field under the subclassification 259A. The BI is to be conducted by the field in accordance with the guidelines set out in MIOG, Part II, 17.

(4) IMPORTANT THINGS TO REMEMBER:

(a) Deadlines in CIPA cases are driven by the trial date established by the U.S. District Court judge hearing the criminal case. Invariably, the time frames for conducting the BIs are extremely short, as is the tolerance of the judges for missed deadlines. More importantly, failure to meet the deadline could result in dismissal of the government's case with prejudice. Therefore, field supervisors managing these cases must be extremely sensitive to the time constraints.

(b) The FBI conducts the BI and the results are provided to DOJ for clearance adjudication. Only DOJ, Office of Security, can authorize discontinuance of these investigations.

(c) In some special cases, DOJ may ask the FBI to provide a security briefing to individuals who are cleared pursuant to the CIPA.

(d) CIPA applies only to CRIMINAL proceedings.

(e) When individuals must be cleared for access to NSI in the context of a civil judicial proceeding wherein the U.S. government is a party, the BIs are handled under the 259D classification.

EFFECTIVE: 10/18/95

259-3 259B - FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978 (FISA) (See MIOG, Part II, 17-2 (6); MAOP, Part II, 3-1.1 & 3-1.2.)

(1) This Act was passed by Congress to ensure that all electronic surveillance targeted against foreign individuals or establishments in the United States were reviewed and approved by a special FISA Court. Orders issued by the FISA Court are classified because of the nature of the information contained therein. Further, this Act authorized the Attorney General (AG) and the Director of Central Intelligence (DCI) to set the guidelines for the security procedures to be followed for all FISA electronic surveillance.

(2) The security requirements as determined by the AG and the DCI are contained in a document entitled SECURITY PROCEDURES FOR SAFEGUARDING RECORDS PERTAINING TO ELECTRONIC SURVEILLANCE WITHIN THE UNITED STATES AUTHORIZED UNDER THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978 which was signed March 13, 1980, and endorsed by the FBI. A copy of this document is to be maintained by the field office (FO) Security Countermeasures Programs Manager. These security procedures hold the FBI responsible for the security of the classified court orders, to include those orders which the communications carrier chooses to store in its own facility. Further, it is incumbent upon the FBI to ensure that any individual who has access to these classified court orders has the proper security clearance. Most often these individuals are cleared for "Top Secret."

The above-referenced security procedures provide for the use of a Trust Receipt which gives the communications carrier full access to the information contained in the classified court order, while the FBI physically maintains the order in the FO. The communications carrier receives a Trust Receipt signed by the SAC which guarantees the communications carrier access to the order at any time during business hours, during nonbusiness hours upon prior notification, and further guarantees that the court order will not be altered or destroyed. Each FO should encourage the communications carrier to utilize the Trust Receipt. The use of the Trust Receipt can be demonstrated as a savings for the communications carrier, since fewer people must be cleared. In addition, communications carriers will not incur the costs normally associated with the storage of classified information. The FBI will benefit since fewer of the communications carrier employees must have a security clearance. The FBI will not have the additional responsibility of periodically inspecting the communications carrier's facilities as mandated by the security procedures.

In the event the communications carrier elects to store the classified FISA order in its space, it is incumbent upon the FO Security Countermeasures Programs Manager to ensure that the classified material is being protected as outlined in Section 2, "Carrier Storage," of the above-referenced Security Procedures.

(3) Procedurally, FISA security clearance background investigations are managed by I/FSU, SCMS, NSD, and any questions and/or consultations may be directed accordingly. The investigations will be reported under the 259B subclassification.

(4) When the field Security Countermeasures Programs Manager identifies communications carrier personnel who need a security clearance, the following procedures are to be followed:

(a) Candidate completes an SF-86, "Questionnaire for Sensitive Positions," and is fingerprinted. The SF-86 and two FD-258s (applicant fingerprint cards) are forwarded to the FO Security Countermeasures Programs Manager.

(b) The field Security Countermeasures Programs Manager opens a 259B case, initiates indices, ALL available automated data base checks, and local criminal checks.

(c) After reviewing the SF-86 and the results of the FO checks, the field Security Countermeasures Programs Manager or designee interviews the candidate and reports same on an FD-302. The interview need not reflect the specific questions asked of the candidate. A question-and-answer format is not desired as it tends to result in a "checklist" style of interview. This interview is intended to obtain information to facilitate our investigative efforts. If a candidate provides information which could become an issue affecting trustworthiness for his/her access to classified information, this should be fully explored at the interview.

The narrative of the FD-302 should be sufficiently detailed to reflect, at a minimum, each of the following points:

1. Completeness and accuracy of the SF-86.

2. Personal and business credit issues, including, but not limited to, repossessions, delinquent student loans, debts placed for collection, and bankruptcy.

3. Civil suits as plaintiff or defendant, including divorces. Identify issues litigated.

4. Any involvement in criminal matters as a suspect or subject or any criminal charge, arrest, and/or conviction.

5. Any denials of employment and/or dismissals. Include reasons.

6. Any contact with representatives of foreign countries.

7. Details of candidate's personal life that could be used to coerce or unduly influence the candidate.

8. 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.

9. Business/investment circumstances that could or have involved conflict of interest allegations.

10. Details of any psychological counseling with psychiatrists, psychologists, or other qualified counselors.

11. Any abuse of prescription drugs or alcohol, illegal drug use, to include marijuana, and participation in drug/alcohol counseling/rehabilitation programs, during candidate's entire adult life (since age 18). Identify all drugs used, when used, duration of usage, amount of drug used, place where used (public or private setting), how the drug was obtained, whether or not candidate has provided drugs to anyone, if candidate has purchased or sold drugs, others having knowledge of candidate's drug use.

12. Any involvement in any organization which advocates the use of force to overthrow the U.S. government; or any involvement in any organization involved in the commission of sabotage, espionage, or assisting others in terrorism.

13. Any current or past circumstances known to the candidate that could have a bearing on his/her trustworthiness for access to classified information.

(d) The candidate should be recontacted to resolve, if necessary, any issues developed during the investigation.

(e) THE FIELD SECURITY COUNTERMEASURES PROGRAMS

MANAGER SPONSORING THE CANDIDATE HAS THE AUTHORITY TO DISCONTINUE THE INVESTIGATION AT ANY TIME BASED ON INFORMATION DEVELOPED.

(f) If the candidate is still viable for clearance, the field submits the original SF-86, two FD-258s (applicant fingerprint cards), results of the FO checks, and candidate interview with a cover communication to |I/FSU| AND auxiliary FOs, as appropriate, setting out type of investigation, 259B file number, and 30-day Buded. FBI Headquarters' Personnel Security Specialist reviews Headquarters checks and, if necessary, advises field of unfavorable information.

(g) FO continues BI consistent with guidelines set out in Part II, Section 17, MIOG. Submit completed investigation to |I/FSU| with copies to office processing the candidate.

(h) The |I/FSU| adjudicates trustworthiness and notifies the sponsoring FO of the clearance decision.

(5) The field Security Countermeasures Programs Manager provides a comprehensive briefing covering the handling of classified information.

(a) The ORIGINAL signed SF-312, "Classified Information Nondisclosure Agreement," is forwarded to the |I/FSU.|

(b) When the candidate's security clearance is terminated for any reason, the field provides a debriefing and forwards the signed SF-312 to the |I/FSU| for the mandatory 50-year retention requirement.

(6) The FISA security procedures provide for EMERGENCY SITUATIONS when it is necessary to grant uncleared individuals access to the classified court order. The SAC or designee must make the determination that the time required to obtain a personnel security clearance in a particular circumstance would cause failure or unreasonable delay in conducting the surveillance. Such emergency authorization must be confirmed in writing to the communications carrier, and the person being served with the classified order must execute the security agreement form required by the FISA security procedures (supra). The emergency procedures are not to be utilized to bypass the clearance process. Subsequent contacts with the same communications carrier for the purpose of serving a classified court order should be anticipated and the appropriate individual(s) submitted for a security clearance.

The FO Security Countermeasures Programs Manager must work closely

with the FO Technical Advisor in an effort to identify key individuals with the communications carriers who will need clearances for FISA orders.

(7) IMPORTANT THINGS TO REMEMBER:

(a) Classified FISA orders should only be served on individuals who possess the required DOJ security clearance.

(b) The communications carrier should be encouraged to utilize the Trust Receipt exclusively.

(c) The FO is responsible for inspecting the facilities of communications carriers which store the classified FISA orders to ensure proper security procedures are in place.

(d) The FO Security Countermeasures Programs Manager is responsible for identifying all communications carriers which are or could be used for a FISA. Appropriate personnel with those carriers are to be cleared. The FO should be aware of the communications carriers' pending retirements or transfers so that a pool of cleared individuals can be maintained.

(e) Emergency procedures exist for those limited situations when an uncleared individual must be served with a FISA order. The SAC or designee must determine an emergency exists and confirm authorization for emergency access in writing to the communications carrier. The uncleared individual must sign the security agreement form. This individual must undergo a security clearance investigation and receive a clearance before he/she can be served with any subsequent FISA order.

(f) The FBI component in the NSD managing the FISA program will, from time to time, identify key communications carrier personnel at the Headquarters level who will require a Top Secret security clearance. In those instances, the|I/FSU,|SCMS, NSD, will initiate the BI and set out leads to the field accordingly.

EFFECTIVE: 10/18/95

259-4 259C - FBI JOINT TASK FORCES (JTFs) (See MIOG, Part II, 17-2|(6); MAOP, Part II, 3-1.1 & 3-1.2.)|

(1) A Joint Task Force (JTF) for purposes of this subsection is the combination of FBI personnel and other resources with STATE AND LOCAL law enforcement agencies to address common crime problems within their respective jurisdictions.

(2) Generally speaking, a JTF is designed so the FBI and state and local participants are on an equal footing as to the sharing of information, personnel, and/or facilities to which access is necessary to accomplish the objectives of the JTF. Very often, the JTF personnel become one force whose participants become indistinguishable. Heretofore, security countermeasures required a ten-year BI and a Top Secret security clearance for ALL state and local JTF participants.

In the late 1980s and early 1990s, there was a proliferation of FBI JTFs across the nation occasioned by the expansion of the FBI's investigative responsibilities, such as Violent Crime/Major Offenders initiative, Domestic and International Terrorism, etc. The traditional task force concept began to lose its identity in that the new JTFs had significant variances in the degree of access to FBI information, personnel, and/or facilities afforded to state and local personnel. As a consequence, the ten-year BI was thought to be excessive when the access was, at times, measurably less than in the traditional task force of the late 1970s and early 1980s.

(3) The entire security countermeasures program as applicable to JTFs was revisited by experienced SAs in the field and representatives of both investigative divisions at FBIHQ. The objective was to make the program more effective in terms of streamlining procedures without sacrificing the security of our information, personnel, and/or facilities.

(a) A threshold decision was made to place responsibility on FO managers to assess JTF security vulnerabilities by utilizing the concept of "RISK FACTOR."

1. "RISK FACTOR" is ascertained by the FO examining and quantifying the access to FBI information, personnel, and/or facilities being afforded to the JTF state and local law enforcement personnel. Thereafter, the FO managers must project the damage to the FBI if the state and/or local law enforcement personnel betray the access afforded them. In other words, if there is compromise, what is the potential damage? For example, will

compromise jeopardize an investigation?; endanger life of an undercover agent?; an informant?; surface covert facility or operation?, etc. When you can estimate the probable impact of compromise, you have established the "RISK FACTOR."

2. The "RISK FACTOR" drives the scope of your security countermeasures program as it applies to a particular JTF.

(b) The group (supra) studying the JTF security countermeasures policy and procedures took the position that, under all circumstances, every FO MUST HAVE a record of ALL state and local participants in FBI JTFs.

(c) The guesswork, as to the scope of the security countermeasures, has been eliminated by establishing two ALL INCLUSIVE categories of JTFs for purposes of security countermeasures, i.e., CATEGORY I and CATEGORY II.

(d) The new JTF security countermeasures policy and procedures were sent out to ALL SACs by airtel dated 11/22/93, captioned "SECURITY PROCEDURES REGARDING JOINT TASK FORCES (JTFs), FBI AND OTHER LAW ENFORCEMENT AGENCIES, FCI - SECURITY COUNTERMEASURES."

(4) These cases will be reported under the 259C subclassification.

The FBI Security Program is managed in each office by the National Foreign Intelligence Program Manager, WHO MUST FAMILIARIZE OTHER FO SUPERVISORY PERSONNEL WITH SECURITY COUNTERMEASURES POLICY AND PROCEDURES.

This facet of the FBI Security Program is being managed at FBIHQ by the|I/FSU,|SCMS, NSD, and any questions and/or consultation may be directed accordingly.

(5) All state and local JTF participants will be investigated in either CATEGORY I OR II, depending on FIELD OFFICE assessment of the RISK FACTOR.

EFFECTIVE: 10/18/95

259-4.1 Category I JTFs Consist of State and Local Candidates Participating in FBI Joint Task Forces Who Need Department of Justice Top Secret Security Clearances Based on a Ten-Year Background Investigation (BI)

(1) Specifically, this category applies to state and local candidates who will have:

(2) Access to national security information in order to participate in joint task forces; OR

(3) Long-term unrestricted access to FBI information, personnel, and/or facilities.

EFFECTIVE: 04/12/94

259-4.1.1 Procedures for Conducting a Ten-Year Background Investigation on State and Local Candidates Participating in FBI Joint Task Forces Who Need Top Secret Security Clearances

(1) Candidate completes an SF-86, "Questionnaire for Sensitive Positions," and is fingerprinted. The SF-86 and two FD-258s (applicant fingerprint cards) are forwarded to the field Security Countermeasures Programs Manager.

(2) The field Security Countermeasures Programs Manager opens a 259C case, initiates indices, ALL available automated data base checks, local criminal checks, and police department Internal Affairs check.

(3) After reviewing the SF-86 and the results of the FO checks, the field Security Countermeasures Programs Manager or designee interviews the candidate and reports same on an FD-302. The interview need not reflect the specific questions asked of the candidate. A question-and-answer format is not desired as it tends to result in a "checklist" style of interview. This interview is intended to obtain information to facilitate our investigative efforts. If a candidate provides information which could become an issue affecting suitability for participation in an FBI JTF or his/her access to sensitive or classified information, this should be fully

explored at the interview.

The narrative of the FD-302 should be sufficiently detailed to reflect, at a minimum, each of the following points:

(a) Completeness and accuracy of the SF-86.

(b) Personal and business credit issues, including, but not limited to, repossessions, delinquent student loans, debts placed for collection and bankruptcy.

(c) Civil suits as plaintiff or defendant, including divorces. Identify issues litigated.

(d) Any involvement in criminal matters as a suspect or subject or any criminal charge, arrest, and/or conviction.

(e) Any denials of employment and/or dismissals. Include reasons.

(f) Any contact with representatives of foreign countries.

(g) Details of candidate's personal life that could be used to coerce or unduly influence the candidate.

(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, or other qualified counselors.

(k) Any abuse of prescription drugs or alcohol, illegal drug use, to include marijuana, and participation in drug/alcohol counseling/rehabilitation programs, during candidate's entire adult life (since age 18). Identify all drugs used, when used, duration of usage, amount of drug used, place where used (public or private setting), how the drug was obtained, whether or not candidate has provided drugs to anyone, if candidate has purchased or sold drugs, others having knowledge of candidate's drug use.

(l) Memberships in organizations whose policies restrict membership on the basis of sex, race, color, religion, or national origin.

(m) Any involvement in any organization which advocates the use of force to overthrow the U.S. Government; or any involvement in any organization involved in the commission of sabotage, espionage, or assisting others in terrorism.

(n) Any current or past circumstances known to the candidate that could have a bearing on his/her suitability for FBI JTF participation and/or access to sensitive and/or classified information.

(4) If necessary, the candidate should be recontacted to resolve any issues developed during the investigation.

(5) THE FIELD SECURITY COUNTERMEASURES PROGRAMS MANAGER SPONSORING THE CANDIDATE HAS THE AUTHORITY TO DISCONTINUE THE INVESTIGATION AT ANY TIME BASED ON INFORMATION DEVELOPED.

(6) If the candidate is still viable for clearance, the field submits original of the SF-86, two FD-258s (applicant fingerprint cards), results of the FO checks, and candidate interview with a cover communication to ISU AND auxiliary field offices, as appropriate, setting out type of investigation, 259C file number and 30-day Buded. FBIHQ Personnel Security Specialist reviews Headquarters' checks and, if necessary, advises field of unfavorable information.

(7) Field offices continue BI consistent with guidelines set out in Part II, Section 17, MIOG. However, this investigation must include ARREST CHECKS ON RELATIVES. Submit completed investigation to ISU with copies to office sponsoring the candidate.

(8) The ISU adjudicates trustworthiness and notifies the sponsoring FO of the clearance decision.

(9) The field Security Countermeasures Programs Manager provides a comprehensive briefing covering the handling of national security information and security policy and procedures of the FO.

(a) A COPY of the signed SF-312, "Classified Information Nondisclosure Agreement," is forwarded to the ISU.

(b) When the candidate terminates the task force, the field provides a debriefing and forwards the ORIGINAL signed SF-312 to the ISU for the mandatory 50-year retention requirement.

EFFECTIVE: 04/12/94

259-4.2 Category II JTFs Consist of State and Local Candidates Participating in FBI Joint Task Forces Who Have NO NEED FOR A SECURITY CLEARANCE But Must Be Subjected to a Limited Security Investigation

(1) Specifically, this category applies to state and local candidates who will NOT have:

(2) Access to national security information in order to participate in joint task forces; OR

(3) Long-term unrestricted access to FBI information, personnel, and/or facilities.

EFFECTIVE: 04/12/94

259-4.2.1 Procedures for Conducting a Limited Investigation on State and Local Candidates Participating in FBI Joint Task Forces Who Have NO NEED FOR A SECURITY CLEARANCE

(1) Candidate completes pages 1, 2, 3, 9 (Certification only), and 10 of the SF-86, "Questionnaire for Sensitive Positions." The SF-86 is forwarded to the field Security Countermeasures Programs Manager.

(2) The field Security Countermeasures Programs Manager opens a 259C case, initiates indices, ALL available automated data base checks, local criminal checks, and police department Internal Affairs check.

(3) After reviewing the SF-86 and the results of the FO checks, the field Security Countermeasures Programs Manager or

designee interviews the candidate and reports same on an FD-302. The interview should cover the following:

(a) Completeness and accuracy of the SF-86.

(b) Any involvement by the candidate in criminal matters as suspect or subject or any criminal charge, arrest, and/or conviction.

(c) Any current or past circumstances known to the candidate that could have a bearing on his/her suitability for participation in an FBI JTF and its investigative mission.

(4) The above items are not all inclusive and may be expanded depending upon the nature of the task force, degree of access, Risk Factor, and other information developed which may adversely affect the candidate's participation in an FBI JTF.

(5) THE FIELD SECURITY COUNTERMEASURES PROGRAMS MANAGER HAS THE AUTHORITY TO DISCONTINUE THE INVESTIGATION AT ANY TIME BASED ON INFORMATION DEVELOPED.

(6) If the field Security Countermeasures Programs Manager determines candidate is acceptable for participation in the FBI JTF, the candidate must be provided a comprehensive briefing covering the security policy and procedures of the FO.

(7) All records regarding the above must be maintained in the FO 259C file. No reporting to FBIHQ is required in Category II cases.

EFFECTIVE: 04/12/94

259-5 SECURITY CLAUSES FOR JOINT TASK FORCE MEMORANDUM OF UNDERSTANDING

(1) An integral part of the JTF process is a Memorandum of Understanding (MOU) to ensure clarity as to the responsibilities for each of the participating agencies.

(2) An MOU is an agreement which is voluntarily entered into between the FBI and a cooperating state or local law enforcement

agency which sets out the objectives of a joint investigation, the method of conducting the investigation, and the responsibilities of all parties.

(3) Depending upon the Category of the JTF (I or II), different security clauses will be necessary.

(a) CATEGORY I task forces require a DOJ Top Secret security clearance for state and local candidates who will have:

1. Access to national security information in order to participate in joint task forces; OR

2. Long-term unrestricted access to FBI information, personnel, and/or facilities.

(b) The CATEGORY I FBI JTF security clauses are as follows:

"Personnel of the (insert agency name) participating in this FBI Joint Task Force will be required to undergo a full background investigation for a Department of Justice Top Secret security clearance. If, for any reason, a candidate is not selected, (name of participating agency) will be so advised and a request will be made for another candidate.

"Sixty days prior to being assigned to this task force, each candidate will be required to furnish a completed "Questionnaire for Sensitive Positions" (SF-86) and two "Applicant Fingerprint Cards" (FD-258s) to the FBI. Sometime thereafter, an interview of each candidate will be conducted by an FBI representative.

"At the completion of the background investigation, each candidate selected will be granted a Department of Justice Top Secret security clearance and will receive a comprehensive briefing on the security policy and procedures of the FBI field office, to include the handling and protection of national security information. During the briefing, each candidate will execute a nondisclosure agreement (SF-312).

"Upon departure from the task force, each candidate will execute a nondisclosure agreement (SF-312) and will be given a security debriefing."

(c) CATEGORY II task forces require a limited

background investigation for all state and local personnel who will NOT have:

1. Access to national security information in order to participate in joint task forces; OR

2. Long-term unrestricted access to FBI information, personnel, and/or facilities.

(d) The CATEGORY II FBI JTF security clauses are as follows:

"Personnel of the (insert agency name) participating in this FBI Joint Task Force will be required to undergo a limited background investigation. If, for any reason, a candidate is not selected, (name of participating agency) will be so advised and a request will be made for another candidate.

"Thirty days prior to being assigned to the task force, each candidate will be required to furnish pages 1, 2, 3, 9 (Certification only), and 10, of the "Questionnaire for Sensitive Positions" (SF-86). Sometime thereafter, an interview of each candidate will be conducted by a representative of the FBI.

"Upon being selected, each candidate will receive a comprehensive briefing covering the security policy and procedures of the FBI field office."

(4) Procedures regarding preparation of MOUs are outlined in the revised "FIELD GUIDE FOR UNDERCOVER AND SENSITIVE OPERATIONS," under the caption "CONTRACTS/AGREEMENTS, MEMORANDUM OF UNDERSTANDING." A sample of an MOU with the Security Clauses for Category I and CATEGORY II JTFs are located in the Appendix of the "Guide." This "Guide" was published by the Undercover and Sensitive Operations Unit, Corruption/Civil Rights Section, Criminal Investigative Division, FBIHQ.

EFFECTIVE: 04/12/94

259-6 259D - OTHERS - ACCESS TO NATIONAL SECURITY INFORMATION (SEE MIOG, PART II, 17-2 (6).)

This category applies to individuals other than those in 259A, B, and C (supra), who must have access to NSI. This miscellaneous category has grown significantly in recent years and the following list is illustrative:

(1) Attorneys representing FBI employees in personnel actions requiring access to NSI;

(2) Federal civil judicial proceedings wherein the U.S. Government is a party and litigants must have access to NSI;

(3) Staff of Federal Independent Counsel, Special Counsel, etc.;

(4) Special Consultants (e.g., security professionals, administrators);

(5) Selected Federal Legislative and Judicial Branch personnel;

(6) Military personnel supporting FBI initiatives (see All SAC airtel, captioned "DEPARTMENT OF DEFENSE (DOD) SUPPORT FOR FBI COUNTERDRUG OPERATIONS SECURITY COUNTERMEASURES POLICY AND PROCEDURES, FCI - SECURITY COUNTERMEASURES," dated 1/10/94);

(7) Chaplains promoting health and welfare of FBI personnel (see All SACs airtel, captioned "FBI CHAPLAINS PROGRAM SECURITY COUNTERMEASURES POLICY AND PROCEDURES, FCI - SECURITY COUNTERMEASURES," dated 3/4/94);

(8) Other Federal personnel supporting FBI initiatives;

(9) Individuals needing access to NSI and, to do so, will need a DOJ security clearance.

If the Field Security Countermeasures Programs Manager receives a request for a security clearance in this miscellaneous category for which there are no existing policy and procedures, it must be coordinated with the ISU, SCMS, NSD, FBIHQ.

EFFECTIVE: 04/12/94

259-7 | 259E - PERIODIC REINVESTIGATIONS/SECURITY CLEARANCES
(See MIOG, Part II, 17-2; MAOP, Part II, 3-1.1 and 3-1.2.)

All FBI noncontractor personnel possessing current and active security clearances five years old or older are to be reinvestigated to ensure trustworthiness for continued access to National Security Information.

(1) Individuals due for the five-year reinvestigation, both at the "Secret" and "Top Secret" levels, will be identified by field offices or divisions within FBIHQ. The reinvestigation will be initiated via electronic communication from field offices or divisions within FBIHQ and include the original Standard Form 86 (SF-86) to FBIHQ and set forth the required investigation.

(2) The reinvestigation for a "Secret" security clearance will include a candidate interview, a check of FBI indices (field and FBIHQ), automated data bases (FBIHQ), national agency checks (FBIHQ), local agency checks/arrest checks (field), and credit bureau checks (FBIHQ).

(3) The "Top Secret" reinvestigation will encompass the same areas as the "Secret" level and, in addition, will include verification of residence, interview of two neighbors, review of employment records, two employment references, and two character references developed by the investigator and not provided by the candidate.

(4) In all instances the investigation must be expanded to resolve any derogatory or adverse information. Newly listed information within the scope of the investigation, such as education, recent divorce, roommate, part-time military service and foreign travel must be addressed.

(5) Conduct investigation in accordance with the policy and procedures set out in MIOG, Part II, 17-6, entitled "Scope of Full Field Investigation."|

EFFECTIVE: 01/03/97

|259-8| CHARACTER - SECURITY CLEARANCE INVESTIGATIONS - CIPA; - FISA; - JTF; -|OTHER; - PERSONNEL REINVESTIGATIONS/ SECURITY CLEARANCES (See MIOG, Part II, 17-2; MAOP, Part II, 3-1.1 and 3-1.2.)|

EFFECTIVE: 01/03/97

# SECTION 260. INDUSTRIAL SECURITY PROGRAM

260-1 BACKGROUND AND PURPOSE (See MIOG, Part I, 67-18 (3) & 259-1; II, 35-9.2.)

(1) The Industrial Security Program (ISP) is designed to manage, control, and safeguard FBI information entrusted to contractors and thereby prevent damage to national security. In order to perform this task, the ISP cannot merely address the threat of espionage posed by contractor personnel who have access to National Security Information (NSI). It must also focus on those situations where there is potential risk to the national security by virtue of access by non-FBI personnel to sensitive unclassified FBI information, personnel, and facilities. The following are illustrative of major concerns the ISP must address: (See MIOG, Part I, 261-2 (6) & MAOP, Part II, 2-4.3.1(1)(p).)

(a) All contracts which include new construction or modification of existing FBI facilities;

(b) All contractual arrangements with the private sector for the installation and/or service of any manufactured item essential to Bureau operations, i.e., computers, typewriters, building maintenance, automobiles, etc.;

(c) Any or all non-FBI individuals who are granted access to FBI facilities for whatever reason, to include but not limited to vendors, consultants, service people, etc.; and

(d) Traditional contractual arrangements involving the release of NSI to a contractor.

(2) The ISP is one segment of the FBI's Security Program which is included within the National Foreign Intelligence Program. The following classification and alpha designators have been approved for capturing field time expended on this aspect of the ISP. (See MIOG, Part II, 17-2 (7) & MAOP, Part II, 3-1.1 & 3-1.2.)

260A ISP - Personnel Clearance
260B ISP - Facility Clearance
260C ISP - Nonclassified Personnel/Access
260D ISP - Other
260E ISP - Personnel Clearance - Reinvestigations

(3) The ISP is managed by the FBI Security Programs Manager (SPM) and the staffs of the Industrial/Facility Security Unit (I/FSU), Security Countermeasures Section, National Security Division.

(4) The guidelines in this section of the MIOG apply to all FBI components, both at FBIHQ and in the field. The policy and procedures set forth in this section apply to obtaining personnel and facility security clearances for contractors and their employees who require access to and/or storage of NSI. These guidelines also apply to personnel facility access approvals to FBI facilities for a contractor, its employees, and/or others accessing sensitive information, FBI personnel, or facilities, including equipment, not requiring access to NSI.

(5) General reporting procedures for 260 matters are contained in Part II, Section 17-6 of the MIOG.

EFFECTIVE: 03/07/96

260-2 PERSONNEL CLEARANCE 260A (See MIOG, Part I, 260-2.1(1) & 260-3.2(3).)

(1) |I/FSU|manages the investigation and clearance of those contractor personnel who will need access to NSI in order to fulfill the terms of their contract. Pursuant to Department of Justice Order 2640.2B, "Automated Information Systems Security," individuals who must also be investigated and cleared include contractor personnel who will require access to FBI computer systems (hardware and software) containing NSI or unescorted access to Bureau automated data processing (ADP) facilities where NSI is processed. Level of clearance required for those individuals involved in ADP or ADP facility maintenance is set forth in 260-4.3.2. Contractor personnel not requiring access to NSI, as set forth in this paragraph, are not subject to regulations promulgated by the|I/FSU;|however, they may be subject to guidelines set forth in|MIOG, Part I,|260-4. |(See MIOG, Part I, 260-2.5(3).)|

|(2)|Cognizant Security Officer

The Cognizant Security Officer (CSO) is the FBI employee given the responsibility by the contracting component of the FBI to oversee security issues, e.g., Contracting Officer's Technical

Representative, Division Security Officer, etc. The CSO will act as liaison between the FBI and the contractor on all matters relating to security.

EFFECTIVE: 07/11/94

260-2.1 FBI National Security Clearance Adjudicative Process

(1) Pursuant to a Letter of Agreement between the Department of Justice and the Department of Defense, dated March 19, 1976, and amended December 11, 1989, the FBI is a User Agency of the Defense Investigative Security Program as administered by the Defense Investigative Service (DIS). Therefore, except as set forth in 260-2.3, FBI contractors meeting the criteria in 260-2 (1) will require FBI background investigations and thereafter be granted clearances issued by the Defense Industrial Security Clearance Office (DISCO) and authority granted by the SPM to participate in Bureau projects involving NSI.

(2) The 1989 amendment to the 1976 Letter of Agreement permits the FBI considerable flexibility in the administration of its ISP. Notwithstanding the fact that a prospective contract employee has the requisite DISCO clearance, the SPM can conduct such investigation as is deemed necessary to make a determination of trustworthiness prior to placement of that contract employee into a Bureau project. Further, if during the course of the security clearance background investigation or at any other time information is developed indicating that the contract employee's continued participation in a Bureau project is not clearly in the best interests of national security, he/she may be removed by the SPM pending resolution of the trustworthiness issue by the DIS.

(3) Participation Authorization

Participation authorization is a determination by the SPM that a contract employee's involvement in a Bureau project is consistent with the best interests of national security. No contract employee may participate in a Bureau project involving NSI without SPM authorization.

EFFECTIVE: 02/12/92

260-2.2 Interim Clearance/Participation Authorization

(1) Definition - DISCO "interim" clearance and SPM "interim" participation authorization are determinations based upon the completion of minimum investigative requirements and are granted on a temporary basis, pending completion of the full investigative requirements.

(2) Upon certification of an immediate need for a contract employee's participation in a Bureau project by the CSO, the |I/FSU| will seek an "interim" clearance from DISCO and the SPM can authorize "interim" participation by the contract employee to the requesting Bureau component. In those cases where the contract employee has the requisite DISCO clearance, |I/FSU| will, after meeting the minimum investigative requirements, request the SPM authorize "interim" participation.

(3) Requests for "interim" clearance/participation authorization must be justified by exigent circumstances and not submitted on a routine basis.

EFFECTIVE: 07/11/94

260-2.3 Department of Justice Clearances Issued to Contractors

The SPM may, from time to time, determine that a clearance for a contractor be sought from the Department of Justice (DOJ) rather than DISCO. In these cases, the field will be so informed by the airtel initiating the investigation. The completed investigation (or results of the preliminary investigation where an "interim" clearance is being sought) will be presented to the Department Security Officer, DOJ, for an adjudicative determination. An example of a contractor clearance issued by the DOJ is that provided to Special Investigators involved in the Background Investigation Contract Services program.

EFFECTIVE: 02/12/92

||260-2.3.1 |Moved To 260-5.1|

EFFECTIVE: 03/07/96

260-2.4 Forms

(1) All contracting components within the FBI (FBIHQ or field) seeking a national security clearance or participation authorization on behalf of a contract employee should submit to the|I/FSU|an original and four copies of Standard Form (SF) 86, "Questionnaire for Sensitive Positions" (Revised date October 19, 1987), and two copies of an FD-258 "Applicant Fingerprint Card." It is the responsibility of the CSO to ensure that all submitted documentation is typewritten, complete, and accurate. All applications not meeting these criteria will be returned unprocessed.

(2) The above forms must be attached to a communication stating:

(a) the identity of the CSO;

(b) whether the candidate will require access (escorted or unescorted) to FBIHQ or field office facilities;

(c) the Corporate and Government Entity (CAGE) code of the contractor indicating that it is a DIS-cleared facility (see 260-3). CSOs must ensure that the contractor facility has the appropriate level of clearance (see 260-3 infra);|(See MIOG, Part I, 260-3.2(2).)|

(d) the level of clearance required;

(e) if applicable, justification for "interim" clearance/participation authorization.

(3) It is incumbent upon the CSO to advise the|I/FSU|expeditiously when a contract employee's participation in a

Bureau project is no longer required.

(4) |I/FSU|will audit, on a semiannual basis, the continued need for contract employees to retain their clearance/participation authorizations.

EFFECTIVE: 07/11/94

260-2.5 Level of Clearance/Types of Investigations

(1) A determination of trustworthiness will be made in accordance with the standards set forth in Department of Defense Personnel Security Program Regulation, 5200.2R, Appendix I, entitled "Adjudication Policy-General." The scope of the FBI security clearance background investigation (BI) to be conducted is determined by the level of clearance sought. In any case, the SPM may expand the scope of the investigation in order to arrive at a determination of trustworthiness.

(a) "Top Secret" - A security clearance BI covering the past |10|years of an individual's life or from age 18 to the present, whichever is shorter. However, in no case may the BI cover less than a scope of two years.

(b) "Secret" - A security clearance BI covering the past five years of an individual's life or from age 18 to the present, whichever is shorter. However, in no case may the BI cover less than a scope of two years.

(c) "Confidential" - An investigation composed of various records checks conducted by FBIHQ and the field, as directed by |I/FSU.|

(d) Sensitive Compartmented Information (SCI) - FBI contractor access to SCI will be determined in accordance with the guidelines set forth in Part II, Section 26-10, of the MIOG.

(2) Investigative procedures for 260A are contained in Part II, Section 17, of the MIOG. Deviation from investigative procedures set forth in Part II, Section 17, may be requested by FBIHQ and will be detailed in the communication directing the investigation.

(3) The procedures set forth above must be adhered to by

Bureau components involved in the use of contractors falling within the parameters set out in 260-2 (1) (supra). Certain CSOs may wish to impose additional security procedures in connection with projects they administer. In such cases, the CSO may institute changes with the prior approval of the I/FSU. (See (4) below.)

(4) Security Awareness Briefings for contractors granted clearances issued by the Department of Justice will be afforded by division Security Officers, as directed by the I/FSU. Briefings for those individuals cleared by DISCO will be conducted by their respective corporate Security Officers in accordance with the INDUSTRIAL SECURITY MANUAL or by the CSO as provided in 260-2.5 (3). Briefings for consultants cleared by DISCO is addressed in 260-3.2 (5) (infra).

EFFECTIVE: 07/11/94

260-3 FACILITY CLEARANCE 260B (See MIOG, Part I, 260-2.4(2)(c).)

(1) Definition - A facility clearance (FCL) is an administrative determination that a facility is eligible from a security viewpoint for access to NSI of the same or lower classification level as the clearance being granted.

(2) An FCL is required of all firms with which the FBI engages in NSI contractual matters. DISCO will only issue personnel clearances for contract employees employed by a cleared facility (except as set forth in 260-3.2). An FCL is required, notwithstanding the fact that the contractor may not be required to possess NSI at its facility.

(3) Components of an FCL investigation are: personnel security clearances of designated owners, officers, directors, executive personnel (OODEPs); a determination of the foreign ownership, control, or influence to which the contractor may be subject; and the adequacy of safeguards to store NSI (if applicable).

(4) The FBI will rely upon the DIS to conduct the appropriate inspection and issue the requisite FCL. All CSOs will ensure that firms with which the FBI contracts to do classified work have an FCL at the requisite level of clearance or must submit a request for issuance or upgrade of FCL to the I/FSU.

(5) The request for issuance or upgrading of an FCL must include:

(a) the identity of the CSO;

(b) the name, address, and telephone number of the contractor facility;

(c) a point of contact at the facility who must be an OODEP;

(d) a brief description of the work to be performed pursuant to the contract;

(e) the level of clearance required;

(f) whether NSI will be stored at the contractor facility.

(6) DIS industrial security representatives will advise the|I/FSU|of the identity of those individuals who will require personnel clearance investigations in connection with the FCL. The |I/FSU|will manage these background investigations and coordinate the results with the DIS and the CSO.

EFFECTIVE: 07/11/94

260-3.1 Contract Security Classification Specification Department of Defense Form 254

(1) The completed DD 254 is the basic document by which classification, regrading, and declassification specifications are documented and provided to contractors. It is designed to identify the specific items of NSI involved in the contract that require security classification protection.

(2) For those programs where the DIS will exercise total or partial control over the facility inspection of a Bureau contractor, the CSO will prepare a DD 254 and provide it to|I/FSU.| The DD 254 advises the DIS that a User Agency has a classified contract at a facility. It also assists the DIS industrial security representatives in determining whether NSI is being handled in

accordance with established DIS policy and specific instructions as set forth on the DD 254.

(3) There may be circumstances when a CSO wishes to exclude a project or a portion thereof from the purview of DIS inspection. This is known as a "carve out." In such a case, the CSO should prepare a communication to the SPM setting forth a security plan containing the following:

(a) justification for this request;

(b) the exact location of the NSI retained at the contractor facility;

(c) documentation that the CSO has the expertise to conduct facility inspections in lieu of the DIS;

(d) a copy of the security guidance to be provided to the contractor.

(4) The |I/FSU| will coordinate notification of this "carve out" request with the Special Actions Branch at DIS Headquarters in Washington, D.C.

(5) In the event a project is removed from DIS inspection responsibilities, the CSO must certify to the SPM at least once per year that a facility inspection has been conducted consistent with the security plan approved by the SPM, as set forth above, and the results thereof.

EFFECTIVE: 07/11/94

260-3.2 Consultant Agreements

(1) An individual may qualify for a personnel security clearance despite the fact that he/she is not employed by a cleared facility if his/her contractual obligation to the Bureau meets the following guidelines: |(See MIOG, Part I, 260-3 (2).)|

(a) NSI shall not be possessed by the consultant away from the premises of the FBI;

(b) The FBI shall not furnish NSI to the consultant

at any location other than the premises of the FBI;

(c) Performance of the consulting services by the consultant shall be accomplished in FBI office space and classification guidance will be provided by the FBI.

(2) The CSO will be provided a Consultant/User Agency Certification by the |I/FSU| which must be executed by the CSO and consultant. The executed Consultant/User Agency Certification should be attached to the memorandum requesting clearance action in lieu of the CAGE code as set forth in 260-2.4 (2).

(3) The scope of the security clearance background investigation and reporting requirements for consultants are identical to those outlined in 260-2 (supra).

(4) Upon issuance of the security clearance to a consultant by the DIS, the Security Officer for the field office covering the location of the consultant's employment or FBIHQ divisional Security Officer will be instructed by |I/FSU| to brief him/her pursuant to guidelines set out in Part I, Section 261, of the MIOG. The executed SF-312, "Classified Information Nondisclosure Agreement," must be returned to the |I/FSU| where it will be maintained.

(5) It is the responsibility of the CSO to advise the |I/FSU| when a consultant's participation in the Bureau project is no longer required. The |I/FSU| will thereafter direct the appropriate field office or FBIHQ Security Officer to debrief him/her, utilizing an SF-312. It is not necessary to debrief the individual on the same form used during the initial briefing. |(See MIOG, Part I, 260-2.5(4).)|

EFFECTIVE: 07/11/94

260-4 NONCLASSIFIED PERSONNEL/ACCESS 260C (See MIOG, Part I, 260-2 (1).)

(1) Definition

The FBI is concerned with any non-Bureau employee having access to our facilities, information, equipment or employees. Due to our investigative responsibilities in criminal and FCI matters, all contract and subcontract individuals have the opportunity to be compromised and directed by outside elements to seek sensitive criminal information or NSI in the course of their employment. This access creates a potential risk to national security, sensitive information, our facilities, equipment and employees' safety. Therefore, a consistent personnel facility access approval program for such a person must be made.

(2) Facility Access Determinations

Determinations of eligibility for personnel facility access will be made by the SPM and shall be made taking into consideration criteria set forth in EO 10450 and Director of Central Intelligence Directive 1-14 (copies maintained with each Security Officer). |All contract individuals who require access to an FBI facility or information, but don't require clearance, shall be processed for either escorted or unescorted access.|

EFFECTIVE: 07/11/94

260-4.1 Types of Personnel/Facility Access Background Investigations|(See MIOG, Part I, 260-4.1.1(2) & 260-4.3.2(3).)|

The basis for facility access eligibility approvals shall be adjudicated upon information concerning contract individuals acquired through investigative procedures or otherwise made available to the SPM. See 260-4.2 for details as to processing requirements. There are two types of background investigations which are used to approve individuals for escorted or unescorted access:

(1) |Ten-Year|Scope

(a) A|ten-year|background investigation covers the last|ten-year|period of the person's life or from age 18 to present,

whichever is shorter.

(b) Part II, Section 17-6, of this manual should be used as a guideline for processing |ten-year| scope investigations.

|(c) Twenty working days shall be allowed for I/FSU to conduct the initial processing (credit check, Criminal Justice Information Services (CJIS) Division checks, etc.) for a determination regarding "restricted" access which might allow the candidate limited access to his/her work area while the BI is being completed.|

(2) Limited

|(a) |A limited background investigation consists of FBIHQ|and/or|field office indices checks,|CJIS|Division checks,|National Crime Information Center (NCIC) wanted files, criminal history records through the NCIC Interstate Identification Index (III),|local police agency checks, and, where applicable verification of citizenship or alien status.

|(b) Five working days shall be allowed for I/FSU to conduct the above processing prior to the granting of escorted access.|

EFFECTIVE: 07/11/94

| 260-4.1.1 Types of Access| (See MIOG, Part II, 35-9.2.)|

(1) ESCORTED

(a) Approvals of ESCORTED ACCESS eligibility shall relate to the short-term, intermittent, or infrequent basis to provide some service, product, or perform some other official function of interest to the FBI. Individuals who fall within this category shall be escorted at all times.

(b) Normally a limited background investigation is required, except in the subsections noted in (c) and (d), below.

(c) Some examples of people within this category include repair service persons for electrical and plumbing equipment, vending machines, etc.

The maintenance and cleaning workers (char force) who provide daily cleaning services in resident agency (RA) offices may also fall in this category. (See paragraph (2)(c) below.)

(d) Individual(s) working on computers, telephones, and radio equipment may require a ten-year background investigation at the discretion and instruction of the SPM, FBIHQ (see Sections 260-4.3.2 and 260-4.3.3). Depending on the location of the worksite, the SAC or other designated official may require an escort for a contract individual in addition to the ten-year background investigation.

(e) A credit check is not required for a limited background investigation; however, it may be conducted at the requestor's discretion. In this instance, an FD-406 (Authority to Release Information) must be completed and forwarded to FBIHQ for processing. Credit checks will then be conducted by contractor personnel at FBIHQ.

(f) The limited background investigation should not be AUTOMATICALLY selected simply because a particular individual is going to have escorted access on a short-term or intermittent basis. (See Section 260-4.3.3 (Telephones) and (2) below (Unescorted).)

(2) UNESCORTED

(a) Approvals of UNESCORTED ACCESS eligibility shall relate to the frequency and/or recurrence of the person's access to the facility (e.g., persons performing daily maintenance or daily contracting duties generally consisting of more than 90 days). Other areas of consideration may include individuals on emergency or 24-hour call status, or an individual being exposed to equipment containing sensitive information. Unescorted access allows the contractor to go to and from his/her work area without an FBI escort. In other words, the contractor employee granted unescorted access may only access these components of the FBI facility consistent with performance of his/her contract duties.

(b) A ten-year background investigation is required. (See MIOG, Part I, 260-4.1.)

(c) The SAC may waive the ten-year background requirement for char force individuals who perform daily janitorial duties within an RA or overt off-site facility, providing that an FBI employee is present in the room while the person is cleaning. This

waiver applies only to RAs and off-site facilities. (See (1)(c).)

|(d)A security briefing should be provided to any contract individual who has been granted unescorted access privileges to FBI space. At the completion of the briefing, the contract individual should execute "Security Acknowledgement Form," FD-835, by reading the form and signing and dating the bottom of page two. The FBI employee who conducts the briefing should be identified as the Witness. The original FD-835 should be maintained in the individual's investigative file located in the field office or at FBI Headquarters (FBIHQ), depending upon where the individual is working.|

EFFECTIVE: 03/07/96

260-4.2 Forms (See MIOG, Part I, 260-4.1 & 260-4.3.2.)

(1) Processing requirements depend on the work to be performed and the type of access (escorted vs. unescorted) needed for a contract individual to perform his/her duty.

(2) Generally, a limited background investigation will be conducted on escorted individuals, whereas a ten-year background investigation will be conducted on unescorted individuals. There are exceptions to this guideline, as noted in Sections 260-4.3.2 and 260-4.3.3.

(3) The below-listed forms must be completed where applicable:

(a) STANDARD FORM (SF)-86 - QUESTIONNAIRE FOR SENSITIVE POSITIONS

The SF-86 must be completed when UNESCORTED access for contract individuals is required to FBI facilities on a daily basis, where the security clause of the contract requires it, or where exposure to sensitive material may be likely due to the type of equipment, location of work area, etc. (See MIOG, Part I, 259-2(1).) When using this form, candidates must be interviewed, to ensure all questions have been answered and information required to conduct the background investigation has been furnished. The results of the interview shall be furnished on an FD-302 and accompany the FD-316, SF-86, and other required forms, upon submission to FBIHQ. Refer to Part II, Section 17-6 of this manual for guidance.

NOTE: An FD-484 and FD-406 are NOT used in conjunction with an SF-86. All SF-86 forms dated prior to December, 1990, are obsolete and should be destroyed. Obsolete forms will not be processed by the Industrial/Facility Security Unit.

(b) Form FD-816, "Access of Non-FBI Personnel to FBI Facilities, Background Data Information Form."

The FD-816 must be completed for all contract individuals who require escorted access to any FBI facility (i.e, Quantico, field office, resident agency, etc.).

(c) FORM FD-258 - FBI FINGERPRINT CARD

Two sets of fingerprint cards (only one card required if fingerprinted at FBIHQ) must be completed for all contract individuals who require access, whether escorted or not, to FBI facilities on two or more occasions. This requirement for contract individuals for access not to exceed five days, on a one-time basis only, may be waived.

(d) FORM FD-316 - "ISP, ACCESS OF NON-FBI PERSONNEL TO FBI FACILITIES"

The FD-316 is the form used to request access to an FBI facility by non-FBI individual(s) contracted to perform a service for the Bureau. The FD-316 is to be completed by the Bureau employee who is requesting the access for the non-FBI contract individual(s).

(e) FORM FD-406 - "AUTHORITY TO RELEASE INFORMATION"

The FD-406 must be completed for obtaining sensitive information, i.e., credit checks, medical records, etc., when an SF-86 is not necessary. This form should not be submitted in conjunction with an SF-86. Credit checks will be processed by contractor personnel at FBIHQ once the FD-406 is completed and forwarded to FBIHQ.

(f) FORM FD-484 - "PRIVACY ACT ACKNOWLEDGEMENT"

A Form FD-484, signed and dated by the contract individual, must be attached to each FD-316 when an SF-86 is not required. A copy should be given to the individual requiring access.

|(g) FORM FD-835 - "SECURITY ACKNOWLEDGEMENT FORM"

The Form FD-835 is to be signed and dated by the contract individual, who has been granted unescorted access privileges to FBI space. The FBI employee who conducts the briefing should be identified as the Witness. By use of this form, in the event of a security violation, the FBI will have a record that the information was provided to the contractor. The original FD-835 should be maintained in the individual's investigative file located in the field office or at FBIHQ, depending upon where the individual is working.|

The below-listed examples should be used as a guideline for processing purposes:

| ESCORTED ACCESS (Field Office or FBIHQ) | UNESCORTED ACCESS (Field Office or FBIHQ) |
|---|---|
| FD-316 | FD-316 |
| FD-816 | SF-86 |
| FD-484 | FD-258 (Two copies) (One copy if taken at FBIHQ) |
| FD-258 (Two copies) (One copy if taken at FBIHQ) | |
| | FD-835 |

EFFECTIVE: 03/07/96

||260-4.3| Special Cases

EFFECTIVE: 04/19/91

||260-4.3.1| Aliens

Immigrant aliens and foreign nationals who contract with or are employed by the United States Government are not eligible for the same type of access eligibility approval that may be granted to United States citizens, but may only be provided with limited access authorizations which shall authorize access only for specific programs, projects, or contracts. Long-term contracts requiring daily access to FBI facilities (i.e., maintenance workers) should be reserved for U.S. citizens.

EFFECTIVE: 04/19/91

260-4.3.2 Computers (See MIOG, Part I, 260-2(1), 260-4.1.1(1)(d) & 260-4.2(2).)

(1) A microcomputer is classified at the highest level of information that has been entered into, stored on, or processed by the system unless the COMPUTER SYSTEM can be appropriately declassified. Automated Data Processing STORAGE MEDIA (operative and inoperative, removable and nonremovable) and NONVOLATILE MEMORY DEVICES may NEVER be downgraded or declassified in the field.

(2) Hardware and/or software maintenance on classified computer devices may only be performed by individuals possessing a clearance commensurate with the classification levels of the computer equipment..

(3) Individuals performing hardware and/or software maintenance on unclassified computer devices must, at a minimum, be subject to a limited background investigation consisting of those checks identified in Section 260-4.1, "Types of Personnel/Facility Access Background Investigations," and 260-4.2, "Forms."

(4) Because hardware and software maintenance activity may affect the integrity of existing protection measures or permit the introduction of security exposures into a system (e.g., computer viruses, trojan horses, logic bombs, implant devices, etc.), all maintenance work must be supervised by FBI personnel knowledgeable in the operation of microcomputers, regardless of the classification of the microcomputer or its associated media.

See MIOG, Part I, 261-2(1), "Federal Bureau of Investigation, ADPT Security Policy," for more information.

EFFECTIVE: 07/11/94

260-4.3.3 Telephones (See MIOG, Part I, 260-4.1.1(1)(d) & (f), 260-4.2(2).)

(1) As all new contracts with telephone companies will contain an updated security clause, the scope of the background investigation will not coincide Bureauwide until all contracts have been renewed.

(2) The field office Supervisory Administrative Specialist (SAS) should be contacted to determine the scope of the background investigation of a telephone company employee in coordination with FBIHQ.

(3) All telephone company employees who require access to FBI facilities to perform installations within or service to the telephone switch shall be afforded a ten-year background investigation.

EFFECTIVE: 07/11/94

260-4.3.4 Photocopiers

All photocopier technicians who require access to FBI facilities to service photocopying machines must be processed for a ten-year background investigation. This policy applies to all FBI facilities, including resident agencies.

EFFECTIVE: 07/11/94

260-4.3.5 Contract Physicians

To assist the FBI in conducting the required periodic and/or fitness-for-duty evaluations for on-board employees and applicants, the Health Care Programs Unit (HCPU), Personnel Division, FBI Headquarters (FBIHQ), grants contracts to physicians within each FBI field office territory, as well as Clarksburg, West Virginia; the FBI Academy, Quantico, Virginia; and FBIHQ. The majority of the fitness-for-duty physicals occur within the office space of the

contract physician, as opposed to the actual FBI facility.

(1) SECURITY REQUIREMENTS

(a) Prior to granting the contract to a medical group or local physician, the HCPU, Personnel Division, FBIHQ, may require the field office to conduct an on-site inspection of the physician's office. The inspection will determine the level of security which will be afforded to the FBI information provided to contract physicians, whether medical, personal, or administrative data.

1. If within regular Bureau space, security of documentary materials shall be no less than a locking file-type or similar cabinet in a restricted access location. If the volume of data requires the open storage of such materials, a dedicated closet, room, or facility shall be provided to which there is restricted access by only medical and other authorized personnel. The door(s) to this location shall be equipped with security locking hardware, uniquely keyed to maintain access to only medical or other authorized personnel.

2. If within contractor space and Bureau material is identifiable as such, security of documentary materials shall be no less than a locking file-type or similar cabinet maintained in a location to which only Bureau-approved personnel have access. If the volume of the materials is such that open storage is required, it shall be maintained in a restricted-access area, the doors to which are equipped with security locking hardware, uniquely keyed to restrict access to only Bureau-approved personnel to have access. The general office space shall have typical business-type facility protections. Although an intrusion detection system is preferred, one is not required. No classified material may be maintained in this facility, unless approved in writing by the Security Programs Manager, FBIHQ, and both the facility and the appropriate employees have been cleared at the appropriate level for handling or maintenance of classified materials.

(2) REQUIRED FORMS

All physicians being considered as potential contractors will be required to complete either an SF-85p, "Questionnaire for Public Trust Positions," or an SF-86, "Questionnaire for National Security Positions." The appropriate form to be completed will be determined based on the location of where the physicals will be performed.

(a) If the physicals will be conducted in the physician's office, then the physician would be required to complete the SF-85p. If the physicals will be performed within the field office space, the physician would be required to complete the SF-86. Regardless of which form is executed, it should be completed in its entirety, and ALL release forms and certification statements must be signed and dated.

(b) Each physician will be required to submit two FD-258 (blue) fingerprint cards.

(3) FIELD OFFICE PRELIMINARY INVESTIGATIVE RESPONSIBILITIES

(a) Appropriate field office checks must be conducted on the contract physician prior to submitting the security forms to FBIHQ for processing. The appropriate checks should include field office indices, local law enforcement checks, and a review of computerized National Crime Information Center (NCIC) Wanted File records and Interstate Identification Index (III) criminal history checks. When conducting the III checks, both "QH" and "QR" checks should be conducted, if possible.

(b) The physician should be provided with a standard candidate interview consisting of a review of information provided by the individual on his/her appropriate background form to ensure the accuracy of the information. Issues of concern or security-related matters should be addressed, if identified. During the interview, the physician should be asked the question, "Have you ever had your medical privileges suspended or revoked?" The results of the candidate interview should be provided on an FD-302.

(c) The requesting field office will be responsible for assigning the 260 file number. Each physician should be assigned an individual file number.

(4) SUBMISSION OF THE REQUEST

Although the physicians will be processed under the 260 classification, the method of requesting the background investigation is different than outlined in Part I, Section 260, MIOG. Requests for conducting a BI on a contract physician shall be submitted using the Electronic Communication (EC) format marked to the attention of the I/FSU, NSD, Room 4362, and the HCPU, Personnel Division, Room 6344, each with leads "For appropriate action."

The same EC shall also set forth field office leads to verify the proposed physician's status with the American Medical Association (AMA) and State Licensing Bureau (SLB). Determine if the candidate physician is currently licensed to practice medicine, certified by the AMA, and if there have been any claims of malpractice filed against the physician. When obtaining this information, the following questions should be used:

QUESTIONS TO THE AMA:

"Is the candidate a person of good standing with the AMA?"

"Has the candidate ever had any medical claims against him/her?" If yes, what are they, when did they occur, and what was the outcome of the claim.

QUESTIONS FOR THE SLB:

"Does the candidate have a current license to practice medicine in this state?"

"Has the candidate ever had his/her license suspended or revoked?" If so, when and for what reason.

LEADS TO CONDUCT THE REMAINING INVESTIGATION SHOULD BE HELD IN ABEYANCE UNTIL FURTHER NOTICE FROM THE I/FSU.

For contractual reasons, the results of the above investigation shall be received at FBIHQ within ten working days from the date of the requesting EC. Copies of the investigative results should be directed to the attention of both the I/FSU and HCPU.

(5) CONDUCTING THE REMAINING INVESTIGATION

The I/FSU will adjudicate the results of all preliminary investigation to determine if the remaining BI should be initiated. If the remaining investigation is to be conducted, the I/FSU will promptly initiate the appropriate leads. At the same time, the EC setting forth the remaining investigation will advise the initiating division if the physician has been approved for access to FBI information or facilities pending completion of his/her BI. This office will be responsible for notifying the appropriate field office personnel of this information. Separate notification may also come from the HCPU.

(6) SUBMISSION OF FINAL BACKGROUND INVESTIGATION RESULTS

(a) Results of the additional BI conducted shall be provided only to the I/FSU, NSD. THE HCPU WILL RECEIVE ONLY THE RESULTS OF THE PRELIMINARY INVESTIGATION QUESTIONS.

(b) Upon review of the completed investigative results, the Security Programs Manager, NSD, will provide the final adjudication concerning the continual access of the physician to FBI information and facilities.

(7) SUBMISSION BY FBIHQ AND FBIHQ FACILITIES

(a) The medical staff assigned to Clarksburg, West Virginia, or Quantico, Virginia, will be responsible for conducting a preliminary review of the application to determine if all of the requested information has been provided. The HCPU will handle this function for FBIHQ.

(b) Once the BI questionnaires are determined to be acceptable, the medical staff or HCPU should contact the AMA and SLB to determine the answers to the questions previously set forth. Upon receipt of this information, the security forms should be furnished to the I/FSU, NSD, by an EC. The results of the questions should be provided. Requests from Clarksburg, West Virginia, and Quantico, Virginia, should send a copy of the requesting EC to the attention of the HCPU, Personnel Division, with the original coming to I/FSU, NSD.

(c) Following the adjudicative review of the initial background checks, the I/FSU will set forth instructions to the appropriate field office or Background Investigative Contract Services (BICS) territory to conduct the initial candidate interview, obtain the file number for each submission, and, when appropriate, initiate the BI, as outlined above.

(8) FBI FIELD OFFICE PROCESSING OF THE PHYSICIAN'S OFFICE STAFF

(a) Each member of the physician's office staff who will have access to the records and administrative information pertaining to FBI referrals will require a limited BI. Noting that these individuals will be responsible for the security of sensitive medical and related data pertaining to Bureau personnel and applicants (through the initial candidate interview, office security visit or other appropriate means), it will be the responsibility of the handling office to identify the applicable staff members. Each

individual will be required to complete Form FD-816, "Access of Non-FBI Personnel to FBI Facilities Background Data Information"; Form FD-484, "Privacy Act Acknowledgement"; and two FD-258 (blue) fingerprint cards. The field office shall conduct appropriate local record checks and submit the results to FBIHQ using the same procedures for processing escorted access requests as set forth in the MIOG, Part I, Section 260.

(b) Upon favorable adjudication of local record checks, the SAC of the requesting office may grant the equivalent of escorted access UACB. Requests which contain derogatory information which cannot be mitigated according to Bureau guidelines will be adjudicated on a case-by-case basis by the Security Programs Manager (SPM).

(9) FBIHQ AND FBIHQ FACILITIES - PROCESSING OF THE PHYSICIAN'S OFFICE STAFF

The security forms outlined above will be required for FBIHQ facilities contracts as well. Once the forms are obtained, they should be forwarded to the I/FSU for processing.

EFFECTIVE: 11/12/96

260-5 PERSONNEL CLEARANCE REINVESTIGATIONS 260E

EFFECTIVE: 03/07/96

260-5.1 Personnel Clearance Reinvestigations - Annual Reinvestigations of Contract Linguists (See MIOG, Part II, 17-2.)

All FBI Contract Linguists on-board in excess of one year will be subject annually to a personnel security interview (PSI) to determine their continued "trustworthiness" to NSI. The PSI will cover, but not be limited to, the following:

(1) Changes in any information provided in the original application.

(2) Foreign travel, if any, during the past year.

(3) Contact, if any, with a foreign national not previously identified in the original SF-86.

(4) Any other employment or source of income not reported to the FBI.

EFFECTIVE: 03/07/96

260-5.2 Personnel Clearance Reinvestigations - Contractors Other Than Contract Linguists (See MIOG, Part II, 17-2.)

All FBI contractor personnel possessing current and active security clearances five years old or more are to be reinvestigated to ensure trustworthiness for continued access to NSI.

(1) Individuals due for the five-year reinvestigation, both at the "Secret" and "Top Secret" levels, will be identified by FBIHQ. The reinvestigation will be initiated via communication from FBIHQ which will enclose the Standard Form 86 (SF-86) and set forth the required investigation.

(2) The reinvestigation for a "Secret" security clearance will include a candidate interview, a check of FBI indices (field and FBIHQ), automated data bases (FBIHQ), national agency checks (FBIHQ), local agency checks/arrest checks (field), and credit bureau checks (FBIHQ).

(3) The "Top Secret" reinvestigation will encompass the same areas as the "Secret" level and, in addition, will include verification of residence, interview of two neighbors, review of employment records, two employment references, and two character references developed by the investigator and not provided by the candidate.

(4) In all instances the investigation must be expanded to resolve any derogatory or adverse information. Newly listed information within the scope of the investigation, such as

education, recent divorce, roommate, part-time military service, and foreign travel must be addressed.

(5) Conduct investigation in accordance with the policy and procedures set out in MIOG, Part II, 17-6, entitled "Scope of Full Field Investigations."

EFFECTIVE: 03/07/96

260-6 CHARACTER - INDUSTRIAL SECURITY PROGRAM - PERSONNEL CLEARANCE; - FACILITY CLEARANCE; - NONCLASSIFIED PERSONNEL/ACCESS; -OTHER; PERSONNEL CLEARANCE REINVESTIGATIONS (See MAOP, Part II, 3-1.1 & 3-1.2.)

EFFECTIVE: 03/07/96

OPCA-20 (12-3-96)

XXXXXX
XXXXXX
XXXXXX

**FEDERAL BUREAU OF INVESTIGATION**
**FOIPA**
**DELETED PAGE INFORMATION SHEET**

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

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

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

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

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

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

8 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:

_____

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

XXXXXX
XXXXXX
XXXXXX

FBI/DOJ

# SECTION 261. SECURITY OFFICER MATTERS (SOM)

261-1 BACKGROUND AND PURPOSE (See MIOG, Part I, 67-18 (3), 259-2 (6), & 260-3.2(4); MAOP, Part I, 15-3.4(1).)

Each FBI Headquarters division and office, field office and Legal Attache will designate a Supervisory Special Agent (GM-14 or above) as the Security Countermeasures Program Manager (SCMPM). This individual is responsible for the management of all FBI Security Program activities, including specific Security Officer responsibilities in their division/office. A Security Officer and as many Alternate Security Officers as necessary should be employed to administer the Security Program. Wherever possible, Special Agents should be designated to serve as Security Officers and Alternate Security Officers. The Security Programs Manager (SPM), National Security Division, FBIHQ, should be kept advised of the identities of designees. To avoid potential conflicts of interest, the Employee Assistance Program (EAP) Coordinator (or counselor) or anyone administering the EAP should not also be assigned the responsibilities of SCMPM and/or Security Officer. (See FCI Manual, Part II, 1-1.)

EFFECTIVE: 11/15/93

261-2 PROGRAM FUNCTIONS (See MAOP, Part II, 3-1.1 & 3-1.2; and National Foreign Intelligence Program Manual (NFIPM), Part I, 8-1.1.)

Under the above caption, the functions of these programs are as follows:

(1) 261A - SOM - AUTOMATED DATA PROCESSING/ TELECOMMUNICATIONS SECURITY (ADP/T)

The ADP/T security will consist of those activities involved in the protection of information while being stored, processed, handled, or transmitted by ADP/T systems. The ADP/T security operates under the guidelines set forth in the FBI's Automated Data Processing and Telecommunications Security Policy, MIOG, Part II, Section 35. The responsibilities of the Security Officer are to ensure compliance with FBIHQ security policy for FBI

c. Private contractor personnel in connection with the Industrial Security Program.

d. If so designated, may conduct or participate in security debriefings of certain Bureau applicants who are the subjects of specific reviews or inquiries directed by the SPM or SPM's designee.

e. If so designated, other non-Bureau personnel, as circumstances may require.

5. Conduct periodic security awareness updates at scheduled SAC, support, and SA conferences, and on other occasions, as appropriate.

6. As designated, special individualized security awareness briefings or debriefings of current Bureau employees who are the subjects of specific reviews or inquiries directed by the SPM or SPM's designee.

7. Briefing FBI personnel involved in the management, operation, programming, maintenance, or use of FBI ADPT systems to make them aware of the threats to and vulnerabilities of those systems, and appropriate security countermeasures.

8. Under the Personnel Security Interview (PSI), the time expended on this interview is to be captured for TURK purposes under the FBI Security Program, entitled "Security Officer Matters," by utilization of classification 261B. Additionally, for TURK purposes a record of the interview is to be maintained in the field office in a control file under the 261B classification. (For complete details see MIOG, Part I, 67-7.9, 67-7.9.1, 67-7.9.2 & 67-7.9.2(11).)

(d) Each field office is to establish a control file under the 261B classification. A record of each briefing/debriefing conducted is to be maintained in this control file, in addition to a copy which is to be maintained in the individual substantive file to which the matter relates. The time expended on any of the above briefings/debriefings is to be captured for TURK purposes under the 261B classification. (See MIOG, Part I, 67-7.9.2 (11).)

(e) All specialized training on the topics of security awareness and Security Awareness Briefings provided to FBI employees shall be documented and placed on record in the security/investigative section of the employee's personnel file.

(3) 261C - SOM - INFORMATION SECURITY

The Executive Order|12958;|Department of Justice Implementation Order 28; Code of Federal Regulations, Part 17; and Part II, Section 26, of this manual, set forth procedures for classifying and safeguarding NSI, and investigating security violations involving NSI. The activities of the Security Officer would be as follows:

(a) Ensure procedures are followed for the classification, storage, transmission and destruction of NSI. (See Part II, Section 26, of this manual.)

(b) Ensure procedures are followed in the conduct of a damage assessment concerning the loss or possible compromise of classified information. See Part II, Section 26-13.1, of this manual, and Memorandum to all SACs 22-85, dated July 23, 1985, entitled "Loss or Possible Compromise of Classified Information."

(c) Act as "Top Secret" and Sensitive Compartmented Information (SCI) Control Officer. See Part II, Sections 26-6 and 26-10, of this manual.

(d) Other activities expended on the protection of NSI are not specifically enumerated.

(4) 261D - SOM - PHYSICAL SECURITY

The goal of Physical Security is to help ensure the safety and integrity of Bureau facilities, information, and personnel through the use of physical barriers designed to prevent unauthorized access by any individual or group whose interests may be inimical to those of the Bureau or the United States. FBIHQ and field divisions should direct any inquiries to the Facility Security Unit, Security Countermeasures Section, National Security Division, FBIHQ.

(a) |The General Services Administration (GSA) tests and provides the minimum standards for storage equipment used to protect classified materials and information. The Department of Justice (DOJ) provides implementing guidelines in Title 28, Code of Federal Regulations, Part 17, or in the form of Orders, Security Bulletins, or letters to the heads of agencies and bureaus. Guidelines for the protection of storage of classified materials and information are set forth in Part II, Section 26-5 of this manual.|

(b) For the administrative responsibilities of a Security Officer with regard to the proper use and changing of lock combinations and the maintenance of lock combination records, refer to Part II, Sections 16-7.2.6(9) and 26-5.4, of this manual. (See National Foreign Intelligence Program Manual, Part I, 8-5.4.)

(c) Electronic Technicians have installation and maintenance responsibilities for Hirsch Access Control Systems.

(5) 261E - SOM - OPERATIONS SECURITY

Operations Security (OPSEC) is an analytical process which denies potential adversaries information concerning operations and intentions by identifying and protecting generally unclassified indications of sensitive operations and activities. Overall management of this program is the responsibility of the Security Programs Manager (SPM). Local management of OPSEC is the responsibility of the Security Countermeasures Program Manager (SCMPM) in each division or office. Inquiries should be directed to the Information Systems Security Unit, Security Countermeasures Section, National Security Division, FBIHQ.

(a) OPSEC addresses five areas:

1. Identification of critical information
2. Threat analysis
3. Vulnerability analysis
4. Risk assessment
5. Applicable countermeasures

(b) OPSEC should be actively practiced in all facets of FBI operations, programs, and administrative procedures.

(c) An OPSEC control file is to be established by each field and FBIHQ division and office, Legat, Regional Computer Center, and, as applicable, other off-site locations. Any time the OPSEC process is formally applied to any investigative or administrative matter, this fact is to be documented in the affected file, with a copy designated to the control file.

(6) 261F - SOM - EMERGENCY PLANS

Executive Order 12656, and various Department of Justice Orders direct the FBI to prepare Emergency Plans (EP) to protect life and property and to ensure the continuity of essential operations in any emergency. Overall management of EP activities is the responsibility of the Security Programs Manager. Local management of EP is the responsibility of the SAC and the Security Officer (SO) in each field and FBIHQ division. Inquiries should be directed to the Information Systems Security Unit, Security Countermeasures Section, National Security Division, FBIHQ.

(a) Emergency Plans address the following areas:

1. Preparation of an Occupant Emergency Plan (OEP) for FBI facilities to minimize risk to life and property during fire, bombing, earthquake, civil disturbance or other emergency. The OEP is a document that sets forth procedures and assigns responsibility for an orderly and systematic response to emergencies in order to protect people, property and information.

In buildings or facilities where the FBI is the prime tenant, the Senior Official in Charge (SOIC) of the FBI resident component, with the assistance of the Division Security Officer and the Collateral Duty Safety Officer, shall be responsible for development of the OEP. Where the FBI is not the prime tenant, the SOIC shall cooperate with the prime tenant to develop an OEP. If the prime tenant fails to develop an adequate OEP, the SOIC shall develop an independent plan to ensure the safety of FBI personnel and the protection of FBI property. The term "prime tenant" is defined as the organization with the largest number of employees in a building or facility.

The OEP shall include a written memorandum to occupants addressing evacuation procedures in the event of fire or other emergency. The plan shall also designate handicap, stairway and floor monitors, where necessary, to assist personnel during an evacuation. Additionally, procedures for the protection of classified and sensitive information during an evacuation should be incorporated into the OEP. To facilitate development of a plan, the NSD, SCMS, ISSU, has available a booklet titled "OCCUPANT EMERGENCY PROGRAM GUIDE," published by the General Services Administration. This booklet outlines a step-by-step approach to development of an OEP.

The OEP shall be reviewed annually and updated as necessary. Prime tenants should also conduct and document an annual evacuation drill. Whenever the FBI occupies a new or modified facility, an OEP shall be developed within 30 days of occupancy.

2. Preparation of tactical security plans for each FBI-controlled facility, whether covert or overt, to manage, contain, and neutralize hostile actions directed at or in those facilities. Plans shall document procedures, outline authorities, and assign responsibilities for an orderly and systematic response. Each facility housing more than 50 personnel shall have its own plan. At the discretion of the preparing office, multiple locations with less than 50 personnel each may be addressed in one plan or contained as an appendix to the headquarters city plan.

Where FBI employees are located in facilities not controlled by the FBI, every effort should be made to afford them the same protections they enjoy in FBI space. If security is deemed inadequate at these facilities, appropriate action should be taken to include removal of employees from the space.

Preparation of tactical security plans should be a cooperative effort between the SAC, the Security Officer, the SOIC of the facility, and the SWAT Team Leader. Additional guidance is available in the Manual of Investigative Operations and Guidelines (MIOG), Part II, 30-1, titled "Crisis Management Program," and FBIHQ airtel to all offices dated February 10, 1995, captioned "Physical Security; Tactical Plans for Field Office, Resident Agency, and Off-Site FBI Space," or from the SAC, Critical Incident Response Group (CIRG), Quantico. Plans shall be reviewed annually and updated as necessary.

3. Identification of critical FBI functions and the resources necessary to carry out those functions in time of emergency.

4. Identification of relocation sites, development and maintenance of plans to relocate critical functions to those sites in time of emergency. (Note that MIOG, Part II, 26-3.4, directs that the identity, location and other factors concerning FBI relocation sites be classified "Secret" until the activation of those sites during a national security emergency.)

5. Promotion of individual and family preparedness among FBI employees to ensure their safety, speedy recovery, and return to duty following an emergency. A variety of preparedness materials are available from local emergency management agencies, the Federal Emergency Management Agency (FEMA), and the NSD, SCMS, ISSU, FBIHQ.

6. Cooperation with certain other government agencies, as directed by the SPM, in the development and maintenance of plans to ensure continuity of government in national security emergencies.

(7) 261G - SOM - ALL OTHER

This category will encompass the duties Security Officers perform which are not specifically addressed in A through F above.

The other classifications in the FBI Security Program are 67E, 259, and 260 and are explained in those sections of the MIOG, Part I.

EFFECTIVE: 09/09/97

261-3 CHARACTER - SECURITY OFFICER MATTERS

EFFECTIVE: 02/12/92

# SECTION 262. OVERSEAS HOMICIDE/ATTEMPTED HOMICIDE - INTERNATIONAL TERRORISM (OHAHT)

## 262-1 OVERSEAS HOMICIDE/ATTEMPTED HOMICIDE - INTERNATIONAL TERRORISM

(1) The Omnibus Diplomatic Security and Antiterrorism Act of 1986 (ODSAA), Public Law 99-399, created Section 2331 in Title 18 of the United States Code (USC), entitled, "Terrorist Acts Abroad Against United States Nationals," which became effective August 27, 1986.

(2) This section makes it unlawful for any person to assault, attempt to kill or kill a United States national while that person is outside the United States or its territories. To enter into a conspiracy to commit an assault, attempt to kill or murder is also considered unlawful under this statute.

EFFECTIVE: 07/14/88

## 262-2 BACKGROUND

In an effort to protect United States nationals abroad from acts of terrorism, as part of the Omnibus Diplomatic Security and Antiterrorism Act of 1986 (ODSAA), Congress enacted a provision regarding assaults and murder of United States nationals. Prior to this legislation only Government officials and diplomatic persons were protected from such attacks under Federal law. These steps were taken as there are no international agreements to protect individuals from such attacks. An important feature of this statute is that before any prosecution of this offense is initiated it requires written certification from the Attorney General or the highest subordinate of the Attorney General with responsibility for criminal prosecutions to state that the offense committed was to coerce or influence a government or civilian population.

EFFECTIVE: 07/14/88

262-3 STATUTE, PENALTY AND DEFINITIONS

Title 18, USC, Section 2331, reads as follows:

"2331. Terrorist acts abroad against United States nationals

"(a) HOMICIDE.-- Whoever kills a national of the United States, while such national is outside the United States, shall--

"(1) if the killing is a murder as defined in section 1111(a) of this title, be fined under this title or imprisoned for any term of years or for life, or both so fined and so imprisoned;

"(2) if the killing is a voluntary manslaughter as defined in section 1112(a) of this title, be fined under this title or imprisoned not more than ten years, or both; and

"(3) if the killing is an involuntary manslaughter as defined in section 1112(a) of this title, be fined under this title or imprisoned not more than three years, or both.

"(b) ATTEMPT OR CONSPIRACY WITH RESPECT TO HOMICIDE.-- Whoever outside the United States attempts to kill, or engages in a conspiracy to kill, a national of the United States shall--

"(1) in the case of an attempt to commit a killing that is a murder as defined in this chapter, be fined under this title or imprisoned not more than 20 years, or both; and

"(2) in the case of a conspiracy by two or more persons to commit killing that is a murder as defined in section 1111(a) of this title, if one or more of such persons do any overt act to effect the object of the conspiracy, be fined under this title or imprisoned for any term of years or for life, or both so fined and so imprisoned.

"(c) OTHER CONDUCT.-- Whoever outside the United States engages in physical violence--

"(1) with intent to cause serious bodily injury to a national of the United States; or

"(2) with the result that serious bodily injury is caused to a national of the United States; shall be fined under this title or imprisoned not more than five years, or both.

"(d) DEFINITION.-- As used in this section the term 'national of the United States' has the meaning given such term in section 101(a)(22) of the Immigration and Nationality Act (8 U.S.C. 1101(a)(22)).

"(e) LIMITATION ON PROSECUTION.-- No prosecution for any offense described in this section shall be undertaken by the United States except on written certification of the Attorney General or the highest ranking subordinate of the Attorney General with responsibility for criminal prosecutions that, in the judgment of the certifying official, such offense was intended to coerce, intimidate, or retaliate against a government or a civilian population."

As used in this section United States nationals are defined pursuant to Section 101(a)(22) of the Immigration and Nationality Act (codified at Title 8, USC, Section 1101(a)(22)) as set forth below:

"The Term 'national of the United States' means (A) a citizen of the United States, or (B) a person who, though not a citizen of the United States, owes permanent allegiance to the United States."

EFFECTIVE: 07/14/88

262-3.1 Extension of Statute of Limitations for Certain Terrorism Offenses (Title 18, USC, Section 3286) (Also see MIOG Part II, 1-4.)

"Notwithstanding section 3282, no person shall be prosecuted, tried or punished for any offense involving a violation of section 32 (aircraft destruction), section 36 (airport violence), section 112 (assaults upon diplomats), section 351 (crimes against Congressmen or Cabinet officers), section 1116 (crimes against diplomats), section 1203 (hostage taking), section 1361 (willful injury to government property), section 1751 (crimes against the President), section 2280 (maritime violence), section 2281 (maritime platform violence), section 2331 (terrorist acts abroad against United States nationals), section 2339 (use of weapons of mass destruction), or section 2340A (torture) of this title or section 46502, 46504, 46505 or 46506 of title 49, unless the indictment is found or the information is instituted within eight years after the offense was

committed."

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

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

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

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

EFFECTIVE: 11/24/95

262-4 ELEMENTS OF THE OFFENSE

(1) HOMICIDE.-- This provision of the statute makes it an offense to kill a United States national, while such is outside the territorial limits of the United States by means of murder, voluntary manslaughter or involuntary manslaughter. It is important to note the commission of the homicide must take place outside of the United States.

(a) MURDER for this section is defined as the unlawful killing of a human being with malice aforethought.

(b) VOLUNTARY MANSLAUGHTER for purposes of this section is defined as the unlawful killing of a human being without malice as the result of a sudden quarrel or heat of passion.

(c) INVOLUNTARY MANSLAUGHTER for purposes of this section is defined as the unlawful killing of a human being without malice during the commission of an unlawful act not amounting to a felony, or in the commission in an unlawful manner, or without due caution and circumspection, of a lawful act which might produce death.

(2) ATTEMPT OR CONSPIRACY WITH RESPECT TO HOMICIDE.-- This provision makes it unlawful for any person outside the United States to attempt to kill or engage in a conspiracy to kill a United States National. Note here that it is the attempt or conspiracy which must take place outside of the United States irrespective of the location of the United States national at the time of the conspiracy. An attempt to kill ordinarily means a person has the intent to kill combined with an act which falls short of actually killing the person.

The conspiratorial aspect of this offense makes it unlawful for two or more persons outside the United States to conspire to commit a killing that is a murder, if one or more members of the conspiracy do any overt act to effect the objective of the conspiracy. It is the conspiracy which must take place outside the United States irrespective of the location at that time of the United States national.

(3) OTHER CONDUCT.-- The statute makes it unlawful for any person outside the United States to engage in any act of physical violence which is intended to cause or actually causes serious bodily injury to a United States national.

(4) LIMITATION ON PROSECUTION.-- Before any suspected violations of this section can be prosecuted, it is required that the Attorney General or the highest ranking subordinate of the Attorney General with responsibility for criminal prosecutions certify in writing that in his judgment the violation of this statute was intended to coerce, intimidate, or retaliate against a government or a civilian population. Therefore, not only is the intent element necessary with respect to the type of offense committed, i.e., homicide or conspiracy, but an additional element of intent must be demonstrated, that is, it must be for the purpose to coerce, intimidate or retaliate against a government or civilian population. These actions are not restricted to the United States Government but to any government.

EFFECTIVE: 07/14/88

262-5 PENALTIES UNDER SECTION 2331

This statute prescribes the imposition of penalties for the various offenses contained therein as follows:

(1) MURDER -- to be fined in accordance with provisions of Title 18 of USC and/or imprisoned for any term of years or for life;

(2) VOLUNTARY MANSLAUGHTER -- to be fined in accordance with provisions of Title 18 of USC and/or imprisoned for not more than ten years;

(3) INVOLUNTARY MANSLAUGHTER -- to be fined in accordance with provisions of Title 18 of USC and/or imprisoned for not more than three years;

(4) ATTEMPTED MURDER -- to be fined in accordance with provisions of Title 18 of USC and/or imprisoned for not more than 20 years;

(5) CONSPIRACY TO COMMIT MURDER -- to be fined in accordance with provisions of Title 18 of USC and/or imprisoned for any term of years or for life;

(6) SERIOUS BODILY INJURY -- to be fined in accordance with provisions of Title 18 of USC and/or imprisoned for not more than five years.

EFFECTIVE: 07/14/88

262-6 INVESTIGATIVE OBJECTIVES

An effective investigative activity must be taken in order to identify and eventually apprehend and prosecute the subject(s) involved.

EFFECTIVE: 07/14/88

262-7 REPORTING PROCEDURES

EFFECTIVE: 07/14/88

262-7.1 Initial Notifications

(1) Immediately advise FBIHQ, Counterterrorism Section, Criminal Investigative Division, by telephone, followed by teletype, of every preliminary inquiry and investigation instituted under the ODSAA of 1986.

(2) Those field offices and Legal Attaches deemed appropriate should be included as recipients of the initial teletype to FBIHQ.

EFFECTIVE: 07/14/88

262-7.2 Notification to FBIHQ regarding Final Outcome

(1) In order that the FBIHQ substantive case file may indicate the final outcome of each investigation of a possible violation, the following FBIHQ notification policy should be adhered to by the office of origin.

(2) In all cases, including those cases in which the United States Attorney declines or defers prosecution and those cases determined not to be a violation of OSDAA of 1986, a closing communication should be directed to FBIHQ clearly setting forth the basis for closing. Legal Attaches should report to FBIHQ information regarding prosecutions or declinations of these cases in foreign countries.

EFFECTIVE: 07/14/88

262-8 LIAISON AND COORDINATING RESPONSIBILITIES

EFFECTIVE: 07/14/88

262-8.1 Legal Attache Responsibilities

(1) Legal Attaches must establish close liaison with affected foreign law enforcement agencies, as well as appropriate U.S. Embassy personnel, to ensure that the FBI is apprised of any terrorist incidents which may fall under our investigative jurisdiction.

(2) Upon the receipt of information that a United States national(s) has been a victim of a homicide/attempted homicide outside United States territorial boundaries and this investigation could fall within the jurisdiction of the FBI under the ODSAA of 1986 (Title 18, USC, Section 2331), the Legal Attache should contact the foreign law enforcement agency handling the investigation and obtain all facts pertinent to the homicide/attempted homicide after coordinating with the appropriate embassy personnel. Particular attention should be paid to whether any demands have been made of the United States Government or any United States corporation.

(3) The Legal Attache should immediately advise the Counterterrorism Section, Criminal Investigative Division, FBIHQ, and the office of origin of an overseas homicide/attempted homicide situation. (See 262-9.)

(4) The Legal Attache, in consultation with FBIHQ and the United States Department of State (USDS), will ascertain if the case is of such magnitude as to warrant the deployment of Special Agent personnel from the office of origin to assist in conducting the investigation in concert with the appropriate foreign law enforcement agencies and whether the host country is in agreement and will allow such personnel in the country.

(5) In those cases where FBIHQ and USDS concur, the Legal Attache should provide an offer of FBI assistance, both investigative and technical, to the principal investigative law enforcement agency.

(6) The Legal Attache is to ensure that immediately after the host government has given permission for FBI investigative involvement that steps are taken to ensure protection of the crime scene and that appropriate FBI personnel (i.e., FBI forensic team, etc.) to the extent possible, are the first investigative group to have access to the crime scene before any other U.S. Government representatives. These procedures are necessary to avoid contamination of the crime scene by noninvestigative personnel.

(7) Because autopsy reports are an integral part of any prosecution, in the event a U.S. citizen is killed, the Legal Attache

is to initiate arrangements with the appropriate USDS representatives for transportation of the victim's body to the United States for autopsy.

(8) The Legal Attache should ensure, to the degree possible, that when investigations are conducted by foreign law enforcement personnel, copies of such investigations are made available to the FBI. In the event the host country does not intend to prosecute the perpetrators, the Legal Attache should, if possible, obtain any evidence available through the investigating foreign law enforcement agency or other authority. In the event foreign prosecution is conducted, the Legal Attache should follow the prosecution and attempt to secure trial transcripts.

(9) The Legal Attache, in consultation with the USDS, should obtain any objections to extradition to the United States should the host government indicate an unwillingness to prosecute identified subjects. This development, should it occur, must be immediately reported to FBIHQ.

EFFECTIVE: 01/18/91

| 262-8.2 |Office of Origin|Responsibilities

(1) Upon receipt of information from Legal Attache involving violations of aforementioned statute, |the office of origin|will immediately establish contact with Counterterrorism Section (CTS), Criminal Investigative Division (CID), FBIHQ.

(2) In cases where U.S. nationals have been murdered, |the office of origin|should obtain all background information regarding each victim and alert the appropriate FBI field office once an address is determined for the next of kin. (While the USDS has the responsibility for notifying the next of kin, a release in order to do the autopsy must be obtained from the next of kin.) The appropriate FBI field office, through contact with CTS, CID, FBIHQ, is to ensure the next of kin has been notified by USDS of circumstances surrounding death before attempting to obtain such release. If the next of kin refuses to authorize an autopsy, FBIHQ must be notified immediately. The field office is to exercise the utmost sensitivity in requesting an autopsy.

(3) |The office of origin|will furnish FBIHQ a summary of available facts concerning the incident as soon as possible to ensure

that appropriate coordination is made by FBIHQ with other affected agencies.

EFFECTIVE: 01/18/91

||262-8.3 FBIHQ Responsibilities

(1) FBIHQ, will determine from DOJ whether the Attorney General has certified that the offense was intended to coerce, intimidate, or retaliate against a government or civilian population in accordance with ODSAA.

(2) Upon certification by the Attorney General, FBIHQ will ensure that the USDS is notified of the above and request that the appropriate U.S. Ambassador be advised of FBI jurisdiction and determine whether host country is willing to permit an FBI investigative team in the country.

(3) FBIHQ will consider activating the Strategic Information Operations Center (SIOC) and advise all field offices and Legats by teletype of the opening of the SIOC.

(4) FBIHQ will obtain background information from Legat concerned, set the number of FBI personnel who will participate in the debriefing of hostages, coordinate FBI Forensic Team responsibilities and ensure appropriate travel orders are issued.

(5) FBIHQ Laboratory Division will maintain a list of language proficient Special Agents/support personnel and will determine whether this terrorist event requires particular language skills, placing such personnel on standby for possible overseas travel. In addition, FBIHQ is to ensure that appropriate passports, visas, shots, etc., are ready so that deployment of such personnel can be done rapidly.

(6) In a case when property of a U.S. corporation is involved, FBIHQ will ensure, through appropriate FBI field offices, that the corporate owners of the property are to be personally notified of the incident relating to their property. Further, corporate officials will be advised that their cooperation in the investigation is expected.

(7) FBIHQ will contact Office of International Affairs (OIA), DOJ, in order to review the United States/country of incident

extradition treaty.

EFFECTIVE: 07/14/88

262-9 OFFICE OF ORIGIN

Office of origin (OO) will be divided among the Washington Metropolitan Field Office (WMFO), the Honolulu Office and the Miami Office for all OHAHT investigations. WMFO will assume OO when the offense occurs in Europe, including Turkey, the Middle East, Africa or Canada. The Honolulu Office will assume OO when the offense occurs in Asia (excluding the Middle East) or Australia and Oceania. The Miami Office will assume OO when the offense occurs in North America (excluding Canada) or South America.

EFFECTIVE: 01/18/91

262-10 CHARACTER

The character of this violation is Overseas Homicide/Attempted Homicide - International Terrorism (OHAHT).

EFFECTIVE: 01/18/91

# SECTION 263. OFFICE OF PROFESSIONAL RESPONSIBILITY MATTER

## 263-1 BACKGROUND (See MIOG, Part I, 62-1.5.)

(1) The Office of Professional Responsibility (OPR) was established in the Inspection Division in October, 1976, in order to bring about a greater awareness of professional responsibility throughout the FBI and to seek a more definitive and uniform policy in our administration of disciplinary personnel matters. OPR has three basic functions: (1) supervise and/or investigate all allegations of criminality and serious misconduct on the part of FBI employees; (2) maintain liaison with the Office of Professional Responsibility, Department of Justice (OPR/DOJ); and, (3) monitor disciplinary action taken concerning all employees of the FBI.

(2) It is OPR's goal to ensure that all such allegations against FBI employees are promptly, objectively, and thoroughly investigated and reported to the Personnel Division (PD) in a timely fashion for their consideration and appropriate action. The maintaining of the integrity of the FBI as an institution is paramount while conducting these mandated responsibilities. The rights of our employees, however, are to be similarly guarded.

EFFECTIVE: 04/21/94

## 263-2 NOTIFICATION OF FBIHQ UPON RECEIPT OF ALLEGATIONS OF CRIMINALITY OR SERIOUS MISCONDUCT

(1) As is set forth in Part I, Section 13 of the Manual of Administrative Operations and Procedures (MAOP), all allegations of employee misconduct must be reported to the Administrative Summary Unit (ASU), PD. Allegations of criminality or serious misconduct, however, must be reported simultaneously to the FBI's OPR. OPR supervises and/or investigates all allegations of criminality or serious misconduct on the part of FBI employees. Judicial criticism of an Agent's conduct in findings of fact, opinions, or court orders, whether oral or written, is to be considered an allegation of serious misconduct and reported to OPR as set forth below.

(2) When an allegation is received concerning criminality or serious misconduct, the appropriate Assistant Director, SAC, or Legal Attache, must advise OPR of the allegation, preferably by telephone. OPR will, in turn, advise |ASU/PD.| A confirming airtel, with a copy designated for the |ASU/PD,| should be directed in a sealed envelope to FBIHQ, Attention: OPR. OPR will determine and advise who will conduct the investigation. In those matters involving nonserious misconduct or performance-related deficiencies, in all likelihood, the SAC will be advised to handle those matters directly with the |ASU/PD.| In most cases, the Assistant Directors, SACs, or Legal Attaches will personally conduct the necessary investigation of OPR matters under the supervision and monitoring of OPR. Representatives of OPR normally investigate only those allegations involving FBIHQ officials, SACs, ASACs, and Legal Attaches, and sometimes FBIHQ and Field Supervisors, or when circumstances of a particular matter dictate.

(3) Timeliness of reporting and resolution of OPR matters are extremely important. It is imperative that upon receipt of an allegation of criminality or serious misconduct against an FBI employee, that OPR be advised promptly in order that appropriate instructions may be given. There should be no delay in contacting OPR while attempting to "round out" an allegation of possible criminality or serious misconduct.

(4) If an allegation of misconduct within the responsibility of OPR arises out of a substantive case (pending or closed), the matter will be coordinated closely between OPR and the FBIHQ Division which has overall responsibility for the substantive matter. FBIHQ Divisions should immediately inform OPR of allegations of possible criminality or serious misconduct which come to their attention and forward that portion of the investigation to OPR for further processing. The allegations arising from a substantive case will be carried separately under the Office of Professional Responsibility Matter caption and handled as a separate "263" classification investigation so that the substantive investigation and/or prosecution is not hindered.

(5) The following is a list of items which for the most part are considered OPR matters. They are furnished for information and are not considered all inclusive. Any question of whether the matter should be handled by OPR should be resolved by contact with OPR:

Abuse of authority
Arrest by local authorities (or subject of investigation by local authorities)

Civil rights violations
Conflict of interest
Driving While Intoxicated (both Bureau cars and personally owned automobiles)
Failure to advise the Bureau of contacts with law enforcement agencies
False statements during applicant processing
Falsification of documents
False reporting
Franking privilege violations
Fraud Against the Government
Improper association/relationship with criminal element
Improper association with informants
Judicial criticism
Narcotics matters
Outside employment
Retaliation matters
Sexual offenses
Subject of a Federal criminal investigation
Theft
Unauthorized disclosure of information
Unauthorized use of a Bureau vehicle
Unauthorized passenger in a Bureau vehicle
Unprofessional conduct
Whistleblower matters

(6) Other infractions, such as lost badges or minor personal misconduct, will continue to be handled by the PD. These matters are well defined and should continue to be handled as in the past. Any question as to whether a matter is or is not within the responsibility of OPR must be referred to OPR for a determination in this regard.

EFFECTIVE: 04/21/94

263-3 INVESTIGATION (See MAOP, Part I, 13-3.)

(1) Investigation necessary to develop complete, essential facts regarding any allegation against Bureau employees must be instituted promptly and every logical lead which will establish the true facts should be completely investigated unless such action might prejudice pending investigations or prosecutions, in which event FBIHQ will weigh the facts along with the recommendation of the Division Head.

(2) The record of the inquiry shall include the initial allegation; the investigative results; aggravating or mitigating circumstances; statement of specific charge(s); and the employee's answer(s) including defenses to the specific charge(s), if any.

(3) SACs should ensure the objectivity in personnel investigations conducted by field offices by not assigning supervisory personnel to them who have a direct working relationship with the employee(s) under investigation. OPR is likewise alert to this possible conflict of interest and will discuss this with the SACs when cases are initially reported to OPR.

(4) Requests to conduct audits of the computer systems activities of employees who are suspected of misconduct or improper performance of duty will be handled only with prior notification to FBIHQ. The term audit refers both to review and/or evaluation of prior transactions or activities of a user and procedures designed to monitor the ongoing activities of a user. The proper form for such a request is a formal written communication to FBIHQ with a request directed to the Information Resources Division's (IRD), Investigative Automation Support Section (IASS), to conduct the audit. In exigent circumstances, which dictate the need for immediate institution of an audit, requests may be made telephonically to OPR and subsequently confirmed in writing. In instances where telephonic requests are authorized, the level of authority is at the ASAC level or above in the field offices and at the Section Chief level or above at FBIHQ, with the exception of requests emanating from OPR. Telephonic requests for user activities audits made by OPR will be authorized at the Supervisory Special Agent level. (See MAOP, Part I, 13-3 (3).)

(5) Approval to conduct the audits will be made at the Section Chief level in IASS, based on the technical feasibility and resource constraints. If the audit cannot be conducted or if additional information is needed to formulate the audit, IASS will contact the requestor. The results of each audit conducted will be

reported on an FD-302 and disseminated to OPR and the requestor, should it be different from OPR. The original FD-302 will be forwarded to the office of origin. In those instances where exigent circumstances dictate that the results of the audit be telephonically disseminated, the results will be disseminated by |IRD| to OPR and to the requestor, should it be different from OPR, and the telephonic response subsequently confirmed in writing to OPR and the requestor. |(See MAOP, Part I, 13-3 (4).)|

EFFECTIVE: 06/01/94

263-4 INTERVIEWS OF EMPLOYEES

(1) Interviews of employees involved in allegations of criminality or serious misconduct should be conducted at the earliest logical time and in a forthright manner following coordination with OPR. There should be no evasiveness on the part of the Bureau official conducting the interview.

(2) The employee should be fully and specifically advised of the allegations which have been made against him/her in order that he/she may have an opportunity to fully answer and respond to them. The employee must be entirely frank and cooperative in answering inquiries of an administrative nature. If allegations are possibly criminal in nature, the employee has the right to seek counsel in the same vein as any other individual.

(3) Such interviews must be complete and thorough with all pertinent information obtained and recorded so that all phases of the allegations may be resolved. The interviews must not be unduly protracted and should be held to a reasonable length by proper preparation and recognition of the purpose of the interviews.

(4) The inquiry shall not be complete until the specific allegations which may justify disciplinary action are made known to the employee who may be disciplined and the employee is afforded reasonable time to answer the specific allegations. The employee's answers, explanations, defenses, etc., should be recorded in the form of a signed, sworn statement which should specifically include the allegations made against the employee in an introductory paragraph. The statement is to be prepared following an in-depth interview under oath of the employee by the Division Head or designated supervisory representative. The employee is not merely to be asked to give a

written response to the allegations, but is to be interviewed in an interrogatory fashion, and a signed, sworn statement prepared from the results by the interviewing official. Since the statement represents that which the employee is willing to sign and swear to, he/she retains the right to make corrections or changes before doing so. If those changes or corrections differ materially from what the employee stated during the interview, that fact and the nature of the statements should be separately recorded. The employee should be sworn prior to the interview in order that the information furnished during the interview will have been under oath. Should there be any question on the part of the interviewing official as to whether a particular allegation (set of facts) might justify disciplinary action, he/she should contact OPR in order to resolve this prior to the interview so the employee will be ensured of an opportunity to appropriately respond.

(5) The results of interviews of nonsubject, "witness" FBI employees in OPR matters should also be recorded in the form of signed, sworn statements. If there is some reason for not doing so, this should be coordinated with OPR/Inspection Division.

(6) When interviewing employees during administrative inquiries to solicit information about themselves or about their own activities, the employee should be provided the Privacy Act notice described in MIOG, Part I, 190-5(2), explaining the purpose of the inquiry and how the information will be used.

(7) When interviewing employees, or others, to solicit information about the subject of an administrative inquiry, the person interviewed as a source should be provided, if appropriate and necessary, the opportunity to request an express promise of confidentiality, as described in MIOG, Part I, 190-7, and SAC Memorandum 51-77(C), dated 11/15/77, in order to protect the source's identity should the subject of the inquiry submit a Privacy Act request for access to records of the inquiry. The source should be cautioned that if a formal adverse personnel action is taken against the subject of the inquiry pursuant to Chapter 75 of the Civil Service Reform Act, the information furnished, along with the source's identity, must, by law, be provided to the subject, if any information provided in that statement is used in whole or in part to support that personnel action. In addition, pursuant to certain administrative inquiries and possible judicial proceedings, it may be necessary to furnish the source's identity if any information provided in the source's statement is used in whole or in part to support a personnel action. The principles discussed in 263-5, infra, are also applicable to an interview of an employee regarding the actions of others, to the

extent such answers might reveal criminal misconduct on the part of the employee being interviewed.

EFFECTIVE: 03/26/90

263-5 ADMINISTRATIVE OR CRIMINAL PROCEEDINGS - USE OF INTERVIEW FORMS | (See MIOG, Part I, 263-4 (7); MAOP, Part I, 13-6.) |

(1) Prior to the interview of an employee against whom allegations of criminal misconduct have been leveled, a decision must be made as to whether the goal of the interview is to obtain a statement admissible in subsequent criminal proceedings or whether the goal is to compel the employee to make a full statement of the facts in order to ascertain what administrative action, if any, is appropriate. This decision is to be made by OPR in coordination with the OPR, DOJ.

(2) To ensure that employees being interviewed are fully and consistently aware of their rights and obligations, two forms have been adopted for use in such interviews. The Office of Professional Responsibility, DOJ, has endorsed the use of these forms. These forms are only to be utilized during OFFICIAL inquiries and only when authorized by OPR.

(3) Neither of these two forms (FD-644 nor FD-645) which are described below are to be routinely used during the investigation of a shooting incident. They will be used only in those shooting inquiries when instructed to do so by FBIHQ as set forth in MIOG, | Part II, Section | 12-11.7. |

The decision as to which form will be used in a particular inquiry will be made by OPR, FBIHQ, on a case-by-case basis, in accordance with the principles set forth below. For your information, there are certain prosecutive guidelines which have been agreed to by OPR, DOJ. The factual situation of any particular allegation will be considered by OPR in line with those prosecutive guidelines.

EFFECTIVE: 10/17/95

||263-5.1 Criminal Proceeding Contemplated or Possible

(1) Form FD-644 captioned "Warning and Assurance to Employee Requested to Provide Information on a Voluntary Basis," is to be utilized in situations where an employee is provided an opportunity to voluntarily respond to questions concerning allegations of job-related misconduct which have the potential for criminal prosecution, but wherein the employee is not being compelled to answer questions or provide a statement. Use of this form should assure that any statements obtained will be freely and voluntarily given and, hence, admissible in any future criminal proceeding.

(2) Full Miranda warnings will be given to employees only in situations where the employee to be interviewed is in custody or is significantly deprived of his/her freedom of action, an arrest is clearly intended at the conclusion of the interview, or whether in custody or not, the employee being interviewed has previously been arrested or formally charged and prosecution is pending on a Federal offense and the questioning concerns that offense or a related Federal offense.

(3) Whenever Form FD-644 is utilized, an interview log should be prepared in accordance with the Legal Handbook for Special Agents, Section 7-9.|

EFFECTIVE: 10/18/88

||263-5.2 Inquiry Solely for Administrative Purposes

(1) In a situation where the allegation, if true, has the potential for criminal prosecution, but a decision has been made not to seek an admissible statement (but rather, to compel the employee to fully and candidly answer all questions concerning the alleged incident), Form FD-645, captioned "Warning and Assurance to Employee Required to Provide Information," should be used. However, prior to the use of this form in any instance where the allegation, if true, would have potential for Federal criminal prosecution of the employee to be interviewed, OPR/Inspection Division must present the facts of the case to OPR/DOJ and obtain an initial opinion that the matter in question should be handled administratively rather than criminally. This is necessary because any incriminating statement obtained after use of Form FD-645 will not be admissible in a criminal prosecution of the employee.

(2) In a situation where the allegation, if true, has potential for non-Federal prosecution, and a decision has been made by FBIHQ to compel full answers from the employee regarding the matter under investigation, Form FD-645 should be used.

(3) In all other instances where an employee is being interviewed in connection with an official administrative inquiry, Form FD-645 should be used.

(4) There is no Sixth Amendment right to counsel in purely administrative interviews. Therefore, even if the employee specifically requests to have an attorney present during the course of the interview, the Bureau is not legally obliged to agree to this condition. Any administrative decision to allow the presence of counsel during an administrative interview is to be made by OPR, FBIHQ.

(5) An interview log is not required when Form FD-645 is utilized. Those conducting such administrative interviews of employees should be alert, however, to circumstances where good judgment might warrant preparation of an interview log; for example, in those interviews of a particularly sensitive nature or in those concerning serious misconduct involving veterans which may ultimately be heard before a Merit Systems Protection Board.

EFFECTIVE: 10/18/88

263-6 POLYGRAPH EXAMINATIONS OF BUREAU EMPLOYEES (See MAOP, Part I, 13-4.1.)

(1) All polygraph examinations of FBI employees and those who have made allegations against FBI employees must be approved by the Assistant Director, Inspection Division, or another person designated by the Director. In the case of polygraph examinations requested pursuant to a security clearance adjudication, the Director has delegated approval authority to the Assistant Director, National Security Division.

(2) Polygraph examinations of employees will be administered away from their own office of assignment. This procedure will help protect the confidentiality of the investigation/inquiry and lessen the outside pressure on the employee which could be associated with an examination conducted with knowledge of an employee's friends

and associates.

(3) Polygraph examinations of Bureau employees are to be administered by an FBIHQ examiner. In the event an FBIHQ examiner is not available, the examination will be conducted by an examiner designated by the Polygraph Unit, FBIHQ.

See MIOG, Part II, 13-22.13.1, 13-22.13.2, 13-22.13.3, and 13-22.14 for additional instructions and information regarding polygraph examinations of employees who are subjects of a criminal investigation or administrative inquiry.

EFFECTIVE: 07/19/95

| 263-7 REPORTING | (See MAOP, Part I, 13-7 & II, 2-3.3 (1).) |

(1) In most instances, after OPR has been initially notified of the allegation, it will be satisfactory for the responsible division head to report the facts pertaining to the serious misconduct or criminality by airtel setting forth a concise statement of the situation together with supporting documentation and statements. In all cases, whether or not it is believed administrative action is necessary, a statement that administrative action is, or is not, recommended must be made.

(2) These cases should not be opened in the Field Office Information Management System (FOIMS) prior to obtaining Bureau approval to open the investigation. A separate file should be opened and indexed under a "263" classification for each OPR investigation and the file should be maintained in the SAC's safe. This file number should be included on all communications between field offices and OPR. Such communications, when directed to the SAC, should be to his/her personal attention and should be enclosed in sealed envelopes when submitted to FBIHQ, Attention: OPR. Proper names of individuals in OPR cases should not be entered in the title field in the case management system of FOIMS. The title field should contain the words "SEE SAC" only. The Index Driven Case Title (IDCT) software will automatically insert the words "SEE SAC" during the data input of the index record. Keystroking the letter "S" in the "Special" field on the index record will generate "SEE SAC" on the first line of the title in the case application. It should be noted that the file number will not be displayed in the general indices of the field

office. OPR cases are to be opened in FOIMS as auxiliary office (AO) cases utilizing the FBIHQ file number as the Universal Case File Number. These cases should be opened with a pending status, not as "DEAD" or "ADM" status. Upon completion of the investigation, the status should be modified to RUC.

(3) Copies of the allegations and subsequent investigation should not be placed in the employee's field office or FBIHQ personnel file. Only if some form of administrative action is taken will there be any need to address the allegation in the employee's personnel file. This is satisfactorily handled by a designated copy of the approved justification memorandum and/or addendum(s) being placed in the employee's personnel file at FBIHQ as well as copies of the outgoing communication to the employee being placed in both the field office and FBIHQ personnel files.

(4) OPR will advise SACs and Assistant Directors when the results of OPR investigations have been reviewed by OPR and referred to |ASU/PD| for appropriate action.

EFFECTIVE: 04/21/94

263-7.1 Investigative Reports

(1) The results of most OPR investigations may be submitted by cover airtel to OPR. In those matters, however, involving more complicated situations or matters involving criminality which may need to be discussed further with the Department of Justice, they should be submitted to FBIHQ by investigative report which should be thorough, precise, and to the point. Any question concerning whether or not to submit an investigative report should be resolved by consulting with OPR.

(2) Synopses of OPR matter investigative reports should be complete to include all allegations, the results of the investigation, and the subject employee's responses to these allegations. Consideration should be given to including a table of contents in these investigative reports.

(3) Three copies of the investigative report (four copies if the matter involves a substantive case) should be submitted by cover airtel in a sealed envelope to FBIHQ, Attention: OPR/Inspection Division. The cover airtel should contain the SAC's observations and

comments, mitigating or aggravating circumstances, as well as the SAC's recommendations for administrative action.

(4) FBIHQ is the office of origin in OPR matter investigations. Upon completion of an investigation, originals of signed, sworn statements, Forms FD-644 and FD-645, etc., should be furnished to OPR.

EFFECTIVE: 04/19/91

263-8 CIVIL RIGHTS ALLEGATIONS AGAINST FBI PERSONNEL

Upon receipt of a complaint involving civil rights allegations against FBI personnel, the following procedures are to be followed:

(1) Advise the Civil Rights Unit (CRU), CID, and OPR by telephone followed by appropriate communications so that FBIHQ may furnish appropriate guidance. The CRU will coordinate with OPR and other FBIHQ components and advise the SAC concerning the proper handling of the matter.

(2) If a civil rights complaint arises during an administrative inquiry, the pertinent administrative inquiry relating only to the civil rights allegation must stop in order to resolve any criminal violations. That portion of the administrative inquiry may not resume until authorized by FBIHQ.

(3) OPR and CRU/CID will coordinate the presentation of the facts of the allegation to OPR/DOJ and the Civil Rights Division (CRD), DOJ, to determine if a criminal investigation is warranted. If no criminal investigation is warranted, the matter will be administratively handled by OPR. If the CRD/DOJ requests a criminal civil rights investigation, the CRU/CID will advise the SAC to initiate an investigation which should be reported to FBIHQ pursuant to Part I, Section 282-3.1 of the MIOG, unless advised to the contrary by FBIHQ.

EFFECTIVE: 01/31/94

263-9 DEPARTMENT OF JUSTICE OFFICE OF PROFESSIONAL RESPONSIBILITY

See MAOP, Part I, Section 1-23.

EFFECTIVE: 09/20/89

# SECTION 264. COMPUTER FRAUD AND ABUSE

## 264-1 BACKGROUND

(1) On October 12, 1984, the President signed into law the "Comprehensive Crime Control Act of 1984." Included in the passage of this Act was "Fraud and Related Activity in Connection with Computers," Title 18, USC, Section 1030. The creation of this statute was an attempt by Congress to address unauthorized access or use of computers. Jurisdiction for investigating violations of this statute has been governed by |Memoranda| of Understanding (MOU) between the Department of the Treasury and the Department of Justice. |An|MOU dated August 23, 1989, supersedes an MOU dated August 29, 1985, |and| outlines the jurisdiction of the FBI and the U.S. Secret Service |(USSS) in these matters.|

(2) On October 16, 1986, the "Computer Fraud and Abuse Act of 1986" (Public Law 99-474) and on October 21, 1986, the "Electronic Communications Privacy Act of 1986" (Public Law 99-508) were signed into law by the President. The Computer Fraud and Abuse Act of 1986 expanded Title 18, USC, Section 1030, unauthorized access or use of "Federal interest" computers (with intent to harm the U.S. Government, by obtaining classified or private financial information; modifying, destroying, or disclosing information; preventing use of the computer by others; and affecting computer operations), by adding fraudulent access to obtain property of value, trafficking in passwords with intent to defraud, and damage to certain stored information. Jurisdiction for investigating |these| violations is set out in |the 8/23/89 MOU (see 264-3).|

(3) Congress also enhanced individual and corporate protection against computer crime by enacting the Electronic Communications Privacy Act of 1986. Title II of this act |amended| Title 18 of the |USC| by adding Section 2701. This statute makes it a Federal offense to, without authorization, access or disclose the contents of a "stored electronic communication."

|(4) On October 1, 1990, the Economic Crimes Subprogram (ECS) of the White Collar Crimes (WCC) Program was formed to address all economic crimes except financial institution fraud. Computer Fraud and Abuse (CFA) matters are within the ECS and are managed at FBIHQ by the Economics Crime Unit (ECU), White Collar Crimes Section (WCCS), Criminal Investigative Division (CID).|

EFFECTIVE: 12/10/91

||264-2 |STATUTES, PENALTIES AND DEFINITIONS|

EFFECTIVE: 12/10/91

||264-2.1 Section 1030. Fraud and Related Activity in Connection with Computers|

| |(1)| Whoever knowingly accesses a computer without authorization or exceeds authorized access, and by means of such conduct obtains information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in paragraph r. of section 11 of the Atomic Energy Act of 1954, with the intent or reason to believe that such information so obtained is to be used to the injury of the United States, or to the advantage of any foreign nation.

||The punishment for an offense of this section is a fine or imprisonment for not more than ten years, or both, for the first offense under this section. The punishment for multiple offenses of this section is a fine or punishment for not more than 20 years, or both.|

| |(2) Whoever|intentionally accesses a computer without authorization, or exceeds authorized access, and thereby obtains information contained in a financial record of a financial institution, or card issuer as defined in section 1602 (n) of Title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act|(Title|15,|USC, Section|1681, et seq.).

||The punishment for an offense of this section is a fine or imprisonment for not more than one year, or both, for the first offense or attempted offense under this section. The punishment for multiple offenses of this section is a fine or imprisonment for not more than ten years, or both.|

| |(3) Whoever|intentionally, without authorization to

access any computer of a department or agency of the United States, accesses such a computer of that department or agency that is exclusively for the use of the Government of the United States or, in the case of a computer not exclusively for such use, is used by or for the Government of the United States and such conduct affects the use of the Government's operation of such computer.

The punishment for an offense of this section is a fine or imprisonment for not more than one year, or both, for the first offense or attempted offense under this section. The punishment for multiple offenses of this section is a fine or imprisonment for not more than ten years, or both.

(4) Whoever knowingly and with intent to defraud, accesses a Federal Interest computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer.

The punishment for an offense of this section is a fine or imprisonment for not more than five years, or both, for the first offense or attempted offense under this section. The punishment for multiple offenses of this section is a fine or imprisonment for not more than ten years, or both.

(5) Whoever intentionally accesses a Federal Interest computer without authorization, and by means of one or more instances of such conduct alters, damages, or destroys information in any such Federal Interest computer, or prevents authorized use of any such computer or information, and thereby-

(a) causes loss to one or more others of a value aggregating $1,000 or more during any one-year period; or

(b) modifies or impairs, or potentially modifies or impairs, the medical examination, medical diagnosis, medical treatment, or medical care of one or more individuals.

The punishment for an offense of this section is a fine or imprisonment for not more than five years, or both, for the first offense or attempted offense under this section. The punishment for multiple offenses of this section is a fine or imprisonment for not more than ten years, or both.

(6) Whoever knowingly and with intent to defraud traffics (as defined in Section 1029) in any password or similar information

through which a computer may be accessed without authorization, if-

|(a)| such trafficking affects interstate or foreign commerce; or

|(b)| such computer is used by or for the Government of the United States.

|The punishment for an offense of this section is a fine or imprisonment for not more than one year, or both, for the first offense or attempted offense under this section. The punishment for multiple offenses of this section is a fine or imprisonment for not more than ten years, or both.|

EFFECTIVE: 12/10/91

||264-2.2| Definitions|as used in Section 1030|

|(1) The term "access" refers to storing data on and retrieving data from a disk or other peripheral device.|

|(2)| The term "computer" means an electronic, magnetic, optical, electrochemical, or other high-speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand-held calculator, or other similar device.

|(3)| The term "Federal interest computer" means a computer-

|(a)| exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects the use of the financial institution's operation or the Government's operation of such computer; or

|(b)| which is one of two or more computers used in committing the offense, not all of which are located in the same State.

|(4)| The term "State" includes the District of Columbia, the Commonwealth of Puerto Rico, and any other possession or territory of the United States.

|(5)| The term "financial institution" means-

|(a)| an institution with deposits insured by the Federal Deposit Insurance Corporation;

|(b)| the Federal Reserve or a member of the Federal Reserve including any Federal Reserve Bank;

|(c)| a credit union with accounts insured by the National Credit Union Administration;

|(d)| a member of the Federal home loan bank system and any home loan bank;

|(e)| any institution of the Farm Credit System under the Farm Credit Act of 1971;

|(f)| a broker-dealer registered with the Securities and Exchange Commission pursuant to section 15 of the Securities Exchange Act of 1934; and

|(g)| the Securities Investor Protection Corporation.

|(6)| The term "financial record" means information derived from any record held by a financial institution pertaining to a customer's relationship with the financial institution.

|(7)| The term "exceeds authorized access" means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accessor is not entitled so to obtain or alter.

|(8)| The term "department of the United States" means the legislative or judicial branch of the Government or one of the executive departments enumerated in section 101 of title 5.

EFFECTIVE: 12/10/91

264-2.3 Section 2701. Unlawful Access to Stored Communications

(1) Whoever intentionally accesses, without authorization, a facility through which an electronic communication is provided.

The punishment for an offense of this section is a fine of not more than $250,000 or imprisonment for not more than one year, or both in the case of a first offense under this subparagraph. The punishment for subsequent offenses of this section is a fine or imprisonment for not more than two years, or both.

(2) Whoever intentionally exceeds an authorization to access that facility, and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system.

The punishment for an offense of this section is a fine of not more than $5,000 or imprisonment for not more than six months, or both, in any other cases.

(3) This section does not apply with respect to conduct authorized-

(a) by the person or entity providing a wire or electronic communications service;

(b) by a user of that service with respect to a communication of, or intended for, that user; or

(c) in section 2703 (Requests for Governmental Access), 2704 (Backup Presentation), or 2518 (Procedure for Interception of Electronic Communications) of Title 18.

EFFECTIVE: 12/10/91

264-2.4 Definitions for Section 2701 are found in Title 18, USC, Section 2510 (See MIOG, Part I, 139-1.1.)

(1) "Electronic communication" means any transfer of signs, signals, writings, images, sounds, data or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but does not include--

(a) any wire or oral communication;

(b) any communication made through a tone-only paging device;

(c) any communication from a tracking device (as defined in section 3117 of Title 18);

(2) "User" means any person or entity who--

(a) uses an electronic communication service; and

(b) is duly authorized by the provider of such service to engage in such use;

(3) "Electronic communication system" means any wire, radio, electromagnetic, photooptical or photoelectronic facilities for the transmission of electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications;

(4) "Electronic communication service" means any service which provides to users thereof the ability to send or receive wire or electronic communications;

(5) "Electronic storage" means--

(a) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and

(b) any storage of such communication by an electronic communication service for purposes of backup protection of such communication.

EFFECTIVE: 12/21/94

264-2.5 Other Statutes which may be used in CFA investigations

EFFECTIVE: 12/10/91

264-2.5.1 Title 18, USC, Section 641 (Theft of Government Property)

This statute covers the theft of any record, voucher money, or thing of value of the United States. This statute has been used to prosecute Government officials, who use their position to obtain computerized information to sell.

"Whoever embezzles, steals, purloins, or knowingly converts to his use or the use of another, or without authority, sells, conveys or disposes of any record, voucher, money, or thing of value of the United States or of any department or agency thereof, ... or

"Whoever receives, conceals, or retains the same with intent to convert it to his use or gain, knowing it to have been embezzled, stolen, purloined or converted...shall be fined not more than $10,000 or imprisoned not more than ten years, or both...." (See MIOG, Part I, Section 52.)

EFFECTIVE: 12/10/91

264-2.5.2 Title 18, USC, Sections 793, 794 and 798 (Espionage)

(1) These statutes deal with gathering, transmitting, or losing defense information for the purpose of injuring the United States or helping any foreign nation. These statutes also deal with delivering defense information to aid foreign government and disclosure of classified information.

(2) Violators of these statutes should be fined not more than $10,000 or imprisoned not more than ten years, or both. (See FCI Manual, Part I, Section 65.)

EFFECTIVE: 12/10/91

264-2.5.3 Title 18, USC, Section 1343 (Wire Fraud) and Section 1341 (Mail Fraud)

The wire fraud statute and mail fraud statute have occasionally been used to prosecute computer criminals. To establish a violation of the wire fraud statute, the Government has to establish three elements beyond a reasonable doubt: i.e., a defendant (1) devised a scheme to defraud either the various networks or the computers on those networks, (2) intended to obtain money or property from them by false pretenses, representations, or promises; and, (3) that to execute the scheme, the defendant used or caused the use of interstate or international wire communication facilities in furtherance of the scheme. In the case of the mail fraud statute, the Government would have to show elements (1) and (2) and the use of the U.S. Postal Service in furtherance of the scheme.

The punishment for offenses under the fraud by wire and mail fraud statutes are a fine of not more than $1,000 or imprisonment not more than five years, or both. (See MIOG, Part I, Section 196 and MIOG, Part I, Section 36, respectively.)

EFFECTIVE: 12/10/91

264-2.5.4 Title 18, USC, Section 1362 (Malicious Mischief)

This statute punishes the willful interference with military communications systems.

The punishment for an offense of this statute is a fine of not more than $10,000 or imprisonment not more than ten years, or both.

EFFECTIVE: 12/10/91

264-2.5.5 Title 18, USC, Section 2314 (Interstate Transportation of Stolen Property)

This statute has been used with varying success to prosecute computer criminals. The Government has to show the interstate transportation of stolen property with a value in excess of $5,000.

The punishment for an offense of this statute is a fine of not more than $10,000 or imprisonment not more than ten years, or both. (See MIOG, Part I, Section 87.)

EFFECTIVE: 12/10/91

264-2.5.6 Title 17, USC, Section 506; Title 18, Sections 2318 and 2319 (Copyright Matters)

Generally, investigations in all copyright cases should be directed toward locating and identifying the producers, principal distributors, and publishers of unauthorized duplications of copyright products in order to eliminate the source of illicit productions.

The punishment for violations of these statutes is a maximum penalty of $250,000 and/or five years' imprisonment. (See MIOG, Part I, Section 28.)

EFFECTIVE: 12/10/91

264-2.5.7 State and Local Legislation as an Additional Tool

A number of the states in the United States have enacted specific legislation to address computer crimes. These violations should not be overlooked when investigating computer crimes.

EFFECTIVE: 12/10/91

||264-3| JURISDICTION

| |(1)| Title 18, USC, Section 1030(d) provides: "The United States Secret Service (USSS) shall, in addition to any other agency having such authority, have the authority to investigate offenses under this Section. Such authority of the United States Secret Service shall be exercised in accordance with an agreement which shall be entered into by the Secretary of the Treasury and the Attorney General."

On August 23, 1989, an amended agreement was entered into and it provides the following:

"4.a. The FBI shall have primary jurisdiction:

"(1) For matters which have traditionally been within its authority. These areas include such matters as organized crime, terrorism, and foreign counterintelligence.

"(2) For violations of Title 18, U.S. Code, Section 1030(a)(1) and (a)(3) which address the unauthorized access of computers used in national defense, foreign relations or any restricted data which may be used to the injury of the United States. However, when allegations involve unauthorized access of the White House complex computer systems or attempts at unauthorized access the USSS will maintain a presence and assist in the investigation.

"(3) For those criminal acts using a Federal-interest computer (as defined in Title 18, U.S. Code, Section 1030(e)(2)), that may be construed as violations of the Bank Fraud and Embezzlement, Fraud by Wire, or Bank Bribery Statutes where the FBI has traditionally had jurisdiction. The term bank is defined in various statutes as it relates to the specific offense (e.g., Title 18, U.S. Code, Sections 215, 1344, and 2113).

"(4) Except as noted in 4.b.(2) below, when a significant fraud against the Government has been committed by an employee of any Government agency. This is a matter that falls within the substantive jurisdiction of the FBI (Title 28, Section 535, U.S. Code), and has been articulated in Memoranda of Understanding between the FBI and Inspectors General of various agencies.

"b. The USSS shall have primary jurisdiction:

"(1) Except as noted in 4.a. (1), (2), (3), (4) above, for violations as outlined in Title 18, Section 1030 (a) (2),

occurring in a consumer reporting agency, as defined in the Fair Credit Reporting Act of 1978 (Title 15, Section 1681, U.S. Code), or a card issuer as defined in Title 15, Section 1602, U.S. Code, and as outlined in Title 18, Sections 1030(a)(3) and (a)(6), U.S. Code.

"(2) When the computer systems of the U.S. Treasury Department are the direct object of the violation and the allegations do not meet the criteria for referral to the Department of Justice set forth in the purpose section of this memorandum.

"c. The FBI and the USSS shall have concurrent jurisdiction:

"(1) Except as noted in 4.a. (1), (2), (3), (4) above, for fraudulent schemes as outlined in Title 18, Sections 1030 (a) (2), (a) (4), and (a) (5), U.S. Code, when such violations are perpetrated against a computer system of a financial institution as defined in Title 18, Sections 1030 (e) (4) (G) and (e) (4) (H).

"(2) Except as noted in 4.a. (1), (2), (3), (4) and 4.b. (1) and (2), above for violations as outlined in Title 18, U.S. Code, Section 1030 (a) (4), and (a) (5) when such violations involve other Federal-Interest computers (as defined in Title 18, U.S. Code, Section 1030 (e) (2) (B)."

|(2) Title 18, USC, Section 2701, provides that the Federal Bureau of Investigation shall have investigative authority for any violations of this statute.|

EFFECTIVE: 12/10/91

||264-4| POLICY

EFFECTIVE: 12/10/91

||264-4.1| Investigative Policy

|(1)| Based on the legislative history and the apparent intent of Congress to address instances of computer trespass, fraud and malicious damage, the FBI's primary investigative role will be those cases which have traditionally formed the basis for our investigative authority and wherein the criminal activity is sizeable and/or widespread. Matters involving national security, |crimes directed at|financial institutions, United States Government computers, |Federal Interest computers, and interstate|frauds or malicious damage will be the primary thrust of FBI investigations. Other matters within the statute, but not covered above, may be referred to|the USSS or|any law enforcement agency of a state, or political subdivision thereof|having jurisdiction.|

|(2) FBIHQ should be promptly notified, by telephone and/or teletype, of the initiation of major or otherwise significant CFA cases which may prompt news media (or other) inquiries to be directed to FBIHQ.

(3) Because of the broad scope of computer-related cases, the FBI is able to apply the substantive violations to the appropriate investigative situation. In instances where the primary direction of work pertains to violations other than CFA, field offices are directed to use the appropriate classification for those violations. The use of other statutes, in addition to CFA statutes, would create a more expansive and effective attack against violators of statutes. The use of other classifications in these situations will more appropriately identify the investigative program within which these individual cases will be managed.|

EFFECTIVE: 12/10/91

||264-4.2| Prosecutive Policy

EFFECTIVE: 12/10/91

||264-4.2.1 Title 18, USC, Section 1030|

(1) The focus of Federal criminal prosecutions will be against those who demonstrate a clear intent to enter, without authorization, computer files belonging to another. The unauthorized access must be the person's conscious objective; however, an unintentional initial contact coupled with access deliberately maintained may not be exempt from prosecution. Section 1030 deals with an "unauthorized access" concept of computer fraud rather than the use of a computer. The conduct prohibited is analogous to that of a trespass (breaking and entering) rather than using a computer in committing the offense.

(2) Allegations of criminal acts involving Federal Government computers require proof that the unauthorized access to, and the use or destruction of, the information affects the operation of the Government. A computer used part time by the Government may become the victim of a Federal crime if it can be shown that the unauthorized access was made at any time when the Federal Government was authorized to use it, or if the unauthorized use left some sort of message, etc., that impacted on the Federal Government when it resumed use of the computer. The phrase "obtain information" is broadly defined.

(3) Thefts of property through computer trespass which occur as part of the fraud scheme require that the use of the computer be directly related to the intended fraud and not merely related to it.

(4) The statute exempts from prosecution under Title 18, USC, Section 1030(a)(4), persons who exceed authorized use of a computer simply to use the computer for purposes to which the authorization does not extend (e.g., to do homework, play video games or if the only thing of value obtained was the use of the computer's time).

EFFECTIVE: 12/10/91

||264-4.2.2 Title 18, USC, Section 2701|

(1) Congressional intent in legislating Title 18, USC, Section 2701, was to protect the privacy of an electronic communication which is transmitted to a communications service, its storage on the behalf of the subscriber, and to ensure that such communication service be available only to the subscriber and others who may have authorized or legal access to it. Thus, privacy is protected either before the communication is transmitted to the recipient, or, if a copy of the message is kept, after it is delivered. The statute was designed to protect electronic communication through such methods as electronic mail and computer transmissions. It was generally recognized that the interruption of|communications|during the transmission stage is intrusive, and these communications are given protection by making it a Federal felony to unlawfully access.

(2) Electronic services covered by this statute include electronic mail service, voice mail, remote computing service, and other like communicating systems.

(3) This provision is intended to address unauthorized "computer hackers" and corporate spies who deliberately gain access to, and sometimes tamper with, electronic communications that are not available to the public. The provision is not intended to criminalize access to "electronic bulletin boards," which are generally open to the public so that interested persons may communicate on specific topics. Where communications are readily accessible to the public, the sender has (for purposes of Title 18, USC, Section 2701 (a)) extended an "authorization" to the public to access those communications. A communication is readily accessible if the telephone number of the system and other means of access are widely known, and if the person does not, in the course of gaining access, encounter any warnings, encryptions, password requests, or other indications of intended privacy. To access a communication on such a system is not a violation of the law.

EFFECTIVE: 12/10/91

264-5 INVESTIGATIVE PROCEDURES

In general, computer-related crimes are not unique, in many cases the facts and circumstances parallel the traditionally criminal mental and physical acts found in such crimes as trespass, embezzlement, theft, fraud, malicious damage, sabotage, and espionage. The investigative approach should comply with traditional case management techniques, while giving appropriate consideration to the unique vocabulary found in the computer industry. Once the language hurdle is overcome, the investigator has the ability to understand what has occurred. The following investigative procedures are suggested for consideration in the investigation of 264 matters and are not considered an all-inclusive list:

(1) All CFA evidence examinations are to be submitted to the FBI Laboratory for examination and data retrieval. All requests for FBIHQ on-site examination and data retrieval will be coordinated through the ECU, WCCS, CID.

(2) When the criminal complaint is from the owner/user of the equipment/data, those who are directly familiar with the victim computer's operation and/or equipment should be called upon, if appropriate, to provide the facts to prove the elements of the offense; explain the modus operandi; aid in gathering the evidence; identify the suspect(s); and assist in simplifying the facts and circumstances for an effective presentation to the jury.

(3) The common investigative steps in any computer-related criminal investigation should be: the initial, preliminary investigation; contact the United States Attorney for a prosecutive opinion; investigative planning; information gathering and analysis; interviewing and interrogation; appropriate technical review, if necessary; and computer examination and documentation for prosecution and court presentation(s).

(4) The preliminary investigative phase should ascertain as much about the allegation as possible. It should determine the nature of the allegation, the probable degree of technicality involved and potential subjects and witnesses. Additionally, Agents investigating those matters should become familiar with the area, people, procedures, processes, security, and equipment involved.

b2 b7E

(5) [redacted]

b2 b7E

b2
b7E

(6) [redacted]

(7) [redacted]

(8) [redacted]

(9) [redacted]

(10) Upon proper predication, surveillance of computer facilities should be used to determine users of the facilities.

(11) [redacted]

(12) [redacted]

(13) [redacted]

(14) Liaison contacts should be developed with local and state agencies investigating similar violations under state statutes. Should a preliminary inquiry not fall within the investigative policy of the FBI and/or the U.S. Attorney declines prosecution, the complainant should be directed to any other state or local law enforcement agency which has authority to conduct such investigations.

(15) Absent sensitive circumstances, instances of computer-related crimes in other Federal Government agencies should be coordinated with the appropriate investigative unit of that agency.

(16) Search warrants are often used in CFA matters. In executing a search warrant, care must be taken to limit the scope of the warrant to seize only evidence pertinent to the crimes under investigation.

EFFECTIVE: 12/10/91

||264-6| REPORTING REQUIREMENTS

|(1) All complaints involving CFA, regardless of classification or whether a case is opened, will be submitted to ECU, WCCS, CID, FBIHQ, by the Computer Fraud and Abuse Data Transmittal Form (FD-801). The submission of the CFA Data Transmittal Form for all complaints will allow FBIHQ to monitor the instances of CFA; fully identify the scope of the crime problem and crime trends; and seek resources as necessary to address these matters. If an investigation is opened as a CFA matter, a letterhead memorandum (LHM) (original and five copies) is to be submitted to FBIHQ and any affected auxiliary offices within 20 calendar days. The transmittal form will replace the transmittal airtel previously utilized in submission of LHMs to FBIHQ. The LHM is to include the field office, field office file number, date the investigation was opened, identified subject(s), predication, estimated loss, investigation conducted to date, the U.S. Attorney's initial prosecutive opinion, and contemplated investigation. The 20-day reporting requirement facilitates the coordination of multijurisdictional matters in a timely manner.

(2) Any investigation which is of a national interest or involves prominent individuals should be initially reported by priority communication, to include telephone, if necessary, followed by the LHM and CFA Data Transmittal Form (FD-801). Any major developments, use of innovative or sensitive investigative techniques, or unusual problems should also be promptly reported to FBIHQ.

(3) FBIHQ will disseminate information regarding the initiation of CFA investigations to the USSS. FBIHQ may also have reason to disseminate information regarding these matters to other

Federal agencies. Sensitive information (i.e., informant/cooperating witness identities, personnel information, undercover Agent identities) should be set forth in the administrative section of the CFA Data Transmittal Form (FD-801). If the need exists not to disseminate, field offices should advise FBIHQ.

(4) Two copies of prosecutive reports prepared in CFA matters should be furnished to FBIHQ.

EFFECTIVE: 12/10/91

||264-7| VENUE

Where the offense is committed, begun or completed.

EFFECTIVE: 12/10/91

264-8 CHARACTER - COMPUTER FRAUD AND ABUSE (CFA)

EFFECTIVE: 12/10/91

264-9 CLASSIFICATION (See MAOP, Part II, 3-1.1 & 3-1.2.)

The CFA classification is subdivided into three types of cases that are characterized by alpha designator. Alpha designators are as follows:

264A COMPUTER FRAUD AND ABUSE - IMPAIRMENT

This includes the modification of existing software on a computer or placing harmful software on a computer which then affects its normal operation.

264B COMPUTER FRAUD AND ABUSE - THEFT OF INFORMATION

Theft of information matters involve the taking of information that is protected for reasons of national defense; the taking or trafficking in passwords; the taking of financial records of a financial institution;

and taking anything of value.

264C COMPUTER FRAUD AND ABUSE - INTRUSION

Intrusion matters involve unauthorized use when it has not yet been determined that an impairment or theft has occurred.

EFFECTIVE: 10/18/95

264-10 CASE TITLE

Set forth below is an example of a case title for use in the CFA Data Transmittal Form (FD-801):

JOHN H. SMITH;
XYZ AGENCY - VICTIM;
COMPUTER FRAUD AND ABUSE - IMPAIRMENT;
OO: NEW YORK
(264A-NY-12345)

EFFECTIVE: 12/10/91

264-11 OFFICE OF ORIGIN

Office of Origin will be established in the manner set forth in MAOP, Part II, Section 10-16.2.

EFFECTIVE: 12/10/91

~~SECRET~~

Sensitive



SECTION 265. ACTS OF TERRORISM - INTERNATIONAL TERRORISTS

265-1 ACTS OF TERRORISM - INTERNATIONAL TERRORISTS

(1) This classification will include any investigation of a criminal act which involves an international terrorist. The investigative procedures will follow the same procedures detailed in the substantive offense under which the investigation is predicated. Alpha designators have been created to identify the investigative program under which the investigation should be classified.

(2) This classification was developed in order to focus on the criminal activity of the international terrorist. This effort does not diminish the importance of intelligence investigations or collection, but emphasizes the criminal nature of terrorism. Therefore, once information is developed in an investigation conducted under the Foreign Counterintelligence Guidelines that evidence exists of criminal activity, the criminal investigation under this classification, with appropriate alpha designator, is to be opened.



EFFECTIVE: 04/26/94

| 265-2 ALPHA DESIGNATORS | (See MIOG, Part I, 265-3.) |

Set forth below are the alpha designators which are applicable to the 265 classification. A case shall be identified with an alpha designator in accordance with the investigative program or subprogram to which the substantive offense would generally belong.

265A - Violent Crimes - Predicate Offense (i.e., kidnaping, bank robbery, etc.)

265B - Organized Crime - Predicate Offense (i.e., racketeering enterprise investigation, etc.)

265C - White-Collar Crime - Predicate Offense (i.e., FIF, etc.)

265D - Government Reservation Crimes - Predicate Offense

(i.e., CGR, TGP, etc.)

265E - Fugitive - Predicate Offense (i.e., bond default, etc.)

265F - Interstate Theft - Predicate Offense (i.e., TFIS, etc.)

265G - Drug Trafficking

EFFECTIVE: 04/26/94

265-3 INVESTIGATIVE POLICY AND PROCEDURES

[redacted] b1 b6

(2) It is most likely that the 265 classification will be applied to one of two possible scenarios.

[redacted] (S) b1

[redacted] b2 b7E

[redacted] b1 (S)

OPCA-20 (12-3-96)

XXXXXX
XXXXXX
XXXXXX

# FEDERAL BUREAU OF INVESTIGATION
## FOIPA
## DELETED PAGE INFORMATION SHEET

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

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

**Section 552**

☐ (b)(1)
☑ (b)(2)
☐ (b)(3)
_____
_____
_____
☐ (b)(4)
☐ (b)(5)
☐ (b)(6)
☐ (b)(7)(A)
☐ (b)(7)(B)
☐ (b)(7)(C)
☐ (b)(7)(D)
☑ (b)(7)(E)
☐ (b)(7)(F)
☐ (b)(8)
☐ (b)(9)

**Section 552a**

☐ (d)(5)
☐ (j)(2)
☐ (k)(1)
☐ (k)(2)
☐ (k)(3)
☐ (k)(4)
☐ (k)(5)
☐ (k)(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 1 Sec 265 p3

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

XXXXXX
XXXXXX
XXXXXX

FBI/DOJ

2. The policy guidance set forth under (a) above applies to this situation also.

(3) Upon initiation of a 265 investigation, a teletype must be expeditiously prepared and forwarded to the attention of the CTS, NSD.

(a) This communication must contain the predication for the criminal investigation including the specific facts which clearly establish the terrorism nexus.

EFFECTIVE: 04/26/94

265-4 CHARACTER - ACTS OF TERRORISM - INTERNATIONAL TERRORISTS (AOTIT)

EFFECTIVE: 04/26/94

SECTION 266. ACTS OF TERRORISM - DOMESTIC TERRORISTS

266-1 ACTS OF TERRORISM - DOMESTIC TERRORISTS (See Attorney General's Guidelines on General Crimes, Racketeering Enterprise and Domestic Security/Terrorism Investigations, Part II, Contained in MIOG, Introduction, 1-3.)

(1) This classification shall include any investigation of a criminal act which involves an individual or individuals affiliated with a domestic terrorist group. The investigative procedures shall follow the same procedures detailed in the substantive offense under which the investigation is predicated. Alpha designators have been created to identify the investigative program under which the investigation should be classified.

(2) The Act of Terrorism (AOT) classification was developed in order to focus upon the specific criminal activity of the domestic terrorist. If a specific, articulable criminal violation on the part of a person or persons affiliated with a domestic terrorist group is determined to have occurred, is occurring, or is about to occur, then a criminal investigation should be opened under this classification with appropriate alpha designator (see Section 266-2). An AOT investigation (266 case) may be initiated in conjunction with, or independent of, a criminal intelligence investigation (100 case).

(3) Section II of the Attorney General Guidelines (AGG) permits field offices to open general crimes investigations when facts or circumstances reasonably indicate that a federal crime has been, is being, or will be committed. Section III of the AGG permits the initiation of criminal investigations of Domestic Security/Terrorism (DS/T) groups when facts or circumstances reasonably indicate that "two or more persons are engaged in an enterprise for the purpose of furthering political or social goals wholly or in part through activities that involve force or violence and a violation of the criminal laws of the United States." (See MIOG, Introduction, 1-3.)

(4) Preliminary Inquiries

(a) Preliminary inquiries are not authorized under Section III of the AGG (criminal intelligence investigations/100 classification). Section I of the AGG states that preliminary inquiries shall be conducted pursuant to the General Crimes Guidelines

(Section II). There is no separate provision for the conduct of preliminary inquiries under the Criminal Intelligence Guidelines described by Section III.

(b) Preliminary inquiries authorized in the General Crimes Section are more limited in scope and purpose than the preliminary investigation formerly authorized under the 1976 Domestic Security Guidelines. However, they permit greater latitude in the use of certain investigative techniques, particularly where informants are involved. The only investigative techniques that are specifically prohibited during a preliminary inquiry are: [redacted] b7E [redacted] At the same time, the Guidelines caution that Agents should consider whether the information sought could be obtained by means which involve less intrusion into the subject's privacy. As an example, if a discreet inquiry to local law enforcement officials would produce the necessary information, it might be inappropriate to question neighbors.

(c) Subject to this general guidance on intrusiveness pertaining to preliminary inquiries, Agents require no special authorization to check FBI files, public records or sources, government records, utilize established informants or confidential sources, interview subjects, complainants or others having knowledge of the facts, or to conduct surveillance. Prior authorization of a Supervisory Agent is required before employers or co-workers may be interviewed, pretext interviews are conducted, or new informants are developed. Other more intrusive techniques, [redacted] b7E [redacted] may be employed only in compelling circumstances and when other investigative means are not likely to be successful. An informant would also fall in that category if he/she is used in a manner that involves a significant intrusion into one's private affairs. "Compelling circumstances" are circumstances requiring the use of techniques to determine the validity of information or allegations concerning possible serious criminal activities such as a threat to life or substantial property interest, the destruction or alteration of evidence, or the serious impairment or hindrance of an investigation.

(d) Preliminary inquiries may be authorized by field supervisors, but in all situations, the inquiry must be completed within 90 days after initiation of the first investigative steps, unless authorized by the Bureau. Subsequent authorizations for extensions are limited to 30-day periods, and will be based upon a written request from the field divisions, including a statement of reasons justifying further "inquiry" when there is no "reasonable

indication" which would allow a full investigation under this classification.

(e) In order to ensure compliance with the Attorney General Guidelines and to avoid duplication of investigative effort, each field office shall advise FBIHQ, in writing, within 10 work days of the opening of a preliminary inquiry, as well as within 10 work days of the closing of a preliminary inquiry.

(5) Criminal intelligence investigations of DS/T enterprises should be initiated and carried as 100 matters. Criminal intelligence information developed during the course of a 266, or other investigation, may be placed in a 100 file to which it relates. Conversely, criminal acts detected in a 100 criminal intelligence investigation may be "spun off" to a 266 general investigation or a PI. DS/T criminal intelligence investigations are similar in nature to a racketeering enterprise investigation (REI).

(a) During the course of a DS/T criminal intelligence investigation, specific articulable criminal violations may be identified which would reasonably indicate enforcement activity or court proceedings (e.g., arrest, discovery hearings, etc.) will occur. At that time, a general criminal investigation (266 case) should be opened to focus upon the specific criminal activity. The criminal intelligence investigation (100 case) would continue to focus on the entire enterprise, as the scope of the AOT case may be limited to a relatively small portion of the total activity of that enterprise.

(b) While it may be appropriate for all investigative results generated from an AOT (266) case to be placed in the corresponding 100 file, the converse is not true. Only those details in the 100 case which specifically pertain to the subjects of the AOT case should be placed in the 266 file.

(6) The correct identification of a criminal intelligence investigation in the 100 classification or a General Crimes Investigation as a 266 is important because it establishes the FBI's investigative focus.

(7) When a general crimes investigation is classified as a 266 matter, it focuses on an individual and his or her criminal conduct which may be incidentally related to that person's affiliation with a DS/T group. These 266 Act of Terrorism-Domestic Terrorism investigations may not necessarily involve the sensitive circumstances which are likely to be involved in an intelligence investigation of

the group itself. Criminal intelligence investigation of DS/T groups are conducted in order to obtain information regarding the nature and structure of the enterprises.

(8) In the past, general crimes investigations and preliminary inquiries have been conducted out of 100 (DS/T) classification files or subfiles. Because preliminary inquiries can only be conducted in general crimes investigations, they should be handled as 266 matters (Acts of Terrorism - Domestic Terrorism), not 100 matters.

EFFECTIVE: 06/23/97

| 266-2 ALPHA DESIGNATORS |(See MIOG, Part I, 266-1.)|

Set forth below are the alpha designators which are applicable to the 266 classification. A case shall be identified with an alpha designator in accordance with the investigative program or subprogram to which the substantive offense would generally belong.

266A - Violent Crimes - Predicate Offense (i.e., ||kidnapping,|bank robbery, etc.)

266B - Organized Crime - Predicate Offense (i.e., racketeering enterprise investigation, etc.)

266C - White-Collar Crime - Predicate Offense (i.e., FIF, etc.)

266D - Government Reservation Crimes - Predicate Offense (i.e., CGR, TGP, etc.)

266E - Fugitive - Predicate Offense (i.e., bond default, etc.)

266F - Interstate Theft - Predicate Offense (i.e., TFIS, etc.)

266G - Drug Trafficking

EFFECTIVE: 06/23/97

266-3 INVESTIGATIVE OBJECTIVES AND PROCEDURES

(1) The objective of this classification is to direct investigative resources toward detection and prevention of a terrorist incident and the prosecution of individuals committing specific criminal acts.

(2) The investigative procedures utilized for a case conducted under these alpha designators will be in accordance with established guidelines for the substantive offense of that alpha designator, except that coordination of the investigation and results thereof will be reported to the Domestic Terrorism/Counterterrorism Planning Section, National Security Division (NSD). For example, an investigation conducted as a 266A case would follow procedures set forth under the Violent Crimes Subprogram except for the coordination and reporting aspects.

(3) In accordance with the AGG, preliminary inquiries (PI) may be initiated by FBI field offices without FBIHQ authority to determine the scope of a terrorist group's criminal activities. Initiation of a PI allows the FBI to conduct a measured review, contact, or observe individuals to determine if there is a "reasonable indication" of criminal activity, warranting a full DS/T investigation.

(4) PIs are to be completed within 90 days after the initiation of the first investigative step. Extension of a PI requires FBIHQ authority. |Written requests for PI extensions should arrive at FBIHQ seven work days prior to the expiration date.|

(5) |During the course of a PI, investigation may determine there is a reasonable indication that criminal activity has been, is being, or will be committed. At that time, the field supervisor is authorized to convert the 266 PI to a full 266 investigation. Upon doing so, a communication is to be sent to FBIHQ providing notification and predication for the conversion.|

EFFECTIVE: 06/23/97

266-4 REPORTING REQUIREMENTS

Upon initiation of a 266 investigation, an electronic communication must be immediately forwarded to the Domestic Terrorism Operations Unit (DTOU), FBIHQ, providing the date the investigation was initiated and the predication for its initiation. Upon closing the investigation, in addition to immediately notifying DTOU, field offices should update records in the FBINET Automated Case System (ACS) to reflect this fact.

EFFECTIVE: 06/23/97

||266-5| CHARACTER - ACTS OF TERRORISM - DOMESTIC TERRORISTS (AOTDT)

EFFECTIVE: 12/16/96

# SECTION 267. DRUG-RELATED HOMICIDE

## 267-1 BACKGROUND

(1) On 11/18/88, the President signed into law the Anti-Drug Abuse Act of 1988, which became Public Law 100-690. This Act, in part, amended Title 21, USC, by adding Subsection 848(e), entitled "Death Penalty."

(2) Under Subsection 848(e), the death penalty or lesser penalties may be imposed on:

(a) any person in or working in furtherance of a continuing enterprise, or any person engaged in an offense punishable under Title 21, USC, Section 841(b)(1)(A) or Section 960(b)(1) who intentionally kills or counsels, commands, induces, procures, or causes the intentional killing of an individual; or

(b) any person during the commission of, in furtherance of, or while attempting to avoid apprehension, prosecution or service of a prison sentence for, a felony violation under Title 21, USC, who intentionally kills, or counsels, commands, induces, procures, or causes the intentional killing of any Federal, state or local law enforcement officer engaged in, or on account of, the performance of such officer's official duties.

(3) Because of the addition of the act of homicide to Title 21, this amendment therefore created new jurisdiction for the FBI and Drug Enforcement Administration (DEA).

EFFECTIVE: 08/28/91

267-2 FBI/DEA Memorandum of Understanding (MOU)

"POLICY:

"1. The FBI and DEA recognize and agree that each agency has concurrent jurisdiction to investigate offenses under Section 7001 (of the Anti-Drug Abuse Act of 1988).

"2. The DEA will have investigative responsibility for drug-related slayings of nonlaw enforcement officers where DEA is the investigative agency in the predicate Title 21 investigation. In joint FBI/DEA investigations in which a nonlaw enforcement officer is killed, lead agency responsibility will be determined by the status of the individual killed. If the individual killed is an FBI informant or witness, the FBI will have lead investigative responsibility.

"3. The DEA will have investigative responsibility for the drug-related slayings of DEA Special Agents and employees, except as noted below. Informants, as well as deputized and nondeputized task force officers, are not considered to be employees for purposes of this MOU.

"a. If at any time during the investigation, facts or circumstances are developed which reasonably indicate that the slaying was an 'act of terrorism' as that term is defined in (Title) 18, U.S. Code, (Subsection) 3077(1), the investigation of the slaying will proceed as a joint investigation with the FBI being the lead agency.

"b. If there are simultaneous multiple slayings in the same predicate investigation resulting in the deaths of a DEA Special Agent and a deputized or nondeputized task force officer or the deaths of a DEA Special Agent and an FBI Special Agent, the investigation will be conducted as a joint investigation with the FBI being the lead agency.

"4. The FBI will have investigative responsibility for all other drug-related slayings.

"5. All investigations of this section of the Anti-Drug Abuse Act of 1988 are to be given top priority by the DEA and the FBI. It is agreed that any and all cooperation between the DEA and the FBI will be coordinated at the Special Agent in Charge level or the level designated by the Special Agent in Charge. Each agency will provide all available support and cooperation as requested and necessary to these investigations. Information will be exchanged as expeditiously

as possible and appropriate resources will be made available in all drug-related homicides investigated by the FBI and/or DEA.

"6. This MOU acknowledges the need to preserve the integrity of the DEA's ongoing drug investigations while also preserving the traditional investigative jurisdiction of the FBI and also its authority to investigate the felonious killings of state and local law enforcement officers as provided for by Section 7331 of the Anti-Drug Abuse Act of 1988.

"DISPUTE RESOLUTION

"In any situation in which this MOU proves to be ambiguous as to which agency has investigative responsibility for a drug-related slaying, any issues concerning the respective responsibilities of the FBI and the DEA for the conduct of the investigation will be promptly resolved between the DEA Assistant Administrator for Operations and the Assistant Director of the Criminal Investigative Division of the FBI.

"DEFINITIONS

"1. 'Lead Agency': The agency ultimately responsible for the management and direction of investigative activity.

"2. 'Law Enforcement Officer': A public servant authorized by law or by a Government agency or Congress to conduct or engage in the prevention, investigation, prosecution or adjudication of an offense, and includes those engaged in corrections, probation or parole functions. (See Title 21, U.S. Code, Subsection 848(e)(2)).

"AMENDMENT

"This MOU may be amended by deletion or modification of any provision contained herein, or by addition of new provisions, after written concurrence of the parties."

EFFECTIVE: 08/28/91

267-3 EXCLUSIVE FBI JURISDICTION

The FBI has investigative jurisdiction in all other DRH cases with the exception of DEA-related cases (see Section 267-2 "Policy") and drug-related slayings of Department of Treasury (DOT) personnel. Pursuant to a 10/2/56 agreement, the DOT has investigative jurisdiction over the assault and killing of its Federal officers. Therefore, the DOT could handle its own drug-related homicide investigations if the homicide did not pertain to any ongoing FBI/DEA investigation. For further information concerning DOT or U.S. Postal Service jurisdiction, refer to Part I, Sections 89-2.13 and 89-2.14 of this manual.

EFFECTIVE: 08/28/91

267-4 INVESTIGATIVE FBI POLICY

(1) FBIHQ is aware that a large percentage of homicides, particularly in the larger urban areas, are drug-related and/or gang-related. Therefore, highly selective criteria must be established in order to maximize the efforts of the limited resources of the Violent Crimes and Major Offenders Program. Furthermore, since the underlying statute of the DRH classification is one of the few federal statutes that provides the death penalty, cases opened under this classification should be significant enough to warrant imposition of the death penalty.

(2) Criteria to be used in opening DRH investigations:

(a) The drug-related "felonious" killing of a federal, state, or local law enforcement officer warrants the imposition of the death penalty. If the underlying provisions of Title 21, Section 848 (e)(1), are satisfied, cases can be opened without FBIHQ authority.

(b) Cases can be opened on murders of FBI, DEA, U.S. Customs, Internal Revenue Service or other federal agency informants, cooperating witnesses, grand jury or trial cases witnesses who currently are, or in the past have assisted the U.S. Government in investigations of violations of Title 21, USC, Section 848 (e)(1). FBIHQ authority is required to open these cases. (See (5) below.)

(c) FBIHQ will consider authorizing investigations involving drug-related homicides of nonlaw enforcement officers or

noninformant(s)/witness(es) if the murders are perpetrated to maintain, expand, consolidate, and/or defend drug trafficking enterprises. These cases should be limited to persons or organizations that are conducting a "Continuing Criminal Enterprise" as defined in Title 21, Section 848 (c). FBIHQ authority is required to open these cases. |(See (5) below.)|

(3) In the event the United States Attorney (USA) is not willing to seek prosecution under this statute and the victim is a Federal law enforcement officer, a "Killing of a Federal Officer" investigation (see Part I, Section 89, of this manual) under Title 18, USC, Section 1114, should be promptly instituted. If the victim is a state or local police officer, consideration should be given to instituting a "Police Killing" investigation (see Part I, Section 184, of this manual) under Title 28, USC, Section 540.

(4) For information of field offices, DOJ requires all federal prosecutors who intend to seek the death penalty to provide the DOJ with the written summary of the completed DRH investigation in order to obtain the personal approval of the Attorney General. Therefore, a final determination of federal prosecution, with the death penalty, will not be known until the investigation is completed and the Attorney General's approval is obtained.

(5) It is not the intention of the FBI to interject itself into matters which can be or should be investigated, prosecuted or otherwise resolved by other state and local law enforcement entities. The intent of this legislation is to assist local and state law enforcement in a united front against drug traffickers and drug trafficking organizations who commit murder(s) to facilitate their drug trafficking activities. Therefore, local homicides which are drug-related, but do not involve victims who are members of federal, state or local law enforcement, or do not involve victims specified in Sections 267-4(2)(b) and (c), supra, should not be used as a basis for instituting a 267 investigation.

EFFECTIVE: 11/25/94

267-5 REPORTING REQUIREMENTS

(1) Within five days of opening a 267A or 267B case, field offices will provide the Violent Crimes/Fugitive Unit, Criminal Investigative Division (CID), with the following:

(a) A summary of facts surrounding the killing and the facts which support the Title 21, USC, Section 848 (e)(1) violation.

(b) The name of the commanding officer of the local or state police department where the killing occurred and verification of his/her request for the FBI to enter the investigation.

(c) The name of the district attorney or state prosecutor who has agreed that the FBI/DOJ should pursue federal death penalty prosecution for those individuals involved in the killing.

(d) The name of the USA who has agreed to prosecute those individuals who violated the DRH statutes.

(2) Prior to opening a 267C case, field offices will send a teletype to the Violent Crimes/Fugitive Unit, CID, under the 267-0 file, requesting authority. The teletype should contain:

(a) Background of murder and circumstances relating to DRH violation.

(b) Facts supporting Title 21, Section 848 (e)(1) violation.

(c) Name of USA/AUSA who has agreed to prosecute DRH violation and a statement that his/her opinion has been/will be confirmed in writing.

(d) If the victim(s) was an FBI informant or cooperating witness, designate a copy to the Criminal Informant Unit, Intelligence Section, CID.

EFFECTIVE: 11/25/94

267-6 CHARACTER - DRUG-RELATED HOMICIDE

EFFECTIVE: 08/28/91

267-7 CLASSIFICATION | AND | SUBCLASSIFICATIONS | (See MAOP, Part II, 3-1.1, 3-1.2.) |

(1) The classification is 267.

(2) Subclassifications are:

(a) 267A - Drug-Related Homicide - Federal Officers (FO)

(b) 267B - Drug-Related Homicide - State/Local Officers (S/LO)

(c) 267C - Drug-Related Homicide - Nonlaw Enforcement Victims

(3) |Deleted|

EFFECTIVE: 10/18/95

267-8 CASE TITLE

(1) The case title should include each subject(s)' |name, | the name of the |victim(s), and the name of the drug trafficking organization, if known. |

(2) Example:

JOHN DOE;
|JOHN DOE DRUG TRAFFICKING ORGANIZATION; |
IAM A. GOODFELLOW - |VICTIM;
DRH - S/LO;
OO: LOS ANGELES
(267B-LA-0001)

EFFECTIVE: 08/28/91

267-9 VENUE

Generally, venue in DRH matters is governed by Title 18, U.S. Code, Subsection 3237. This section states that venue lies in any district in which the offense was begun, continued or completed. Logically, in single homicide cases involving law enforcement officers, venue will lie in the district where the homicide occurred. In multiple homicide cases, involving a major drug trafficking organization, venue will usually lie in the district where the organization is headquartered.

EFFECTIVE: 08/28/91

267-10 OFFICE OF ORIGIN

In DRH violations, office of origin will be determined by the place where the homicide(s) occurred or where the drug trafficking organization is headquartered.

EFFECTIVE: 08/28/91

# SECTION 268. ENGINEERING TECHNICAL MATTERS - FCI

## 268-1 ENGINEERING TECHNICAL MATTERS - FCI

The classification for "Engineering Technical Matters - FCI" was established for FBIHQ's use in capturing official correspondence related to classified engineering projects. The Technical Services Division (TSD), Engineering Section (ES) oversees these projects and generates most of the related documentation. Because it is strictly an administrative classification for recordkeeping purposes, the 268 classification is not intended for Time Utilization Recordkeeping (TURK) usage and will not be found in the FOIMS tables since it is mainly for FBIHQ's use. Field time expended on technical matters will continue to be recorded within the appropriate investigative program.

EFFECTIVE: 02/20/90

SECTION 269. ENGINEERING TECHNICAL MATTERS - NON-FCI

269-1 ENGINEERING TECHNICAL MATTERS - NON-FCI

The classification for "Engineering Technical Matters - Non-FCI" was established for FBIHQ's use in capturing official correspondence related to unclassified engineering projects. The Technical Services Division (TSD), Engineering Section (ES) oversees these projects and generates most of the related documentation. Because it is strictly an administrative classification for recordkeeping purposes, the 269 classification is not intended for Time Utilization Recordkeeping (TURK) usage and will not be found in the FOIMS tables since it is mainly for FBIHQ's use. Field time expended on technical matters will continue to be recorded within the appropriate investigative program.

EFFECTIVE: 02/20/90

# SECTION 270. COOPERATIVE WITNESSES

## 270-1 BACKGROUND

(1) Historically, the policy and procedures have not been established for the use of cooperative witnesses in criminal investigations. Interim guidelines on the use of cooperative witnesses have been established in this section until the new Attorney General Guidelines on the use of informants and cooperative witnesses are published.

(2) The policy and procedures for cooperative witnesses have been patterned after the Criminal Informant Program as closely as possible to help minimize differences in the administration of both programs.

(3) For details of the policy and procedures relative to the operation of cooperative witnesses, see the Memorandum to all Special Agents in Charge, number 8-90, entitled "Cooperative Witness (CW) Program - Interim Guidelines (IG)," dated 4/10/90.

EFFECTIVE: 02/12/92

## 270-2 DEFINITION

A cooperative witness is an individual whose relationship with the Government is concealed until testimony is required at trial and who, on a continuing basis and under the direction of an Agent, contributes substantial operational assistance to the resolution and/or direction of a case through active participation in the investigation.

EFFECTIVE: 02/12/92

# SECTION 271. ARMS CONTROL TREATY MATTERS

## 271-1 ARMS CONTROL TREATY MATTERS

Information concerning classification 271, Arms Control Treaty Matters, is set forth in a separate FBI manual, the NATIONAL FOREIGN INTELLIGENCE PROGRAM MANUAL (NFIPM).

EFFECTIVE: 02/14/97

SECTION 272. MONEY LAUNDERING (SEE MIOG, PART I, 281-15.)

272-1 INTRODUCTION

(1) The laundering of money, with its wide range of criminal applications, plays an integral role in concealing, enhancing and expanding crime. The money laundering statutes (Title 18, U.S. Code, Sections 1956 and 1957) proscribe virtually any transaction which involves the proceeds of a wide range of criminal activity. Consequently, the use of the money laundering statutes should be thoroughly explored in ALL Bureau cases.

(2) The money laundering statutes should be used in conjunction with the Bank Secrecy Act (BSA), Title 31, U.S. Code, Sections 5311 - 5322. [redacted] b2 b7E

(3) Title 18, U.S. Code, Section 1956 prohibits virtually any dealings with the proceeds of a wide range of "specified unlawful activities" (SUA) when those dealings are aimed at furthering or promoting the SUA or at concealing or disguising the nature, location, source, ownership, or control of the proceeds. (See Subsection 272-4(10) for a list of these SUAs.) Title 18, U.S. Code, Section 1956 also criminalizes money laundering transactions made with undercover law enforcement officers.

(4) Title 18, U.S. Code, Section 1957 effectively criminalizes any knowing monetary transaction or attempted monetary transaction in criminally derived property when three factors exist: (1) over $10,000 is involved, (2) a financial institution is utilized as defined in Title 31, U.S. Code, Section 5312, and (3) the property is derived from an SUA. The statute does not require that the property be used for any additional criminal purpose.

(5) The major impact of the money laundering statutes is that although the Government must prove that the proceeds were IN FACT derived from a "specified unlawful activity," e.g., drugs, it need only prove that the defendant knew, by direct or circumstantial proof, that the property involved in the financial transaction was the proceeds of SOME state or Federal FELONY crime.

EFFECTIVE: 10/26/93

272-2 MONEY LAUNDERING STATUTES

(1) Included in the Anti-Drug Abuse Act of 1986 and its amendments of 1988 are money laundering statutes that have a wide range of applications for many FBI cases. Violations of the money laundering laws are usually tied to other criminal activities, which range from the various RICO predicates and drugs, to bank fraud, espionage, etc.

(2) These money laundering laws are contained in Title 18, U.S. Code, Sections 1956 and 1957, with companion forfeiture provisions in Sections 981 (Civil) and 982 (Criminal).

(3) The following citations, 272-2.1 through 272-2.4 will assist the Agent in identifying these statutory areas.

EFFECTIVE: 10/26/93

272-2.1 Title 18, U.S. Code, Section 1956 (a)(1) - (Domestic Financial Transactions) (See MIOG, Part I, 272-2.)

(A)(i) is directed toward situations where the financial transaction involves illegal proceeds which are used to promote criminal activity (e.g., illegal proceeds are used to purchase drugs, storage facilities, vehicles, etc., in order to continue drug trafficking activity.)

(A)(ii) is directed toward situations where the financial transaction involves an intent to commit tax fraud or evasion.

(B)(i) is directed towards situations where the financial transaction involves illegal proceeds which are used to conceal the nature, location, source, ownership or control of the proceeds (e.g., the subject places the illegal proceeds into a "legitimate" business

in order to make the subject's wealth appear legitimate).

(B)(ii) is directed towards situations where the financial transaction is designed to avoid or attempt to avoid State or Federal reporting requirements (e.g., subject directs others (smurfs) to buy cashiers checks with illegal proceeds in amounts less than $10,000 to avoid Currency Transaction Reporting requirements).

EFFECTIVE: 10/26/93

272-2.2 Title 18, U.S. Code, Section 1956(a)(2) - International Financial Transactions (Transport, Transmit or Transfer Funds) (See MIOG, Part I, 272-2.)

(A) is directed toward situations where funds or monetary instruments are being moved into or out of the U.S. with the intent to promote an illegal activity (e.g., the proceeds are moved out of the United States to buy drugs).

(B)(i) is directed toward situations where illegal funds or monetary instruments are moved into or out of the U.S. in order to conceal the nature, source, etc., of the illegal proceeds (e.g., the subject moves or transmits an "illegal" monetary instrument to an offshore account or business in order to conceal or legitimatize the money).

(B)(ii) is directed toward situations where illegal funds are moved into or out of the U.S. in order to avoid a State or Federal transaction reporting requirement (e.g., subject moves the "illegal" funds out of the U.S. in amounts greater than $10,000 and does not file the appropriate Currency and Monetary Instrument Report).

EFFECTIVE: 10/26/93

272-2.3 Title 18, U.S. Code, Section 1956(a)(3) - Undercover Money Laundering Transactions (See MIOG, Part I, 272-2.)

(A) is directed toward situations where a financial transaction involving government undercover (UC) funds or property is used to promote an illegal activity (e.g., a subject uses money provided by a UCA to purchase a stash house).

(B) is directed toward situations where a financial transaction involving UC funds is used to conceal the fact that the funds are (believed to be) illegal (e.g., a subject uses property provided by a UCA to conceal the nature or control of the so-called illegal proceeds by purchasing a vehicle with hidden compartments for drugs or drug proceeds).

(C) is directed toward situations where a State or Federal financial transaction involving UC funds is used to avoid a transaction reporting requirement (e.g., a subject using property provided by a UCA buys several cashiers checks in amounts less than $10,000).

EFFECTIVE: 10/26/93

272-2.4 Title 18, U.S. Code, Section 1957 - Monetary Transactions in Criminally Derived Property Over $10,000 (See MIOG, Part I, 272-2.)

This section is generally designed to address a subject who "knowingly" engages in a monetary transaction involving criminally derived proceeds greater than $10,000 (e.g., an automobile dealer sells a $20,000 car to a drug dealer for cash, and then deposits those funds to his/her bank account, "knowing" that these funds were derived from illegal drug sales).

EFFECTIVE: 10/26/93

272-3 PENALTIES

EFFECTIVE: 10/26/93

272-3.1 Title 18, U.S. Code, Section 1956 (a)(1) and (2)

(1) The criminal penalty for a violation of either Subsection (a)(1) or (a)(2) of Section 1956 is a maximum sentence of 20 years' incarceration for each offense and/or a maximum fine of $500,000, or twice the value of the monetary instruments or funds involved, whichever is greater.

(2) Violators of Subsections 1956(a)(1) and (a)(2) are also liable to the United States for a civil penalty of not more than the greater of the value of the property, funds or monetary instruments involved in the transaction or $10,000. Such civil penalty is intended to be imposed in addition to any fine imposed for the criminal offense.

(3) It should also be noted that the forfeiture provisions of this act (See Title 18, U.S. Code, Sections 981 and 982) may be applied in addition to civil and criminal penalties. (See FORFEITURE AND ABANDONED PROPERTY MANUAL for additional information regarding civil and criminal forfeiture.) Thus, a person who violates Section 1956 by laundering $250,000 might have the funds civilly forfeited, be subject to a fine of up to $500,000 if convicted of the criminal offense, and pay a civil penalty of another $250,000. For payment of the criminal fine and civil penalty, the Government may look to other assets of the defendant not involved in the offense.

EFFECTIVE: 10/26/93

272-3.2 Title 18, U.S. Code, Section 1956(a)(3)

Maximum of 20 years' imprisonment; or a fine under Title 18; or both.

EFFECTIVE: 10/26/93

272-3.3 Title 18, U.S. Code, Section 1957

Maximum of 10 years' imprisonment; or a fine under Title 18 or twice the amount of the criminally derived property involved in the transaction; or both.

EFFECTIVE: 10/26/93

272-4 DEFINITIONS

(1) "Knowing that the property involved in a financial transaction represents the proceeds of some form of unlawful activity" (as in Title 18, U.S. Code, Section 1956 (c) (1)) means that the person knew the property involved in the transaction represented proceeds from some form, though not necessarily which form, of activity that constitutes a felony under State or Federal law, regardless of whether or not such activity is specifically defined as an SUA.

(2) The term "conducts" (as in Title 18, U.S. Code, Section 1956 (c) (2)) includes initiating, concluding, or participating in initiating, or concluding a transaction;

(3) The term "transaction" (as in Title 18, U.S. Code, Section 1956 (c) (3)) includes a purchase, sale, loan, pledge, gift, transfer, delivery, or other disposition, and with respect to a financial institution includes a deposit, withdrawal, transfer between accounts, exchange of currency, loan, extension of credit, purchase or sale of any stock, bond, certificate of deposit, or other monetary instrument, or any other payment, transfer, or delivery by, through, or to a financial institution, by whatever means effected;

(4) "Financial transaction" (as in Title 18, U.S. Code, Section 1956 (c) (4)) means a transaction involving the movement of funds by wire or other means or involving one or more monetary instruments, which in any way or degree affects interstate or foreign commerce, or a transaction involving the use of a financial institution which is engaged in, or the activities of which affect, interstate or foreign commerce in any way or degree;

(5) "Monetary instruments" (as in Title 18, U.S. Code, Section 1956 (c) (5)) means coin or currency of the United States or of any other country, travelers' checks, personal checks, bank checks, money orders, investment securities in bearer form or otherwise negotiable instruments in bearer form or otherwise in such form that title thereto passes upon delivery;

(6) The term "financial institution" (as in Title 18, U.S. Code, Section 1956 (c) (6)) includes the following:

"(A) an insured bank of the Federal Deposit Insurance Act;
(B) a commercial bank or trust company;
(C) a private banker;
(D) an agency or branch of a foreign bank in the United States;
(E) an insured institution of the National Housing Act;
(F) a thrift institution;
(G) a broker or dealer registered with the Securities and Exchange Commission;
(H) a broker or dealer in securities or commodities;
(I) an investment banker or investment company;
(J) a currency exchange;
(K) an issuer, redeemer, or cashier of travelers' checks, checks, money orders, or similar instruments;
(L) an operator of a credit card system;
(M) an insurance company;
(N) a dealer in precious metals, stones or jewels;
(O) a pawnbroker;
(P) a loan or finance company;
(Q) a travel agency;
(R) a licensed sender of money;
(S) a telegraph company;
(T) a business engaged in vehicle sales, including automobile, airplane, and boat sales;
(U) persons involved in real estate closings and

settlements;

(V) the United States Postal Service;

(W) an agency of the United States Government or of a state or local government carrying out a duty or power of a business (described in this paragraph);

(X) any business or agency which engages in any activity which the Secretary of the Treasury determines, by regulation, to be an activity which is similar to, related to, or a substitute for any activity in which any business (described in this paragraph) is authorized to engage; or

(Y) any other business (designated by the Secretary of Treasury) whose cash transactions have a high degree of usefulness in criminal, tax, or regulatory matters."

(7) "Represented" (as in Title 18, U.S. Code, Section 1956(a)(3)) means any representation made by a law enforcement officer or by another person at the direction of, or with the approval of, a federal official authorized to investigate or prosecute violations of Title 18, U.S. Code, Section 1956 (a) (3).

(8) "Monetary transaction" (as in Title 18, U.S. Code, Section 1957 (f) (1)) means the deposit, withdrawal, transfer, or exchange, in or affecting interstate or foreign commerce, of funds or a monetary instrument by, through, or to a financial institution, but such term does not include any transaction necessary to preserve a person's right to representation as guaranteed by the sixth amendment to the Constitution;

(9) "Criminally derived property" (as in Title 18, U.S. Code, Section 1957 (f) (2)) means any property constituting, or derived from, proceeds obtained from a criminal offense;

(10) "Specified Unlawful Activity" (SUA) (as in Title 18, U.S. Code, Section 1956) means: (See MIOG, Part I, 272-1(3).)

(a) with respect to a financial transaction occurring in whole or in part in the United States, an offense against a foreign nation involving the manufacture, importation, sale or distribution of a controlled substance (as in Title 21, U.S. Code, drug-type offenses;

(b) any act or acts constituting a continuing criminal enterprise (21, USC, 848);

(c) an offense under the following: (See 272-9, 272-13.)

- 18 USC 152 (relating to concealment of assets; false oaths and claims; bribery),
- 18 USC 215 (relating to commissions or gifts for procuring loans),
- 18 USC 500 through 503 (relating to certain counterfeiting offenses),
- 18 USC 513 (relating to securities of States and private entities),
- 18 USC 542 (relating to entry of goods by means of false statements),
- 18 USC 545 (relating to smuggling goods into the United States),
- 18 USC 549 (relating to removing goods from Customs Custody),
- 18 USC 641 (relating to public money, property, or records),
- 18 USC 656 (relating to theft, embezzlement, or misapplication by bank officer or employee),
- 18 USC 657 (relating to lending, credit and insurance institutions),
- 18 USC 658 (relating to property mortgaged or pledged to farm credit agencies),
- 18 USC 666 (relating to theft or bribery concerning programs receiving Federal funds),
- 18 USC 793, 794 or 798 (relating to espionage),
- 18 USC 875 (relating to interstate communications),
- 18 USC 1005 (relating to bank fraud and embezzlement),
- 18 USC 1006 (relating to fraudulent credit institution entries),
- 18 USC 1007 (relating to bank fraud and embezzlement),
- 18 USC 1014 (relating to fraudulent loan or credit applications),
- 18 USC 1032 (relating to concealment of assets from a financial institution),
- 18 USC 1201 (relating to kidnapping),
- 18 USC 1203 (relating to hostage taking),
- 18 USC 1341 (relating to frauds and swindles against financial institutions involving mail),
- 18 USC 1343 (relating to wire fraud affecting a financial institution),
- 18 USC 1344 (relating to bank fraud),
- 18 USC 2113 or 2114 (relating to bank and postal robbery and theft),

|- 18 USC 2251, 2251A, 2252, and 2258 (relating to sexual exploitation of children) (FBI) (USCS) (The jurisdiction of USCS under this SUA involves the importation or exportation of material involving the sexual exploitation of children.)|

- 18 USC 2319 (relating to copyright infringement),

|- 18 USC 2320 (relating to trafficking in counterfeit goods or services) (FBI),|

- 19 USC 1590 (relating to aviation smuggling),

- 21 USC 830 (relating to precursor and essential chemicals),

- 21 USC 857 (relating to transportation of drug paraphernalia),

|- Section 15 of the Food Stamp Act of 1977 (relating to Food Stamp Fraud) involving a quantity of coupons having a value of not less than $5,000 (FBI),|

- Section 38(C) (relating to criminal violations), of the Arms Export Control Act (22 USC 2778),

- Section 11 (relating to violations) of the Export Administration Act of 1979 (50 USC App. 2410),

- Section 206 (relating to penalties) of the International Emergency Economic Powers Act (50 USC 1702), or

- Section 16 (relating to offenses and punishment) of the Trading with the Enemy Act (50 USC App. 3);

- 33 USC 1251 et seq. (felony offenses relating to the discharge of pollutants into the Nation's waters),

- 33 USC 1401 et seq. (felony offenses relating to the dumping of materials into ocean waters),

- 33 USC 1901 et seq. (felony offenses relating to the discharge of pollutants from ships),

- 42 USC 300f et seq. (felony offenses related to the safety of public water systems),

- 42 USC 6901 et seq. (felony offenses relating to resource conservation and recovery); or

(d) Any act or activity constituting one of the predicate offenses to the Racketeer Influenced and Corrupt Organizations (RICO) Statute (Title 18, U.S. Code, Section 1961(1)) except an act which is indictable under the Currency and Foreign Transactions Reporting Act. |(See MIOG, Part I, 183-1.2.)| These offenses are as follows:

1. Any act or threat involving:

Murder
|Kidnapping|
Gambling

Arson
Robbery
Bribery
Extortion
Dealing in obscene matter, or
Dealing in a controlled substance or listed chemical (as defined in Section 102 of the Controlled Substances Act) which is chargeable as a state felony;

2. Any act which is indictable under any of the following:

- 18 USC 201 (relating to bribery),
- 18 USC 224 (relating to sports bribery),
- 18 USC 471-473 (relating to counterfeiting),
- 18 USC 659 (relating to theft from interstate shipment) if the act indictable under section 659 is felonious,
- 18 USC 664 (relating to embezzlement from pension and welfare funds),
- 18 USC 891-894 (relating to extortionate credit transactions),
- 18 USC 1028 (related to fraud and related activity in connection with identification documents) if the act indictable under Section 1028 was committed for the purpose of financial gain,
- 18 USC 1029 (relating to fraud and related activity in connection with access devices),
- 18 USC 1084 (relating to the transmission of gambling information),
- 18 USC 1341 (relating to mail fraud),
- 18 USC 1343 (relating to wire fraud),
- 18 USC 1344 (relating to bank fraud),
- 18 USC 1461-1465 (relating to obscene matter),
- 18 USC 1503 (relating to obstruction of justice),
- 18 USC 1510 (relating to obstruction of criminal investigations),
- 18 USC 1511 (relating to the obstruction of state or local law enforcement),
- 18 USC 1512 (relating to tampering with a witness, victim, or an informant),
- 18 USC 1513 (relating to retaliating against a witness, victim, or an informant),
- 18 USC 1542 (relating to false statement in application and use of passport) if the act indictable under Section 1542 was committed for the purpose of financial gain,
- 18 USC 1543 (relating to forgery or false use of passport) if the act indictable under Section 1543 was committed for

the purpose of financial gain,
- 18 USC 1544 (relating to misuse of passport) if the act indictable under Section 1544 was committed for the purpose of financial gain,
- 18 USC 1546 (relating to fraud and misuse of visas, permits, and other documents) if the act indictable under Section 1545 was committed for the purpose of financial gain,
- 18 USC 1581-1588 (relating to peonage and slavery),
- 18 USC 1951 (relating to interference with commerce, robbery, or extortion),
- 18 USC 1952 (relating to racketeering),
- 18 USC 1953 (relating to interstate transportation of wagering paraphernalia),
- 18 USC 1954 (relating to unlawful welfare fund payments),
- 18 USC 1955 (relating to the prohibition of illegal gambling business),
- 18 USC 1956 (relating to the laundering of monetary instruments),
- 18 USC 1957 (relating to engaging in monetary transactions in property derived from SUA),
- 18 USC 1958 (relating to use of interstate commerce facilities in the commission of murder-for-hire),
- 18 USC 2251, 2251A, 2252 and 2258 (relating to sexual exploitation of children),
- 18 USC 2312 and 2313 (relating to interstate transportation of stolen motor vehicles),
- 18 USC 2314 and 2315 (relating to interstate transportation of stolen property),
- 18 USC 2321 (relating to trafficking in certain motor vehicles or vehicle parts),
- 18 USC 2341-2346 (relating to trafficking in contraband cigarettes),
- 18 USC 2421-2424 (relating to white slave traffic);

3. Any act which is indictable under:

- 29 USC 186 (dealing with restrictions on payments and loans to labor organizations) or,
- 29 USC 501(c) (relating to embezzlement from union funds);

4. Any offense involving:

fraud connected with a case under Title 11 (except a case under Section 157 of this title), fraud in the sale of securities, or the

felonious manufacture, importation, receiving, concealment, buying, selling, or otherwise dealing in a controlled substance or listed chemical (as defined in Section 102 of the Controlled Substances Act), punishable under any law of the United States;

5. Any act which is indictable under the Immigration and Naturalization Act, Section 274 (relating to bringing in or harboring certain aliens), Section 277 (relating to aiding or assisting certain aliens to enter the United States), or Section 278 (relating to importation of alien for immoral purpose) if the act indictable under such section of such Act was committed for the purpose of financial gain.

NOTE: The investigatory jurisdiction for money laundering violations is shared by numerous federal law enforcement agencies and is set forth in a Memorandum of Understanding (MOU) among the Department of Justice, Treasury Department and the Postal Service. (See MIOG, Part I, 272-13.) Generally, this jurisdiction is determined by the particular SUA(s) involved. For further information regarding money laundering jurisdiction, see MIOG, Part I, 272-9.

EFFECTIVE: 10/02/96

272-5 [redacted]

b7E

OPCA-20 (12-3-96)

XXXXXX
XXXXXX
XXXXXX

# FEDERAL BUREAU OF INVESTIGATION
## FOIPA
## DELETED PAGE INFORMATION SHEET

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

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

**Section 552**

☐ (b)(1)
☑ (b)(2)
☐ (b)(3)
_____
_____
_____
☐ (b)(4)
☐ (b)(5)
☐ (b)(6)
☐ (b)(7)(A)
☐ (b)(7)(B)
☐ (b)(7)(C)
☐ (b)(7)(D)
☑ (b)(7)(E)
☐ (b)(7)(F)
☐ (b)(8)
☐ (b)(9)

**Section 552a**

☐ (d)(5)
☐ (j)(2)
☐ (k)(1)
☐ (k)(2)
☐ (k)(3)
☐ (k)(4)
☐ (k)(5)
☐ (k)(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 Sec 272 p14-23

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

XXXXXX
XXXXXX
XXXXXX

FBI/DOJ

(USSS), Bureau of Alcohol, Tobacco and Firearms (ATF), and the Postal Inspection Service (USPS). The FBI has investigatory jurisdiction, in general, over SUAs relating to its existing jurisdiction, i.e., drugs, white-collar crime, violent crimes, foreign counterintelligence, etc.

(2) The investigatory jurisdiction of the FBI, DEA, USCS, USSS, ATF, and the USPS is determined by the specific SUAs involved. A list of these SUAs is set forth below followed by the abbreviated name of the agency or agencies having money laundering jurisdiction for that SUA:

(a) with respect to a financial transaction occurring in whole or in part in the United States, an offense against a foreign nation involving the manufacture, importation, sale, or distribution of a controlled substance (FBI, DEA);

(b) any act or acts constituting a continuing criminal enterprise (21, USC, 848) (FBI, DEA, USPS);

(c) an offense under the following:

- 18 USC 152 (relating to concealment of assets; false oaths and claims; bribery) (FBI),
- 18 USC 215 (relating to commissions or gifts for procuring loans) (FBI),
- 18 USC 500 through 503 (relating to certain counterfeiting offenses) (USSS, USPS) (The jurisdiction of USPS under this SUA involves counterfeiting of money orders, postcards, indicia of postage and postmarking stamps.)
- 18 USC 513 (relating to securities of states and private entities) (FBI),
- 18 USC 542 (relating to entry of goods by means of false statements) (USCS),
- 18 USC 545 (relating to smuggling goods into the United States) (USCS),
- 18 USC 549 (relating to removing goods from Customs Custody) (USCS),
- 18 USC 641 (relating to public money, property, or records) (FBI, USPS),
- 18 USC 656 (relating to theft, embezzlement, or misapplication by bank officer or employee) (FBI),
- 18 USC 657 (relating to lending, credit and insurance institutions) (FBI, USSS) (The jurisdiction of USSS under this SUA involves theft, embezzlement or misapplication by employees of the Federal Deposit Insurance Corporation.)
- 18 USC 658 (relating to property mortgaged or

pledged to farm credit agencies) (FBI),

- 18 USC 666 (relating to theft or bribery concerning programs receiving federal funds) (FBI),
- 18 USC 793, 794 or 798 (relating to espionage) (FBI),
- 18 USC 875 (relating to interstate communications) (FBI),
- 18 USC 1005 (relating to bank fraud and embezzlement) (FBI),
- 18 USC 1006 (relating to fraudulent credit institution entries) (FBI),
- 18 USC 1007 (relating to bank fraud and embezzlement) (FBI),
- 18 USC 1014 (relating to fraudulent loan or credit applications) (FBI),
- 18 USC 1032 (relating to concealment of assets from a financial institution) (FBI),
- 18 USC 1201 (relating to kidnapping) (FBI),
- 18 USC 1203 (relating to hostage taking) (FBI),
- 18 USC 1341 (relating to frauds and swindles against financial institutions involving mail) (FBI),
- 18 USC 1343 (relating to wire fraud affecting a financial institution) (FBI),
- 18 USC 1344 (relating to bank fraud) (FBI),
- 18 USC 2113 or 2114 (relating to bank and postal robbery and theft) (FBI, USPS) (FBI and USPS share money laundering jurisdiction regarding the Section 2114 SUA.),
- 18 USC 2251, 2251A, 2252, and 2258 (relating to sexual exploitation of children) (FBI) (USCS) (The jurisdiction of USCS under this SUA involves the importation or exportation of material involving the sexual exploitation of children.)
- 18 USC 2319 (relating to copyright infringement) (FBI),
- 18 USC 2320 (relating to trafficking in counterfeit goods or services) (FBI),
- 19 USC 1590 (relating to aviation smuggling) (USCS),
- 21 USC 830 (relating to precursor and essential chemicals) (FBI, DEA),
- 21 USC 857 (relating to transportation of drug paraphernalia) (FBI, DEA, USCS, USPS) (The jurisdiction of USCS under this SUA involves the illegal importation or exportation of drug paraphernalia.),
- Section 15 of the Food Stamp Act of 1977 (relating to Food Stamp Fraud) involving a quantity of coupons having a value of not less than $5,000 (FBI),

- Section 38(c) (relating to criminal violations), of the Arms Export Control Act (22 USC 2778) (USCS, ATF) (The jurisdiction of USCS under this SUA involves exportation, intransit, temporary import, or temporary export transactions. The jurisdiction of ATF under this SUA involves the importation of items on the U.S. Munitions Import List, except those relating to exportation, intransit, temporary import, or temporary export transactions.)
- Section 11 (relating to violations) of the Export Administration Act of 1979 (50 USC App. 2410) (USCS)
- Section 206 (relating to penalties) of the International Emergency Economic Powers Act (50 USC 1702) (USCS) or
- Section 16 (relating to offenses and punishment) of the Trading with the Enemy Act (50 USC App. 3) (USCS),
- 33 USC 1251 et seq. (felony offenses relating to the discharge of pollutants into the Nation's waters) (FBI, EPA),
- 33 USC 1401 et seq. (felony offenses relating to the dumping of materials into ocean waters) (FBI, EPA),
- 33 USC 1901 et seq. (felony offenses relating to the discharge of pollutants from ships) (FBI, EPA),
- 42 USC 300f et seq. (felony offenses relating to the safety of public water systems) (FBI, EPA),
- 42 USC 6901 (felony offenses relating to resource conservation and recovery) (FBI, EPA);

(d) Any act or activity constituting one of the predicate offenses to the Racketeer Influenced and Corrupt Organizations (RICO) Statute (Title 18, U.S. Code, Section 1961(1)) except an act which is indictable under the Currency and Foreign Transactions Reporting Act. These offenses are as follows:

1. Any act or threat involving:

   Murder (FBI)
   Kidnapping (FBI)
   Gambling (FBI)
   Arson (FBI, ATF)
   Robbery (FBI)
   Bribery (FBI)
   Extortion (FBI)
   Dealing in obscene matter (FBI), or
   Dealing in narcotic or other dangerous drugs (FBI, DEA, USPS),

   which is chargeable as a state felony;

2. Any act which is indictable under any of the following:

- 18 USC 201 (relating to bribery) (FBI, USPS),
- 18 USC 224 (relating to sports bribery) (FBI),
- 18 USC 471, 472, and 473 (relating to counterfeiting) (USSS),
- 18 USC 659 (relating to theft from interstate shipment) if the act indictable under section 659 is felonious (FBI, USCS) (The jurisdiction of USCS under this SUA involves theft from foreign shipment.),
- 18 USC 664 (relating to embezzlement from pension and welfare funds) (FBI),
- 18 USC 891-894 (relating to extortionate credit transactions) (FBI),
- 18 USC 1028 (relating to fraud and related activity in connection with identification documents) if the act indictable under Section 1028 was committed for the purpose of financial gain (FBI, USSS),
- 18 USC 1029 (relating to fraud and related activity in connection with access devices) (FBI, USSS, USPS),
- 18 USC 1084 (relating to the transmission of gambling information) (FBI),
- 18 USC 1341 (relating to mail fraud) (FBI, USPS),
- 18 USC 1343 (relating to wire fraud) (FBI, USPS) (The USPS shares this wire-fraud money laundering jurisdiction with the FBI when the primary focus of the offense is mail fraud.),
- 18 USC 1344 (relating to bank fraud) (FBI),
- 18 USC 1461-1465 (relating to obscene matter) (FBI, USCS, USPS) (The jurisdiction of USCS under this SUA involves Sections 1461-63 and 1465 relating to illegal importation or exportation of obscene matter. The jurisdiction of USPS under this SUA involves Sections 1461 and 1463 regarding mailing of obscene matter.),
- 18 USC 1503 (relating to obstruction of justice) (FBI, USPS),
- 18 USC 1510 (relating to obstruction of criminal investigations) (FBI, USPS),
- 18 USC 1511 (relating to the obstruction of state or local law enforcement) (FBI, USPS),
- 18 USC 1512 (relating to tampering with a witness, victim, or an informant) (FBI, USPS),
- 18 USC 1513 (relating to retaliating against a witness, victim, or an informant) (FBI, USPS),
- 18 USC 1542 (relating to false statement in

application and use of passport) if the act indictable under Section 1542 was committed for the purpose of financial gain (FBI),

- 18 USC 1543 (relating to forgery or false use of passport) if the act indictable under Section 1543 was committed for the purpose of financial gain (FBI),

- 18 USC 1544 (relating to misuse of passport) if the act indictable under Section 1544 was committed for the purpose of financial gain (FBI),

- 18 USC 1546 (relating to fraud and misuse of visas, permits, and other documents) if the act indictable under Section 1545 was committed for the purpose of financial gain (FBI),

- 18 USC 1581-1588 (relating to peonage and slavery) (FBI),

- 18 USC 1951 (relating to interference with commerce, robbery, or extortion) (FBI),

- 18 USC 1952 (relating to racketeering) (FBI, ATF) (The jurisdiction of ATF under this SUA involves traveling in interstate commerce with respect to arson and to liquor on which federal excise tax has not been paid. The jurisdiction of USPS under this SUA involves mailing in aid of racketeering enterprises.),

- 18 USC 1953 (relating to interstate transportation of wagering paraphernalia) (FBI),

- 18 USC 1954 (relating to unlawful welfare fund payments) (FBI),

- 18 USC 1955 (relating to the prohibition of illegal gambling business) (FBI),

- 18 USC 1956 (relating to laundering of monetary instruments) (FBI),

- 18 USC 1957 (relating to engaging in monetary transactions in property derived from SUA) (FBI),

- 18 USC 1958 (relating to use of interstate commerce facilities in the commission of murder-for-hire) (FBI),

- 18 USC 2251, 2251A, 2252, and 2258 (relating to sexual exploitation of children) (FBI, USCS) (The jurisdiction of USCS under this SUA involves the importation or exportation of material involving the sexual exploitation of children.),

- 18 USC 2312 and 2313 (relating to interstate transportation of stolen motor vehicles) (FBI),

- 18 USC 2314 and 2315 (relating to interstate transportation of stolen property) (FBI, USCS) (The jurisdiction of USCS under this SUA involves foreign transportation of stolen property.),

- 18 USC 2321 (relating to trafficking in certain motor vehicles or vehicle parts) (FBI, USCS) (The jurisdiction of USCS under this SUA involves importation or exportation of certain motor vehicles or vehicle parts.),

- 18 USC 2341-2346 (relating to trafficking in contraband cigarettes) (ATF),
- 18 USC 2421-2424 (relating to white slave traffic) (FBI);

3. Any act which is indictable under

- 29 USC 186 (dealing with restrictions on payments and loans to labor organizations) or (FBI),
- 29 USC 501(c) (relating to embezzlement from union funds) (FBI);

4. Any offense involving fraud connected with a case under Title 11, fraud in the sale of securities, or the felonious manufacture, importation, receiving, concealment, buying, selling, or otherwise dealing in a controlled substance or listed chemical (as defined in Section 102 of the Controlled Substances Act) (FBI), punishable under any law of the United States.

5. Any act which is indictable under the Immigration and Naturalization Act, Section 274 (relating to bringing in or harboring certain aliens), Section 277 (relating to aiding or assisting certain aliens to enter the United States), or Section 278 (relating to importation of alien for immoral purpose) if the act indictable under such section of such Act was committed for the purpose of financial gain.

EFFECTIVE: 10/02/96

272-10 INTERRELATED STATUTES

EFFECTIVE: 10/26/93

272-10.1 Interstate Transportation In Aid of Racketeering (ITAR) Statute

The money laundering violations (Title 18, USC, Sections 1956 and 1957) and Title 31 violations dealing with reporting of currency transactions (acts indictable under subchapter II of Chapter 53 of Title 31, United States Code) have been added as predicate offenses ("unlawful activities") for the ITAR Statute (Title 18, USC, Section 1952).

EFFECTIVE: 10/26/93

272-10.2 Racketeer Influenced and Corrupt Organizations (RICO) Statute

The money laundering violations (Title 18, USC, Sections 1956 and 1957) have been added as predicate offenses ("racketeering activities") for the RICO Statute (Title 18, USC, Section 1961).

EFFECTIVE: 10/26/93

272-10.3 Interception of Wire, Oral, or Electronic Communications

Section 2516 of Title 18 of the USC, also referred to as "Title III," includes the money laundering violations (Title 18, USC, Sections 1956 and 1957) within the enumerated offenses which authorize the interception of communications.

EFFECTIVE: 10/26/93

272-11 INTERNATIONAL LEADS

In ALL CASES, including drug matters, money laundering leads to be conducted in foreign countries will be covered by the appropriate FBI Legal Attache.

EFFECTIVE: 10/26/93

272-12 THE BANK SECRECY ACT (See MIOG, Part I, 272-5.1(1).)

(1) On October 26, 1970, the President signed the "Bank Records and Foreign Transaction Act" into law. Titles I and II of this Act constitute what is commonly known as the Bank Secrecy Act (BSA). The BSA is codified under Title 31, U.S. Code, Sections 5311 - 5322 and should not be confused with the "Money Laundering Statutes." The intent behind the BSA is to enhance law enforcement investigations of criminal enterprises dealing in large sums of currency, whether the underlying criminal activity involves drugs, organized crime or white collar crime. The primary purpose of the reporting requirements of the BSA is to identify the sources and movements of United States currency being transported into or out of the country or being deposited into financial institutions.

(2) The BSA has not been well understood since its passage. However, it is now being realized that the currency reporting statutes can be used to attack criminal enterprises by focusing on the profits they reap. The BSA is specifically designed to aid in this attack by creating a "paper trail" to trace those proceeds back to their illegal source.

EFFECTIVE: 10/26/93

272-12.1 BSA Reporting Requirements and IRS Form 8300

(1) Under the BSA requirements, individuals, banks, and financial institutions must report cash transactions which involve the payment, receipt, or transfer of cash of $10,000 or more. The report is made on Internal Revenue Service (IRS) Form 4789, Currency Transaction Report (CTR).

(2) Casinos are required to report cash transactions of $10,000 or more. Casinos file a Currency Transaction Report by Casino (CTRC), which is IRS Form 8362.

(3) The BSA requires two types of foreign financial reports.

(a) Individuals who transport "monetary instruments" into or out of the United States or receive such instruments in the United States from abroad must report the transaction. This report is made on United States Customs Service (USCS) Form 4790, International Transportation of Currency or Monetary Instrument Report (CMIR).

(b) Any person of the United States who has a financial interest in bank securities or other financial accounts in a foreign country must report certain information. This report is made on Department of Treasury Form 90-22.1, Foreign Bank and Financial Accounts Report (FBAR).

(4) In addition, under the authority of the Secretary of the Treasury, the IRS requires that businesses or other entities file a report when a product or service is paid for with United States currency of $10,000 or more. That report is made on IRS Form 8300.

EFFECTIVE: 10/26/93

272-12.2 Access to BSA Report Information

(1) Under the BSA, the Department of Treasury is responsible for collection, administration, and dissemination of BSA report information. United States Customs Service and Internal Revenue Service officials at their respective headquarters and field offices may disseminate BSA report information to Federal, state, and local law enforcement agencies.

(2) Because BSA report information consists of personal and sensitive financial data, strict guidelines have been adopted for disseminating BSA report information. Under these guidelines, BSA report information includes all data reported to the Department of Treasury on the following forms:

(a) Currency Transaction Report (CTR), IRS Form 4789;

(b) Currency Transaction Report by Casinos (CTRC), IRS Form 8362;

(c) International Transportation of Currency or Monetary Instrument Report (CMIR), USCS Form 4790;

(d) Foreign Bank and Financial Accounts Report (FBAR), Department of Treasury Form 90-22.1;

(e) IRS Form 8300.

EFFECTIVE: 10/26/93

272-12.3 Procedures for Requesting BSA Report Information (See MIOG, Part I, 272-12.5.)

All requests for BSA report information should be made to the appropriate USCS or IRS field office. Requests must be made in writing unless exigent circumstances exist. Requests should be made by letter, on letterhead, and signed by the SAC. The letter should state the intended purpose for the information, specific violations or potential violations of law involved, and identifying data for the individuals or businesses being checked. If a verbal request for BSA

report information is made under exigent circumstances, a written confirmation of the verbal request must be made.

EFFECTIVE: 10/26/93

272-12.4 Requesting Statistical BSA Report Information

Field offices may request statistical BSA report information where no specific personal or financial information is involved. For example, a request can be made for a list of all companies and individuals who have CTRs with a cumulative amount of $1,000,000 filed by banks within a certain area. As almost 17 million CTRs were filed between 1987 and 1989, caution should be used when framing such a request. Investigative personnel may wish to contact IRS or USCS representatives regarding requests for statistical information in order to ensure a comprehensive and manageable work product.

EFFECTIVE: 10/26/93

272-12.5 Unsolicited Disclosure of BSA Report Information

The IRS or USCS may disclose BSA report information to the FBI or other Federal, state, or local law enforcement agencies when it is determined that such information may be useful in a particular investigation or procedure. Follow-up requests for additional BSA report information must be made according to MIOG, Part I, 272-12.3, above.

EFFECTIVE: 10/26/93

272-12.6 Disclosure of BSA Report Information Within Task Force or Joint Investigations

Representatives of IRS or USCS may disclose BSA report information to other members of a joint or task force investigation, for use in that particular investigation. In such instances, no written request is necessary.

EFFECTIVE: 10/26/93

272-12.7 Direct Access to BSA Report Information by FBI Analysts

The Assistant Secretary of the Treasury has approved direct access to BSA report information by FBI analysts through the IRS or USCS. Prior to initial access to BSA report information the analyst will be required to acknowledge a statement reflecting that he/she understands the restrictions on disclosure outside the FBI.

EFFECTIVE: 10/26/93

272-12.8 Access to BSA Report Information Through the Financial Crimes Enforcement Network (FinCEN)

(1) In those selective, high priority investigations where it would be beneficial to have additional information from FinCEN's criminal, commercial, and financial data bases, to include BSA report information, a letter should be forwarded to FinCEN requesting analytical assistance. The letter, on FBI letterhead, should be directed to:

b7C

[redacted]

(2) If exigent circumstances exist which would preclude a

written request, it is possible to telephonically contact the FinCEN Operations Center at telephone number 1 (800) 707-2825. It should be noted that FinCEN is an agency of the Department of Treasury which functions, in part, to support Federal, state, and local law enforcement agencies.

(3) It should be noted that under the operating procedures of FinCEN, records are maintained on each request received. The law enforcement agency which submitted the first request will be notified of all subsequent inquiries without exception.

EFFECTIVE: 10/26/93

272-13 "Memorandum of Understanding Among the Secretary of the Treasury, the Attorney General and the Postmaster General Regarding Money Laundering Investigations" (See MIOG, Part I, 183-1.2, 272-4(10)(d)4. & 272-9.)

"This Memorandum of Understanding (MOU) constitutes an agreement among the Secretary of the Treasury ("the Secretary"), the Attorney General and the Postmaster General as to the investigatory authority and procedures of Treasury and Justice bureaus and the Postal Service under 18 U.S.C sections 1956 and 1957, as amended by the Anti-Drug Abuse Act of 1988, Pub. L. 100-690 (Nov. 18, 1988). This replaces a previous MOU on this subject between the Secretary and the Attorney General effective May 20, 1987.

"Section I. Purpose

"The Attorney General, the Secretary and the Postmaster General have entered into this MOU in order to encourage effective and harmonious cooperation by Treasury and Justice bureaus and the Postal Service in the development of cases by bureaus with appropriate experience, to reduce the possibility of duplicative investigations, to minimize the potential for dangerous situations which might arise from uncoordinated multi-bureau efforts, and to enhance the potential for successful prosecution in cases presented to the various United States Attorneys.

"As clearly stated in the legislative history of the Act, this MOU does not confer any rights on any third party, including a defendant or other party in litigation with the United States. The fact that a bureau investigates a violation of section 1956 or section 1957 that

should have been investigated by another bureau under the terms of this MOU, or that any agency not a party to this MOU investigates a violation of section 1956 or section 1957, confers no rights and provides no defense to any party.

"While this MOU allocates jurisdiction to investigate violations of sections 1956 and 1957, nothing in this MOU is intended to augment or diminish the investigatory authority of any Justice or Treasury bureau or the Postal Service over violations of any Federal criminal law, independent of the money laundering statute, or to alter the existing allocation or delegation of such authority. This MOU governs all investigations involving 18 U.S.C. 1956 and 1957 and is intended to be used together with MOU's presently existing between the bureaus. This MOU does not supersede the provision of 26 U.S.C. 6103 (confidentiality and disclosure of returns and return information).

"Section II. Definitions

"1. 'Bureau' includes the Postal Inspection Service.

"2. 'Treasury bureaus' mean the Internal Revenue Service (IRS), the United States Customs Service, the Bureau of Alcohol, Tobacco, and Firearms (ATF), and the United States Secret Service.

"3. 'Justice bureaus' means the Drug Enforcement Administration (DEA) and the Federal Bureau of Investigation (FBI).

"4. 'Violations of section 1956' refers to both civil and criminal violations.

"5. 'Specified unlawful activities' has the definition set forth in 18 U.S.C. section 1956 (c)(7).

"6. 'Justice Department attorney' means the appropriate Assistant United States Attorney or designated Justice Department attorney assigned to the prosecution of the case.

"Section III. Investigatory Jurisdiction

"A bureau's investigatory actions in pursuit of a section 1956 or 1957 violation shall be conducted only in those areas in which the investigating bureau has existing jurisdiction, independent of the money laundering statutes, as set forth in this Section.

"A. Treasury Bureaus

"1. Internal Revenue Service

"The Internal Revenue Service will have investigative jurisdiction over all violations of Section 1956 and 1957 where the underlying conduct is subject to investigation under Title 26 or the Bank Secrecy Act.

"2. United States Customs Service

"a. The United States Customs Service will have investigatory jurisdiction over violations of section 1956 or section 1957 involving the following specified unlawful activities: criminal offenses under 18 U.S.C. section 542, (relating to entry of goods by means of false statements), section 545 (relating to the smuggling of goods into the United States), section 549 (relating to removing goods from Customs custody), section 659 (relating to theft from foreign shipment), sections 1461-63 and 1465 (relating to illegal import or export of obscene matter), sections 2251-52 (relating to imports or exports of material involving sexual exploitation of children), section 2314 (relating to foreign transportation of stolen property), and section 2321 (relating to the import or export of certain motor vehicles or vehicle parts); 19 U.S.C. section 1590 (relating to aviation smuggling); 21 U.S.C. section 857 (relating to the illegal import or export of drug paraphernalia); criminal offenses under section 11 of the Export Administration Act of 1979 (50 U.S.C. App. section 2410); criminal offenses under section 206 of the International Emergency Economic Powers Act (50 U.S.C. 1705); criminal offenses under section 16 of the Trading with the Enemy Act (50 U.S.C. App. 16); and criminal offenses under section 38(c) of the Arms Export Control Act (22 U.S.C. section 2778) (relating to exportation, intransit, temporary import, or temporary export transactions).

"b. The United States Customs Service will have investigatory jurisdiction over violations of section 1956(a)(2)(B)(ii), involving the international transportation of monetary instruments or funds which are proceeds of some form of unlawful activity and where the defendant knew that the transportation was designed in whole or in part to avoid a transaction reporting requirement under 31 U.S.C. 5316 (Reports on exporting and importing monetary instruments).

"3. United States Secret Service

"The United States Secret Service will have investigatory jurisdiction over violations of section 1956 or section 1957 involving the specified unlawful activity of an offense under 18 U.S.C. sections

471-473 (counterfeiting of obligations or securities of the United States), sections 500-503 (counterfeiting of blank or postal money orders, postage stamps, foreign governments postage and revenue stamps, and postmarking stamps), section 657 (involving theft, embezzlement or misapplication by employees of the FDIC), and section 1029 (fraud and related activity in connection with access devices).

"4. Bureau of Alcohol, Tobacco and Firearms

"The Bureau of Alcohol, Tobacco and Firearms will have investigatory jurisdiction over violations of section 1956 or section 1957 involving the specified unlawful activity of an offense under 18 U.S.C. sections 2341-2346 (trafficking in contraband cigarettes); section 38(c) of the Arms Export Control Act, 22 U.S.C section 2778 (relating to the importation of items on the U.S. Munitions Import List, except those relating to exportation, intransit, temporary import, or temporary export transactions); and 18 U.S.C. 1952 (relating to travelling in interstate commerce, with respect to liquor on which federal excise tax has not been paid and arson); or any act or activity constituting an offense listed in 18 U.S.C. 1961(1), with respect to any act or threat involving arson, which is chargeable under State law and punishable for more than one year.

"B. Justice Bureaus

"1. Federal Bureau of Investigation

"The Federal Bureau of Investigation will have investigatory jurisdiction over violations of section 1956 or section 1957 involving the specified unlawful activities of an offense under 18 U.S.C. section 152 (relating to concealment of assets; false oaths and claims; bribery), section 215 (relating to commissions or gifts for procuring loans), section 513 (relating to securities of States and private entities), section 641 (relating to public money, property, or records), section 656 (relating to theft, embezzlement, or misapplication by bank officer or employee), section 657 (relating to lending, credit, and insurance institutions), 658 (relating to property mortgaged or pledged to farm credit agencies), section 666 (relating to theft or bribery concerning programs receiving Federal funds), sections 793, 794, or 798 (relating to espionage), section 875 (relating to interstate communications), section 1201 (relating to kidnapping), section 1203 (relating to hostage taking), section 1344 (relating to bank fraud), or section 2113 or 2114 (relating to bank and postal robbery and theft), sections 2251, 2251A, 2252, and 2258 (relating to sexual exploitation of children); section 2319 (relating to copyright infringement); or section 2320 (relating to trafficking

in counterfeit goods and services); or 7 U.S.C. section 2024 (relating to food stamp fraud); 21 U.S.C. section 830 (relating to precursor chemicals), section 857 (relating to transportation of drug paraphernalia) and, with respect to a financial transaction occurring in whole or in part in the United States, an offense against a foreign nation involving the manufacture, importation, sale, or distribution of a controlled substance (as such term is defined for the purposes of the Controlled Substances Act); and any act or acts constituting a continuing criminal enterprise, as that term is defined in section 408 of the Controlled Substances Act (21 U.S.C. 848); or any act or activity constituting an offense listed in 18 U.S.C. 1961(1), with respect to any act or threat involving murder, kidnapping, gambling, arson, robbery, bribery, extortion, dealing in obscene matter, or in dealing in narcotics or other dangerous drugs which is chargeable under State law and punishable for more than one year; 18 U.S.C. 201 (bribery); 18 U.S.C. 224 (sports bribery); 18 U.S.C. 659 (theft from interstate shipment); 18 U.S.C. 664 (embezzlement from pension and welfare funds); 18 U.S.C. 891-894 (extortionate credit transactions); 18 U.S.C. 1029 (fraud and related activity in connection with access devices); 18 U.S.C. 1084 (the transmission of gambling information); 18 U.S.C. 1341 (mail fraud); 18 U.S.C. 1343 (wire fraud); 18 U.S.C. 1461-1465 (obscene matter); 18 U.S.C. 1503 (obstruction of justice); 18 U.S.C. 1510 (obstruction of criminal investigation); 18 U.S.C. 1511 (the obstruction of State or local law enforcement); 18 U.S.C. 1512 (tampering with a witness, victim or informant); 18 U.S.C. 1513 (retaliating against a witness, victim or informant); 18 U.S.C. 1951 (interference with commerce, robbery or extortion); 18 U.S.C. 1952 (racketeering, except with respect to untaxed paid liquor and arson); 18 U.S.C. 1953 (interstate transportation of wagering paraphernalia); 18 U.S.C. 1954 (unlawful welfare fund payments); 18 U.S.C. 1955 (the prohibition of illegal gambling businesses); 18 U.S.C. 1958 (use of interstate commerce facilities in the commission of murder-for-hire); 18 U.S.C. 2251, 2251A, 2252, and 2258 (sexual exploitation of children); 18 U.S.C. 2321 (trafficking in certain motor vehicles or motor vehicle parts); 18 U.S.C. 2312 and 2313 (interstate transportation of stolen motor vehicles); 18 U.S.C. 2314 and 2315 (interstate transportation of stolen property); 18 U.S.C. 2421-24 (white slave traffic); any act which is indictable under 29 U.S.C. 186 (restrictions on payments and loans to labor organizations) or 29 U.S.C. 501(c) (embezzlement from union funds); any offense involving fraud connected with a case under title 11, fraud in the sale of securities, and the felonious manufacture, importation, receiving, concealment, buying, selling, or otherwise dealing in narcotic or other dangerous drugs, punishable under any law of the United States."

(The above SUAs in Section 1956 and violations specified in Section

1961 are changed occasionally. See MIOG, Part I, 183-1.2 (for current RICO predicate offenses), 272-4, and 272-9 (for current SUAs).)

"2. Drug Enforcement Administration

"The Drug Enforcement Administration shall have investigatory jurisdiction over violations of sections 1956 or 1957 involving the specified unlawful activities of, with respect to a financial transaction occurring in whole or in part in the United States, an offense against a foreign nation involving the manufacture, importation, sale, or distribution of a controlled substance (as such term is defined for the purpose of the Controlled Substances Act) including 21 U.S.C. 830 (relating to precursor and essential chemicals) and 857 (relating to transportation of drug paraphernalia); or any act or acts constituting a continuing criminal enterprise, as that term is defined in section 408 of the Controlled Substances Act (21 U.S.C. 848); or any of the predicate offenses enumerated in 18 U.S.C. 1961(1) dealing in narcotics or other dangerous drugs which are chargeable under State law and punishable for more than one year, or the felonious manufacture, importation, receiving, concealment, buying, selling, or otherwise dealing in narcotics or other dangerous drugs, punishable under any law of the United States.

"C. United States Postal Service

"The investigative jurisdiction of the Postal Inspection Service is limited by 18 U.S.C. 3061 to offenses regarding property in the custody of the Postal Service, property of the Postal Service, use of the mails, other postal offenses, and offenses for which the Postal Service has been delegated investigative authority pursuant to 18 U.S.C. 3061 (b)(2). Subject to these limitations, the Postal Inspection Service shall have investigative jurisdiction over violations of sections 1956 and 1957 involving the specified unlawful activities of 18 U.S.C. 201 (bribery of public officials and witnesses); 18 U.S.C. 500-503 (counterfeiting of money orders, post cards, indicia of postage and postmarking stamps); 18 U.S.C. 641 (theft of public money, property or records); 18 U.S.C. 1029 (fraudulent activity in connection with access devices) with respect to violations involving postal employees, fraud against the Postal Service or where the primary focus of the offense is mail fraud or a violation of 18 U.S.C. 2114 (postal robbery); 18 U.S.C. 1341 (mail fraud); 18 U.S.C. 1343 (wire fraud) where the primary focus of the offense is mail fraud; 18 U.S.C. 1461 and 1463 (mailing of obscene matter); 18 U.S.C. 1503, 1510-1513 (obstruction of justice); 18 U.S.C. 1952 (mailing in aid of racketeering enterprises); 18 U.S.C. 1961

(1)(A) (organized crime); 18 U.S.C. 2114 (robbery of mail, other property); 18 U.S.C. 2251, 2252 (sexual exploitation of minors); any 18 U.S.C. 1961 (1) offense dealing in narcotics and other dangerous drugs which are chargeable under state law and punishable for more than one year, or by the felonious manufacture, importation, receiving, concealment, buying, selling, or otherwise dealing in narcotics or other dangerous drugs punishable under any law of the United States, or any act or acts constituting criminal enterprise, as that term is defined in section 408 of the Controlled Substances Act (21 U.S.C. 848); 21 U.S.C. 843 (b) (use of mails to violate Controlled Substances Act); and, Section 1822 of the Mail Order Drug Paraphernalia Control Act (21 U.S.C. 857) (transportation of drug paraphernalia).

"Section IV. Undercover Operations

"This MOU will govern the conduct of all money laundering investigations under sections 1956 and 1957 in that all parties hereto agree that all undercover operations will be reviewed using each bureau's internal guidelines, the objectives of which are consistent with existing Attorney General Guidelines on undercover operations.

"Section V. Seizure and Forfeiture

"Any property involved in a violation of section 1956 or 1957 that a Treasury or Justice bureau or the Postal Service has authority to investigate under Section III of this MOU may be seized by that bureau or the Postal Service, if that property is subject to forfeiture to the United States under 18 U.S.C. 981(a)(1)(A) or 981(a)(1)(B).

"Where a Treasury or Justice bureau or the Postal Service would have authority to seize property under the authority stated in the preceding paragraph is not present to make the seizure, any Treasury or Justice bureau or the Postal Service that is present may seize the property and shall immediately turn over that property to the bureau having Section III investigatory jurisdiction, where the forfeiture processing shall occur.

"Any property seized under this Section shall, upon forfeiture under 18 U.S.C. 981 or 982, be apportioned among the appropriate Treasury or Justice bureaus or the Postal Service in accordance with their respective contribution to the overall efforts expended in the investigation, seizure, or forfeiture.

"Pursuant to 18 U.S.C. 981(e) and, where appropriate, the Justice Department, the Treasury Department or the Postal Service forfeiture

guidelines, apportionment may include equitable transfers to any other Federal agency or State or local authorities, which participated directly in any of the acts which led to the seizure or forfeiture.

"Any dispute regarding the seizure, forfeiture, apportionment, or disposition of property under this section shall be governed by the disputes resolution procedure in Section IX of this MOU.

"This MOU does not affect Treasury or Justice bureaus' or the Postal Service's authority to seize property or the disposition of such property under statutory seizure and forfeiture provisions not based on section 1956 and 1957 violations.

"A. Seizure of Attorney Fees: Treasury and Justice bureaus and the Postal Service will follow DOJ guidelines in reference to the seizure and forfeiture of any money or property that is held by an attorney for payment for the defense of a client. See United States Attorneys Manual 9-111.000, et seq.

"Section VI. Prosecution

"A bureau that conducts an investigation under the authority of this MOU shall coordinate with Justice Department attorneys.

"Section VII. Notice, Coordination, and Lead Bureau

"A. Notice

"1. If, during the investigation of a section 1956 or 1957 violation, a bureau discovers a specified unlawful activity or a transaction reporting violation over which another bureau has investigatory jurisdiction, that bureau shall give notice to the bureau which has investigatory jurisdiction over the specified unlawful activity or to the Internal Revenue Service or Customs, as appropriate, in the case of a transaction reporting violation, and to consult prior to taking any investigative actions impacting on the other bureau's jurisdiction.

"2. If a bureau discovers transactions involving the proceeds of a specified unlawful activity conducted with intent to engage in a violation of section 7201 or 7206 of the Internal Revenue Code, that bureau shall give notice to the Internal Revenue Service and coordinate the subsequent investigation with the IRS. To the extent that any IRS money laundering investigation requires the acquisition of evidence concerning an underlying specified unlawful activity, the IRS shall notify the bureau having jurisdiction over the specified

unlawful activity and coordinate the subsequent investigation with that bureau.

"3. Notice under this section will ordinarily be made at supervisory field level and will, at a minimum, require a complete summary of the facts and circumstances of the investigation. However, in those instances where a bureau undertakes an investigation in which it determines that field level disclosure would be detrimental to the investigation, the required notice will be made at the headquarters level and dissemination restricted to selected individuals consistent with the need to maintain security of the investigations.

"B. Coordination and Determination of Lead Bureau

"Investigatory actions which involve areas outside the investigating bureau's existing jurisdiction, independent of the money laundering statute, shall be conducted only in coordination with the bureau(s) which do have existing jurisdiction independent of the money laundering statute. Coordination requires, at a minimum, a determination of the degree of cooperation necessary between the coordinating bureau(s) and includes continuing dialogue as the case develops. At the request of any coordinating bureau, at any time as the case develops, there shall be a determination of the lead bureau for the Section 1956 or 1957 investigation. The determination of lead bureau does not preclude a subsequent request by a coordinating bureau for redetermination of the lead as compelling facts and circumstances warrant.

"The determination of the lead bureau will be made at the supervisory field level by the bureaus involved and will be governed by which bureau has the paramount investigatory interest. In determining which bureau has the paramount investigatory interest, the factors to be considered shall include, but not be limited to:

- Likely impact on major criminal enterprises;
- Likelihood of successful prosecution;
- Existence of a specified unlawful activity, as defined in section 1956(c)(7);
- Jeopardy to informants, undercover agents, or third parties;
- Commitment of investigatory resources; and

- Any other matter of substantive investigative interest.

"Section VIII. Jointly Conducted Investigations

"Treasury and Justice bureaus and the Postal Service are encouraged to enter into joint investigatory endeavors in circumstances that may necessitate or justify the use of skills and resources of more than one bureau. The specific details of each joint investigation, including the role of each bureau in the endeavor, will be formulated at the onset of the investigation and will be provided to each bureau's headquarters by each bureau's established procedures. While differing circumstances will result in varied arrangements from project to project, certain conditions will always apply:

- Participating personnel will be supervised by their respective bureaus. This does not alter any other concerning supervision of investigatory personnel.

- Only one evidentiary document, such as a record of interview will be prepared, and a copy will be furnished to the other bureau at the time the document is prepared.

- Resources and investigatory expertise will be provided to the requesting bureau when the investigatory matter meets the criteria of the requested bureau and when available resources allow.

- Any contact with the news media, such as press releases, will be coordinated and agreed to in advance by the bureaus involved.

"Section IX. Dispute Resolution

"The Secretary, the Attorney General and the Postmaster General contemplate that in cases of overlapping jurisdiction, the appropriate bureaus will work in concert to the extent authorized by law. Any disputes between bureaus should be resolved at the field level. When this cannot be accomplished, the matter will be referred to the respective headquarters' point of contact. In the event that disputes cannot be resolved by the bureau headquarters, the matter will be expeditiously referred to the Assistant Attorney General, Criminal Division, Department of Justice, and the Assistant Secretary for Enforcement, Department of the Treasury, and in disputes involving the Postal Service, to the Chief Postal Inspector, whose decisions shall

be final.

"Section X. Extraterritorial Jurisdiction

"Treasury and Justice bureaus and the Postal Service must immediately notify the appropriate prosecuting attorney or other designated Department of Justice official if, in the course of a section 1956 or section 1957 investigation, it becomes likely that extraterritorial jurisdiction under section 1956(f) or section 1957(d) will be invoked. See United States Attorneys Manual 9-105.100.

"Section XI. Amendment

"This MOU may be amended by deletion or modification of any provision contained herein, or by addition of new provisions, after written concurrence of all the parties to the MOU.

"Section XII. Termination

"This MOU will remain in effect until terminated by the Attorney General or the Secretary or the Postmaster General upon 30 days' written notice.

"Section XIII. Approval

"This MOU becomes effective when approved by the parties identified below.

Peter K. Nunez
Assistant Secretary (Enforcement)
U.S. Department of Treasury

JUL 31 1990
Date

William P. Barr
Deputy Attorney General
U.S. Department of Justice

8/11/90
Date

Charles R. Clauson
Charles R. Clauson
Chief Postal Inspector

8/16/90

Date"

EFFECTIVE: 10/02/96