SECRET

FEDERAL BUREAU OF INVESTIGATION

United States Department of Justice

REVISED

NATIONAL FOREIGN INTELLIGENCE PROGRAM MANUAL (NFIPM)

(Original issue April 29, 2002)

Last Updated: 03/22/06

This manual will be revised periodically. The "Updated" date above reflects the date the most recent revisions were inserted into the manual; however, the date does not imply that all citations were revised on that date. As new and/or revised policy/procedures are developed, substantive divisions will advise FBI employees by appropriately classified electronic communications (ECs). The ECs' authors or substantive units will then submit appropriate changes to this manual.

Section 1 (U) Mission Statement, The National Security List, Acronyms, and File Classifications

Section 1-01 (U) Mission Statement

A. (U) The President has instructed the FBI to:

1. Conduct foreign counterintelligence and counterterrorism activities within the United States, and to coordinate similar activities of other agencies within the U.S. Intelligence Community;

2. Conduct foreign counterintelligence and counterterrorism activities outside the United States, in coordination with the CIA;

3. Conduct foreign intelligence activities, and support foreign intelligence collection requirements of other agencies within the U.S. Intelligence Community, and to support the communications security activities of the U.S. Government, as requested;

4. Produce and disseminate foreign counterintelligence, international terrorism and foreign intelligence information; and

5. [redacted]

B. (S) [redacted]

b2
b7E
b1

C. (U) In keeping with the foregoing, the FBI's National Foreign Intelligence Program seeks to:

1. Detect and prevent intelligence and international terrorism activities conducted in the United States by or on behalf of foreign powers;

2. Investigate violations of the espionage statutes (irrespective of whether such violations are committed at the direction of foreign powers);

3. Conduct within the United States activities in support of the foreign intelligence collection requirements of other U.S. Intelligence Community agencies when requested by officials within the U.S. Intelligence Community designated by the President to make such requests;

4. Collect foreign intelligence within the United States when requested by officials within the U.S. Intelligence Community designated by the President to make such requests;

5. Disseminate foreign counterintelligence, foreign intelligence and international terrorism information reports and studies to appropriate Federal agencies and foreign governments;

6. Coordinate all foreign counterintelligence activities conducted within the United States by other agencies within the U.S. Intelligence Community;

7. Request appropriate U.S. Government and foreign government agencies to conduct investigations outside the United States in connection with matters falling inside the FBI's jurisdiction;

8. Conduct certain investigations within the United States at the request of foreign government law enforcement, security and intelligence agencies; and

9. Conduct foreign counterintelligence, foreign intelligence and international terrorism activities outside the United States, in coordination with the CIA.

D. (U) In managing the FBI's National Foreign Intelligence Program, the Counterintelligence Division,, Counterterrrorism Division and Investigative Services Division have five priorities: (a) foreign counterintelligence; (b) international terrorism; (c) foreign intelligence; (d) security countermeasures and (e) the proper handling of classified National Security information and materials.

E. (U) This Manual specifically addresses three of those priorities: (a) foreign counterintelligence; (b) international terrorism; and (c) foreign intelligence.

F. (U) As respects classification matters, see: the Manual of Investigative Operations and Guidelines, Sections Part II, Sections 26-1 thru 26-14. As respects security countermeasures, see: the Manual of Investigative Operations and Guidelines and the Manual of Administrative Operations and Procedures, Scattered Sections.

EFFDATE: 04/29/2002 MCRT# 1262 Div. ~~D5 Cav:~~ SecClass: Secret

Section 1-02 (U) The National Security List

A. (U) [redacted] generally defines the types of investigative activities which are engaged in with respect to the FBI's National Foreign Intelligence Program. [redacted]

b2
b7E

[redacted] It is constantly evaluated in the light of U.S. National Security needs; and it is subject to a yearly updating process [redacted] may be added and/or removed. [redacted]

B. (U) [redacted] are of such concern to U.S. National Security interests that foreign counterintelligence, international terrorism and/or intelligence gathering activities concerning them are warranted.

b2
b7E

C. [redacted] which pose such threats to U.S. National Security interests that foreign counterintelligence, international terrorism and/or intelligence gathering activities concerning them are warranted.

D. (U) [redacted]

EFFDATE: 04/29/2002 MCRT# 1262 Div. D5 Cav. SecClass: Unclassified

Section 1-03 (U) Acronyms

A. U.S. Government Agencies

(U) AFOSI: Air Force Office of Special Investigations

(U) AG: Attorney General

(U) ATF: Bureau of Alcohol, Tobacco and Firearms

(U) CIA: Central Intelligence Agency

(U) DCI: Director of Central Intelligence

(U) DIA: Defense Intelligence Agency

(U) DISCO: Defense Industrial Security Clearance Office

(U) DOC: Department of Commerce

(U) DOD: Department of Defense

(U) DOE: Department of Energy

(U) DOJ: Department of Justice

(U) DOS: Department of State

(U) DOT: Department of Transportation

(U) DTRA: Defense Threat Reduction Agency

(U) FEMA: Federal Emergency Management Agency

(U) GSA: General Services Administration

(U) INS: Immigration and Naturalization Service

(U) INSCOM: Army Intelligence and Security Command

(U) JCS: Joint Chiefs of Staff

(U) MCIS: Military Counterintelligence Service

(U) NACOB: National Counterintelligence Operations Board

(U) NACIPB: National Counterintelligence Policy Board

(U) NCIS: Naval Criminal Investigative Service

(U) NFIB: National Foreign Intelligence Board

(U) NHRTC: National HUMINT Requirements Tasking Center, CIA

(U) NRC: Nuclear Regulatory Commission

(U) NRD: National Resources Division, CIA

(U) NSA: National Security Agency

(U) NSC: National Security Council

(U) NSTISSC: National Security Telecommunications and Information Systems Security Command

(U) OFAC: Office of Foreign Asset Control

(U) OIPR: Office of Intelligence Policy and Review, DOJ

(U) OMB: Office of Management and Budget

(U) OSD: Office of the Secretary of Defense

(U) TECS: The Treasury Enforcement Communication Service

(U) USCS: United States Customs Service

(U) USIA: United States Information Agency

(U) USIC: United States Intelligence Community

B. FBI terms

(U) AO: Auxiliary Office

(U) CD: Counterintelligence Division, FBI (formerly NSD)

(U) CIS: The Central Index System

(U) [redacted]

(U) CTD: Counterterrorism Division, FBI

(U) [redacted]

(U) ELSUR: Electronic Surveillance

(U) [redacted]

(U) FISA: Foreign Intelligence Surveillance Act

(U) [redacted]

(U) III: Interstate Identification Index

(U) [redacted]

b2
b7E

(U) IS: Investigative Specialist

(U) ISD: Investigative Services Division, FBI

(U) [redacted]

(U) [redacted]

(U) MOU: Memorandum of Understanding

(U) NDPO: National Domestic Preparedness Office, FBI

(U) NFIP: National Foreign Intelligence Program

(U) NIPC: National Infrastructure Protection Center, FBI

(U) NIPCIP: National Infrastructure Protection and Computer Intrusion Program

(U) NSL: National Security Letter

(U) OGC: Office of the General Counsel, FBI

(U) OO: Office of Origin

(U) [redacted]

(U) [redacted]

(U) UCSA/USCP: Undercover Special Agent/Undercover Support Person

(U) WFO: Washington Field Office, FBI

C. General Terms

(U) CI: Counterintelligence

(U) COMSEC: Communications Security

(U) CT: Counterterrorism

(U) [redacted]

(U) FCI: Foreign Counterintelligence

(U) FIS: Foreign Intelligence Service

(U) HUMINT: Human Intelligence

(U) IC: Intelligence Community

(U) IO: Intelligence Officer

(U) IT: International Terrorism

b2
b7E

(U) MOU: Memorandum of Understanding

(U) NFPO: No Foreign Policy Objection

(U) PNG: Persona Non Grata

(U) PRA: Permanent Resident Alien

(U) RFPA: Right to Financial Privacy Act

(U) [redacted]

(U) SCI: Sensitive Compartmented Information

(U) SCIF: Sensitive Compartmented Information Facility

(U) SIGINT: Signals Intelligence

(U) SRAC: Short Range Agent Communication

(U) UC: Undercover

(U) USPER: United States Person

(U) WMD: Weapons of Mass Destruction

EFFDATE: 04/29/2002 MCRT# 1262 Div: D5 ~~Cav:~~ ~~SecClass: Unclassified~~

Section 1-04 (S) [redacted]

(S) [redacted]

b1
b2
b7E

(S) 4. [redacted]

EFFDATE: 04/29/2002 MCRT# 1262 Div: D5 Cav: SecClass: Secret

Outside the Scope

Section 2-15 (U) [redacted]

A. (S) [redacted]

EFFDATE: 01/17/2003 MCRT# 1273 Div: D5 Cav: SecClass: Secret

Section 2-16 (U) Monitoring Devices Which Do Not Impose Upon Reasonable Expectations of Privacy

A. (U) See: Section 2-04, supra.

EFFDATE: 04/29/2002 MCRT# 1262 Div: D5 Cav: SecClass: Unclassified

Section 2-17 (U) Financial Records

A. (U) Financial institutions must comply with requests for customers' or entities' financial records which are made by the Director; the Deputy Director; the Assistant and Deputy Assistant Directors of CD/CTD; the general Counsel and the deputy General Counsel for National Security Affairs; ADICs and all SACs of the New York, Washington, D.C., and Los Angeles field offices; and SACs in all other field offices, generally by means of a National Security Letter (NSL).

1. Such requests must certify that the information is relevant to an authorized investigation to protect against IT or clandestine intelligence activities, provided that such an investigation of an USPER is not conducted solely on the basis of activities protected by the First Amendment of the U.S. Constitution. See: Title 12, USC, Section 3414(a)(5)(A).

B. (U) Though not required to do so, financial institutions may also comply with requests for financial records which are made by SACs or ASACs.

1. Such requests must clearly indicate that releases pursuant thereto are voluntary. See: id. Section 3414(a)(1).

C. (U) To expedite their processing, requests submitted to FBI Headquarters or to SACs should include:

1. The subject's full name and address and an indication whether he/she is an USPER;

2. The date the investigation was initiated;

3. A summary of the investigation's predication;

4. A succinct description of the information desired; and

5. The name, title and address of the financial institution representative who should receive the request.

D. (U) Whichever of the foregoing means is utilized, recipient financial institutions must be advised that the requests may not be disclosed. See: id. Section 3414(a)(3) and (a)(5)D).

E. (U) On a semiannual basis, the FBI must fully inform the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence of requests made by the foregoing means. See: id. Section 3414(a)(5)(C).

F. (U) Unless it relates to violations of Federal, State or local statutes, information acquired by the foregoing means must be destroyed if found not relevant to foreign counterintelligence, foreign intelligence or international terrorism concerns. All disseminations of such information must be accompanied by a statement that further disseminations must first be cleared with FBI Headquarters. See: Attorney General Guidelines for FBI Foreign Intelligence Collection and FCI Investigations, Sections III.F and VII.B.5.

EFFDATE: 04/29/2002 MCRT# 1262 Div: D5 Cav: SecClass: Unclassified

Section 2-18 (U) Consumer Reporting Agency Records

A. (U) Consumer reporting agencies must comply with requests for the names and addresses of financial institutions at which consumers maintain or have maintained accounts, which are made by the Director; the Deputy Director; the Assistant and Deputy Assistant Directors of CD/CTD; the general Counsel and the deputy General Counsel for National Security Affairs; ADICs and all SACs of the New York, Washington, D.C., and Los Angeles field offices; and SACs in all other field offices, generally by means of a National Security Letter (NSL).

1. Such requests must certify that the information is relevant to an authorized investigation to protect against IT or clandestine intelligence activities, provided that such an investigation of an USPER is not conducted solely on the basis of activities protected by the First Amendment of the U.S. Constitution. See: Title 15, USC, Section 1681u(a).

B. (U) Consumer reporting agencies must also comply with requests made by the Director or his/her designee, for consumers' identifying information.

1. Customers' identifying information is limited to names, addresses, former addresses, places of employment and former places of employment.

2. Requests must certify that the information is necessary for the conduct of authorized foreign counterintelligence, foreign intelligence or international terrorism investigations and that there is reason to believe that the consumers have been or are

about to be in contact with foreign powers or agents of foreign powers. See: id. Section 1681u(b).

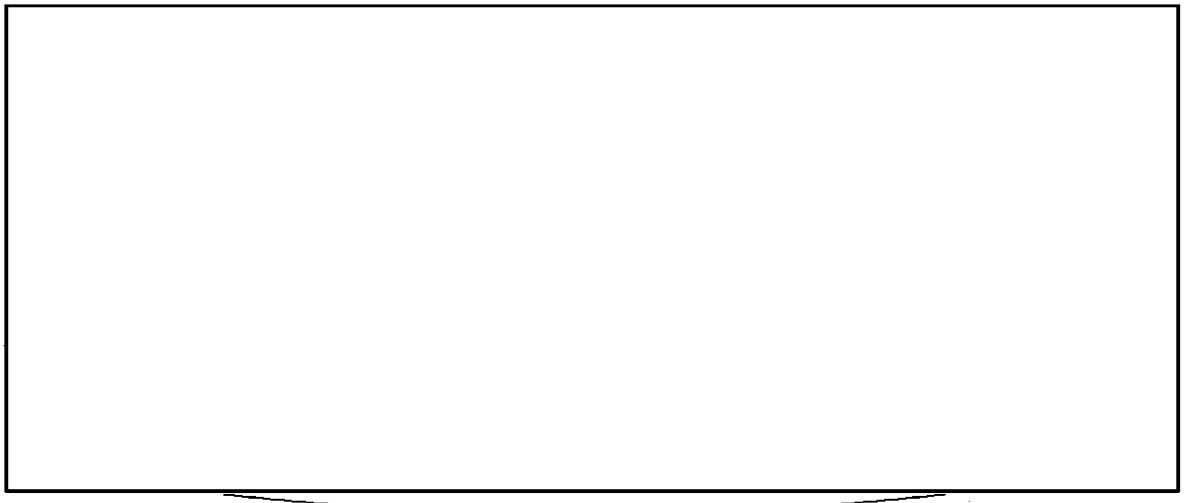
C. (U) Further, at the request of the Director or his/her designee, Federal Courts may issue ex parte orders, directing consumer-reporting agencies to furnish consumer reports.

1. Orders may be issued upon showings that: consumer reports are necessary for the conduct of authorized foreign counterintelligence, foreign intelligence or international terrorism investigations; and there are specific and articulable facts giving reason to believe that the consumers are agents of foreign powers, and that they are or have engaged in international terrorism acts or clandestine intelligence activities that do or may involve violations of Federal criminal statutes. See: id. Section 1681u(c).

D. (U) Records so obtained may only be disseminated to other Federal agencies and Military Counterintelligence Services as necessary in connection with foreign counterintelligence, foreign intelligence or international terrorism investigations. See: id. Section 1681u(f).

E. (U) On a semiannual basis, the Attorney General must inform the House Permanent Select Committee on Intelligence; the House Committee on Banking, Finance and Urban Affairs; the Senate Select Committee on Intelligence and the Senate Committee on Banking, Housing, and Urban Affairs of requests made by the foregoing means. See: id. Section 1681u(h).

EFFDATE: 04/29/2002 ~~MCRT# 1262 Div. D5 Cav:~~ ~~SecClass: Unclassified~~



EFFDATE: 04/29/2002 MCRT# 1262 ~~Div. D5 Cav:~~ SecClass: Unclassified Outside the Scope

EFFDATE: 04/29/2002 MCRT# 1262 Div. D5 Cav: SecClass: Unclassified

Section 2-48 (U) Disseminating Information to the Federal Judiciary

A. (U) Justices of the U.S. Supreme Court, and Judges of the U.S. Courts of Appeal and District Courts do not require a determination of eligibility for access to classified information. Federal Magistrate Judges and all other Judicial personnel, however, must be determined eligible by the DOJ Security Officer. See: 28 Code of Federal Regulations Section 17.46(c).

EFFDATE: 04/29/2002 MCRT# 1262 Div. D5 Cav: SecClass: Unclassified

Section 2-49 (U)

A. (S)

EFFDATE: 04/29/2002 MCRT# 1262 Div. D5 Cav: SecClass: Secret

b1

Section 2-50 (U) Disseminating Information to Foreign Governments, and Investigations at their Behest

A. (S)

B. (U)

C. (U) The dissemination of information which may significantly affect foreign relations must be coordinated with the DOS. See: id. Section VII.B.2.c.

EFFDATE: 04/29/2002 MCRT# 1262 Div: D5 Cav: SecClass: Secret

Section 2-51 (U) Disseminating Information to State and Local Government Agencies

A. (U) Information relating to crimes may be disseminated to State and local governments with appropriate jurisdiction, if such dissemination is consistent with U.S. National Security interests. See: id. Section VII.B.2.b.

1. Information disseminated to State and local government agencies must include statements that the information may be used for evidentiary purposes only with the express written approval of DOJ, after consultation with the FBI.

B. (U) Classified information may not be disseminated to representative of State or local government agencies unless it can be ascertained that they possess appropriate security clearances. See: Manual of Administrative Operations and Procedures, Section 9-3.1.3.

EFFDATE: 04/29/2002 MCRT# 1262 Div: D5 Cav: SecClass: Unclassified

Section 2-52 (U) Disseminating Information to the Private Sector

A. (U) Classified information may not be disseminated to individuals in the private sector, unless it can be ascertained that they possess appropriate security clearances.

EFFDATE: 04/29/2002 MCRT# 1262 Div: D5 Cav: SecClass: Unclassified

Section 2-53 (U) Data Collection Method for Foreign Counterintelligence, Foreign Intelligence and International Terrorism Statistics

A. (U) An automated method is utilized for collecting information regarding FBI National Foreign Intelligence Program investigative accomplishments.

1. When claiming an accomplishment [redacted] must be used to present both required data elements and supporting narratives.

2. [redacted]

b2
b7E

B. (U) All persons involved in foreign counterintelligence, foreign intelligence and international terrorism investigations may claim investigative accomplishments.

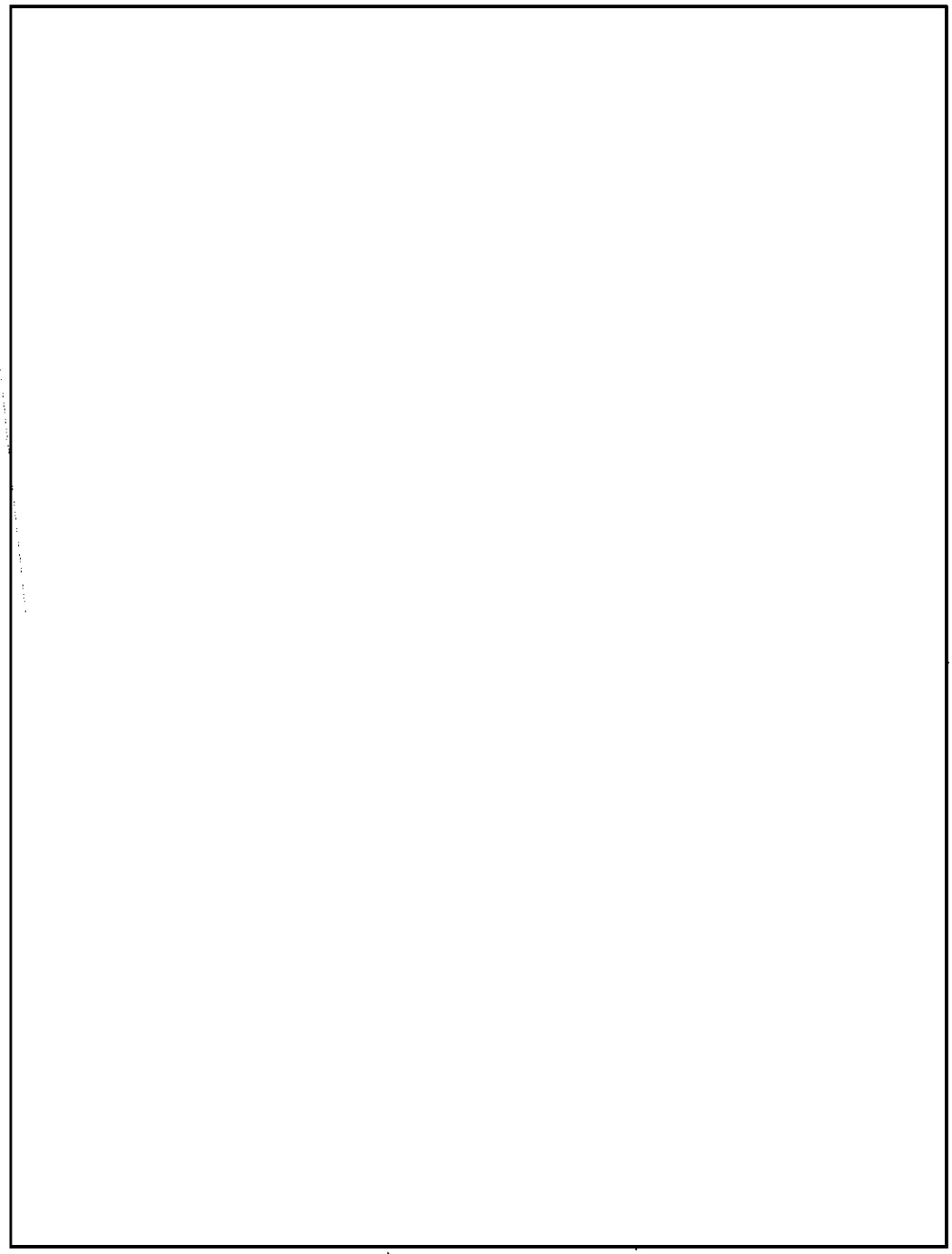
C. (S)

b1
b2
b7E

(S)

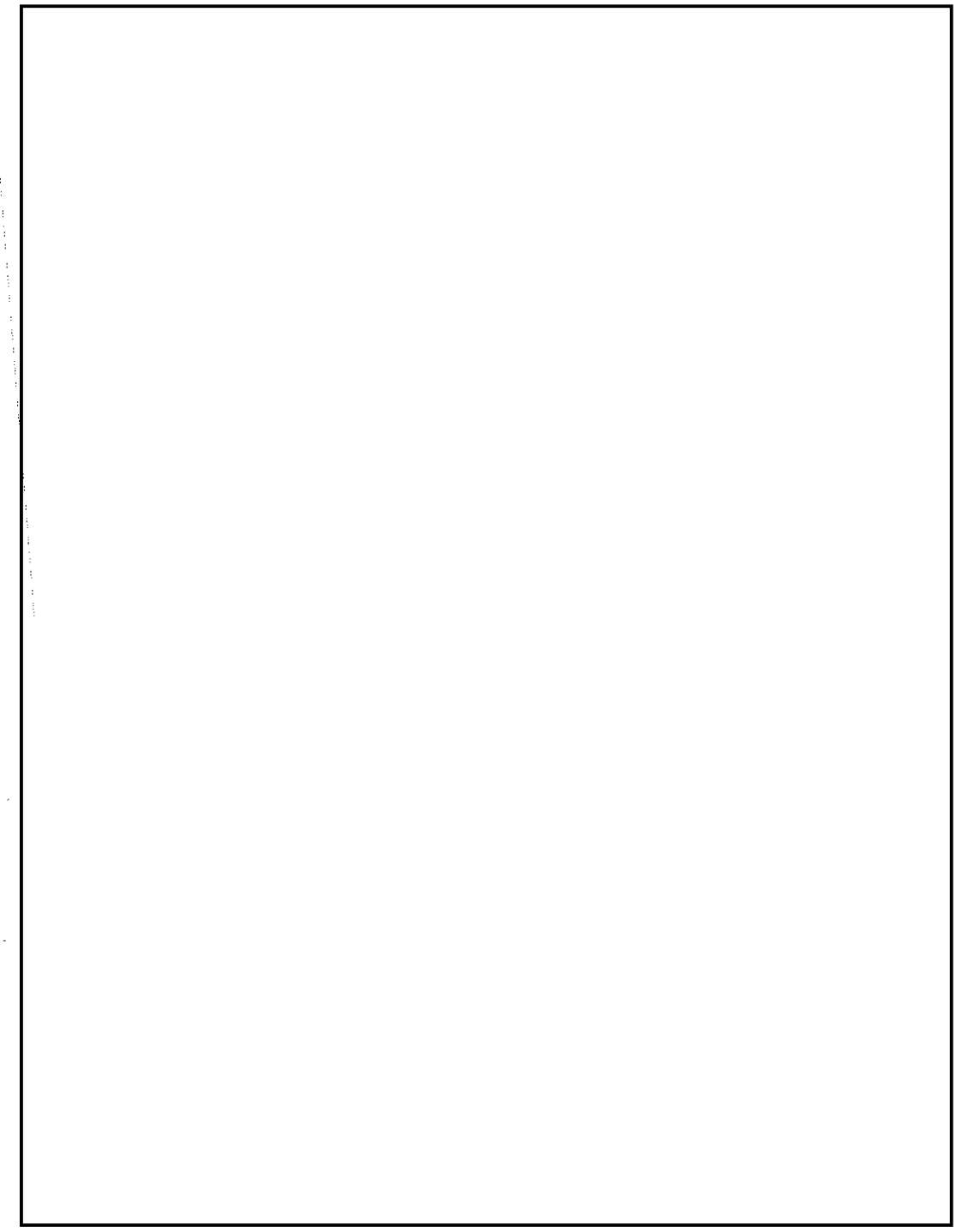
b1
b2
b7E

(S)



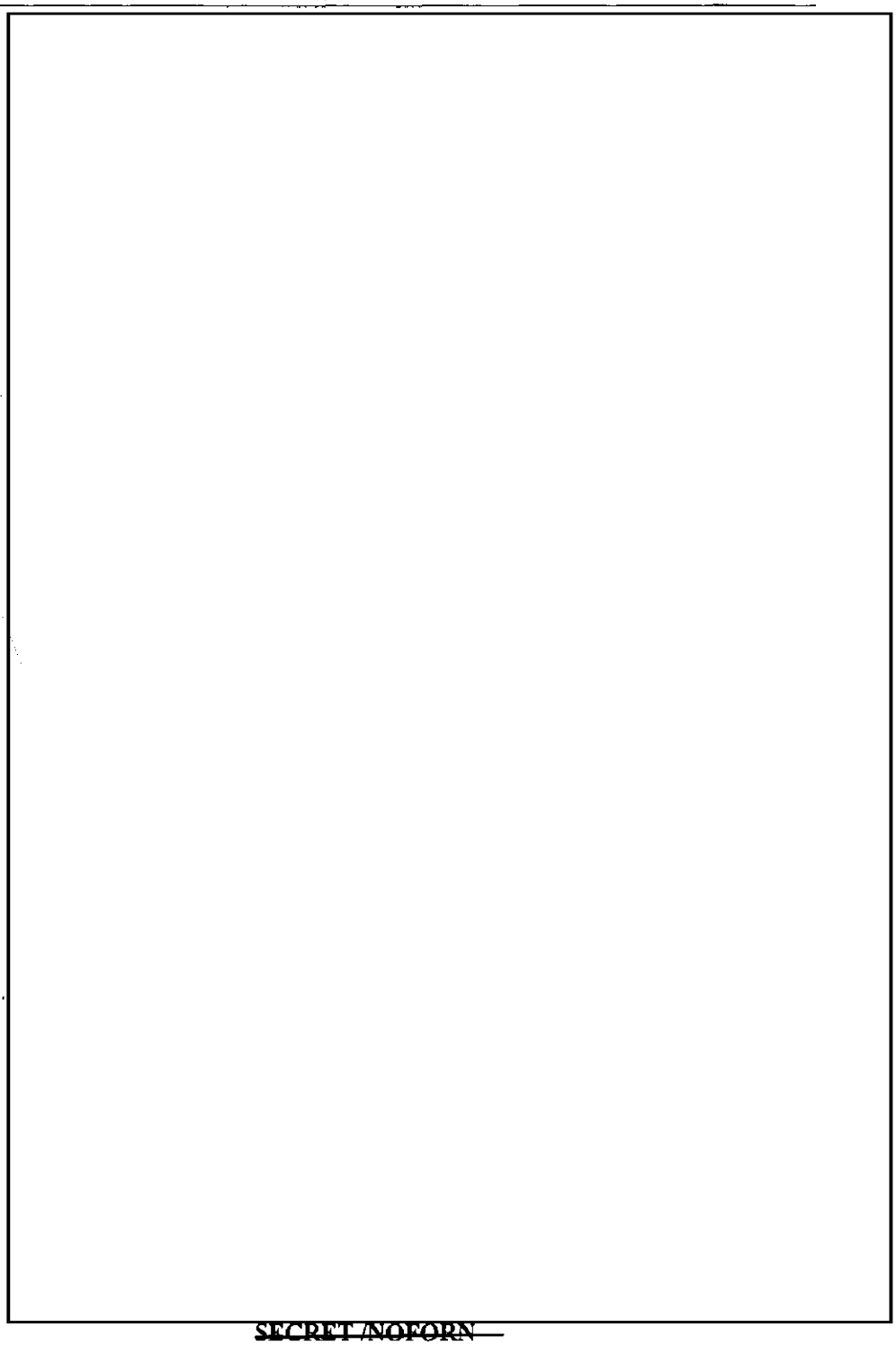
b1
b2
b7E

(S)



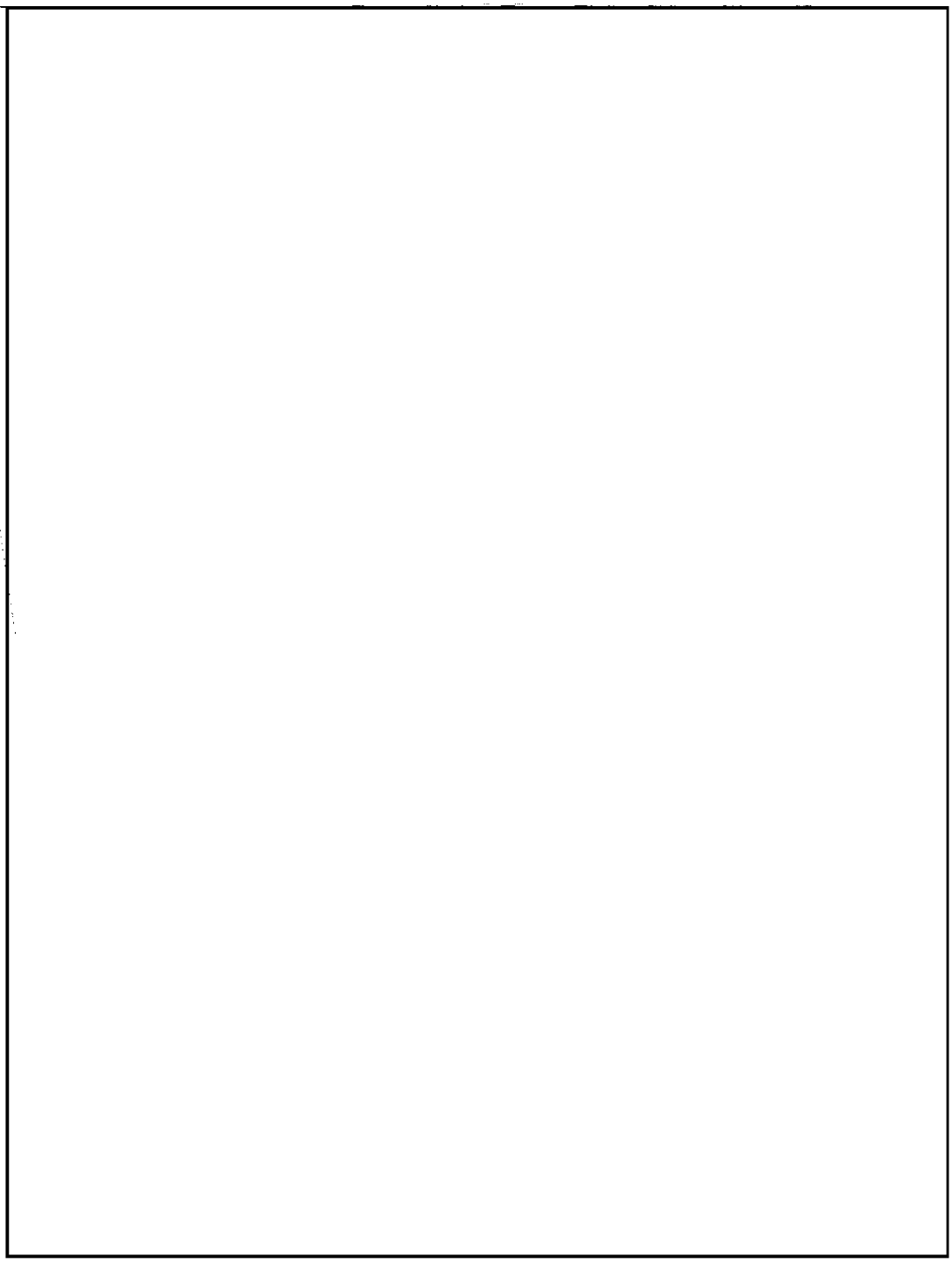
b1
b2
b7E

(S)



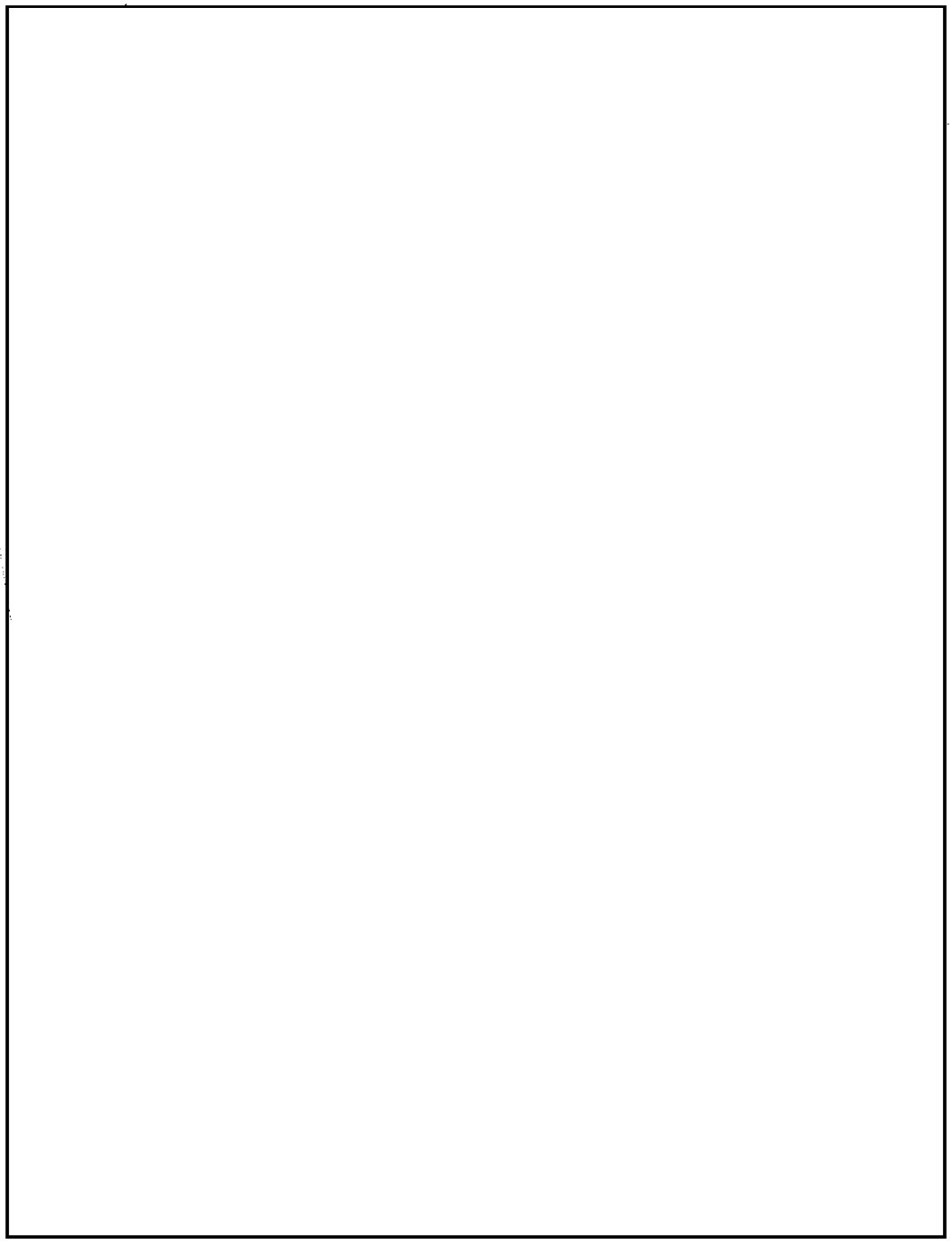
b1
b2
b7E

(S)



b1
b2
b7E

(S)



b1
b2
b7E

(S)

b1
b2
b7E

EFFDATE: 04/29/2002 MCRT# 1262 Div: D5 Cav: SecClass: Secret

Section 2-54 (U)

A. (U) is used to

See: Manual, Part A, Section 1.

B. (U) permits information to be

C. (U) are controlled by FBI Headquarters

b2
b7E

D. (U) Additional types of data available

E. (U) Additional automated information systems available at FBI Headquarters and/or select field offices include

EFFDATE: 04/29/2002 MCRT# 1262 Div: D5 Cav: SecClass: Unclassified

Section 2-55 (U) President's Foreign Intelligence Advisory Board Matters

A. (U) The PFIAB is a body of not more than 16 persons who are not employed by the Government, who are appointed by the President, and who are charged with assessing the quality and adequacy of: (a) intelligence collection, (b) intelligence analyses and estimates, and of (c) foreign counterintelligence and other intelligence activities. It is authorized to review the performance of all agencies within the U.S. Intelligence Community. See: Executive Order 12863, Section 1.2.

Outside the Scope

EFFDATE: 04/29/2002 MCRT# 1262 Div: D5 Cav: SecClass: Unclassified

[Section 2-56 (U) Intelligence Oversight Board Matters [(Case [Identification Number 278-HQ-C1229736-VIO)]

[A. (U) [Background. The Intelligence Oversight Board (IOB) was established as [a standing committee of the President's Foreign Intelligence Advisory Board by Executive [Order (EO) 12863 dated September 13, 1993. Among its other responsibilities, the IOB [has been given authority to review the FBI's practices and procedures relating to foreign [intelligence and foreign counterintelligence collection. Within the FBI, the "IOB process" [is the means by which the FBI reports to the IOB intelligence activities conducted by the [FBI which may have been unlawful or contrary to Executive Orders, Presidential [Directives, Departmental guidelines or the investigative procedures set forth in this [manual.

[(U) Section 2.4 of EO 12863 requires that the Inspectors General and General [Counsel of the Intelligence Community components report to the IOB "concerning [intelligence activities that they have reason to believe may be unlawful or contrary to [Executive order or Presidential directive." This language was adopted verbatim from EO [12334 when the IOB was known as the President's Intelligence Oversight Board (PIOB). [By longstanding agreement between the FBI and the IOB (and its predecessor, the [PIOB), this language has been interpreted to mandate the reporting of any violation of a [provision of the foreign counterintelligence guidelines or other guidelines or regulations [approved by the Attorney General, in accordance with EO 12333, if such provision was [intended to protect the individual rights of a United States person. Counsel for [Intelligence Policy, Office of Intelligence Policy and Review (OIPR), Department of [Justice (DOJ), has further opined that the words "may be unlawful" in the Executive [Order should be interpreted to include violations of agency procedures issued under the [Executive Order, unless they involve purely administrative matters.]

[B. (U) [Obligation to Report Potential IOB Matters. FBI employees have an [obligation to report potential IOB matters within 14 days of the discovery of a possible [error or violation. The failure to report such matters, for whatever reason, may result in [severe disciplinary action, up to and including dismissal from the FBI.]

[C. (U) [Reporting Procedures. National Security Law Branch (NSLB), Office of [the General Counsel (OGC), is responsible for coordinating all reporting procedures [relating to possible IOB matters. FBI Headquarters (FBIHQ) divisions and field offices [are responsible for monitoring intelligence activities and reporting possible IOB matters to [OGC as discussed in this section.

[(U) Reports of potential IOB Matters are to be reported to OGC (Attn: NSLB) by [electronic communication (EC), uploaded into Case ID # 278-HQ-C1229736-VIO, and [include the following information:

[1. identification of the substantive investigation in which the questionable

activity occurred;

2. identification of the target by name [redacted]

3. identification of the subject's [redacted] status as a United States (U.S.) person or non-U.S. person;

4. a statement concerning the controlling legal authority for the investigation or the administrative requirements of the NFIPM that pertain (for example: "The Foreign Intelligence Surveillance Court authorized an electronic surveillance [redacted]

5. a statement of the error believed committed and when it occurred (including, in instances of delayed reporting, an explanation for the delayed submission).

EC reports of potential IOB matters must be signed out by the ADIC/SAC or Assistant Director, as appropriate. FBI personnel are encouraged to call NSLB concerning questions as to what is required or should be included in initial reports of IOB matters.]

D. (U) [Quarterly Reports. In addition to the foregoing, on a quarterly basis, each field office and FBIHQ division is required to submit to OGC (Attn: NSLB) an EC certifying that all employees of the office or division were contacted concerning the requirement to report possible IOB matters. (See MAOP, Part 1, 1-22.) The canvassing of employees may be accomplished by e-mail within field offices and FBIHQ divisions. EC certifications to OGC may be signed out by an ASAC or Deputy Assistant Director, as appropriate.]

E. (U) [Action by Inspection Division (INSD). IOB errors or other suspected violations of Executive Orders, Presidential Directives, Departmental guidelines or other regulations approved by the Attorney General in accordance with EO 12333, detected by INSD through case reviews or other inspection procedures, shall be reported to OGC within 14 days of discovery.]

F. (U) [Action by OGC. OGC shall review reports of potential IOB matters to determine if a reported error or violation requires notification to the IOB based on the requirements of EO 12863 and guidance previously provided by the IOB and OIPR. If the reported matter is determined to require such notification, OGC will prepare the necessary correspondence to the IOB setting forth the basis for the notification. That correspondence will be signed by the General Counsel or the General Counsel's designee and then be hand carried to the IOB. A copy of the correspondence will also be sent to [redacted] and to [redacted] for action deemed appropriate. Copies of that correspondence will also be delivered to the Office of the Attorney General, Department of Justice (DOJ); the Office of Professional Responsibility, DOJ; and the Office of Intelligence Policy and Review, DOJ. The reporting ADIC/SAC or Assistant Director will also be notified if a potential IOB matter was determined by OGC not to require notification to the IOB.

b2
b7E

b2
b7E

(U) Reports of potential IOB matters determined by OGC not to require notification to the IOB will be retained by OGC for three years for possible review by the Counsel to the IOB, together with a statement concerning the basis for the determination that notification was not required.]

G. [(S)

1. (S)

2. (S)

b1
b2
b7E

3. (U) Initiating a form of electronic surveillance or a search without authorization from the Foreign Intelligence Surveillance Court (FISC), or failing to terminate an authorized surveillance at the time prescribed by the Court. (See Title 50, USC, Sections 1805, 1824.)

4. (U) Failing to adhere to the minimization or dissemination requirements specified in a FISC Order. (See Title 50, USC, Section 1806.)]

H. [(S)

EFFDATE: 03/08/2004 MCRT# 1324 Div. D9D5 Cav: SecClass: Secret

Section 2-57 (U) Alpha Designations

A. (U) Alpha designators are part of the Time Utilization Recordkeeping System, which is designed to identify time utilization of investigative personnel.

B. (U) See: Section 1-04, supra.

EFFDATE: 04/29/2002 MCRT# 1262 Div. D5 Cav: SecClass: Unclassified

NFIPM Section 3 (U) Electronic Surveillances and Unconsented Physical Searches

Section 3-01 (U) Consensual Monitoring

A. (U) Monitoring that would constitute an ELSUR under the FISA statute, but for the lawful consent of a party to the monitored communication, must be personally approved by SACs, or FCI/Foreign Intelligence/IT ASACs in certain large field offices. Those field offices are as follows: New York, Washington Field, Chicago, San Francisco, Los Angeles, Atlanta, Baltimore, Boston, Cleveland, Detroit, Houston, Miami, Newark and Philadelphia.

1. Authorizations may be for periods of up to 90 days. *See: Attorney General Guidelines for FBI Foreign Intelligence Collection and FCI Investigations, Section IV.F.*

EFFDATE: 04/29/2002 ~~MCRT# 1262 Div: D5 Cav: SecClass: Unclassified~~

Section 3-02 (U) Volunteered Tape Recordings

A. (U) Volunteered non-FBI ELSUR recordings should be retained for reasonable periods of time. Their receipt should be documented in case files.

B. (U) If determined to be non-relevant to FBI concerns, contributors should be requested to retrieve them within specified reasonable periods of time. If not retrieved, they may be destroyed.

C. (U) The disposition of volunteered tape recordings should be appropriately documented (e.g., via FD-597s and FD-192s).

EFFDATE: 04/29/2002 MCRT# 1262 ~~Div: D5 Cav:~~ SecClass: Unclassified

Section 3-03 (U) Telephone Subscriber, Toll and Transactional Records

A. (U) Wire and electronic communication service providers must comply with requests for telephone subscriber and toll billing records or electronic communication transactional records which are made by the Director; the Deputy Director; the Assistant and Deputy Assistant Directors of CD/CTD; the general Counsel and the deputy General Counsel for National Security Affairs; ADICs and all SACs of the New York, Washington, D.C., and Los Angeles field offices; and SACs in all other field offices, generally by means of a National Security Letter (NSL). *See: Title 18, U.S. Code, Section 2709(a).*

1. Requests for telephone subscriber information must certify that the information is relevant to an authorized investigation to protect against IT or clandestine intelligence activities, provided that such an investigation of an USPER is not conducted solely on the basis of activities protected by the First Amendment of the U.S. Constitution. *See: id. Section 2709(b)(2).*

2. Requests for telephone subscriber information and toll records must certify that the information is relevant to an authorized investigation to protect against IT or clandestine intelligence activities, provided that such an investigation of an USPER is not conducted solely on the basis of activities protected by the First Amendment of the U.S. Constitution. *See: id. Section 2709(b)(1).*

3. To expedite processing, all requests submitted to FBI Headquarters should include:

a) The subject's full name, and whether he/she is an USPER;

b) The date the investigation was initiated;

c) A brief summary of the investigation's predication;

d) A succinct description of the information desired; and

e) The name, title and address of the communication service provider who should receive the request.

B. (U) Telephone subscriber and toll records acquired by the foregoing means may be disseminated to other agencies of the Federal Government only when such information is clearly relevant to their authorized responsibilities. See: id. *Section 2709(d).*

C. (U) On a semiannual basis, the FBI must fully inform the House Permanent Select Committee on Intelligence; the House Committee on the Judiciary; the Senate Select Committee on Intelligence and the Senate Committee on the Judiciary; of requests made by the foregoing means. See: id. *Section 2709(e).*

EFFDATE: 04/29/2002 MCRT# 1262 ~~Div: D5 Cav:~~ SecClass: Unclassified

Section 3-04 (U) Pen Registers and Trap and Trace Devices

A. (U) Generally, applications for pen registers and trap and trace devices must be submitted to the FISA Court, or to specially designated Federal Magistrates. All such applications must include:

1. The identity of the Federal officer making the application;
2. A certification that the information likely to be obtained is foreign intelligence information not concerning an a USPER; or is relevant to an authorized investigation to protect against IT or clandestine intelligence activities, provided that such an investigation of an USPER is not conducted solely on the basis of activities protected by the First Amendment of the U.S. Constitution;
3. Information which demonstrates a reason to believe that the target telephone line, communication instrument or device has been, or is about to be used in communication with: an individual who has or is engaging in international terrorism or clandestine intelligence activities which violate U.S. criminal law; or a foreign power or agent thereof which is engaged in international terrorism or clandestine intelligence activities which violate U.S. criminal law.

B. (U) Court Orders approving pen registers and trap and trace devices, authorize their installation and operation for periods not to exceed 90 days. Extensions of additional 90 day periods may be obtained.

C. (U) Notwithstanding the foregoing, however, whenever the Attorney General determines that an emergency exists, and that factual bases exist for a Court Order, the Attorney General may authorize the execution of an emergency pen register or trap and trace device; if the Court is informed at the time of the authorization, and application is in fact made no more than 48 hours after the authorization.

1. Authorized emergency pen registers and trap and trace devices shall terminate when the information sought is obtained, when the application is denied, or 48 hours after the authorization is given, whichever comes first.
2. If a Court Order is denied after an emergency pen register or trap and trace device has been installed, no information collected as a result shall be used in any manner, except with the approval of the Attorney General if the information indicates a threat of death or serious bodily harm to any person.

[Section 19 (U) International Terrorism Investigations [(See also MIOG, Part 1, 100-1.2, 100-1.2.2, 100-2.3, 199-1, 256-10, 262-1, 265-1, and 315-1.)]

EFFDATE: 04/30/2004 MCRT# 1338 Div: CT Cav: SecClass: Unclassified

[Section 19-01 (U) [Introduction to]International Terrorism Investigations

[A. (U) [The 199 (International Terrorism), 265 (Act of Terrorism), 256A (Hostage Taking by International Terrorists), and 262 (Overseas Homicide/Attempted Homicide) classifications have been deleted from the Manual of Investigative Operations and Guidelines (MIOG). The 315 classification (International Terrorism) replaces these four previous violations and will be the appropriate classification for International Terrorism investigations.

[B. (U) International Terrorism investigations are national security investigations that support the FBI's priority to protect the United States from terrorist attack. This goal drives the Counterterrorism Division's (CTD's) mission to prevent, disrupt, and defeat terrorist operations before they occur.

[C. (U) The nature of International Terrorism investigations must focus on:

[1.

[2.

[3.

[4.

b2
b7E

[D. (U)

[E. (U) There were three significant legal developments after September 11, 2001 that affected International Terrorism investigations:

[1. "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001" (USA PATRIOT Act), effective October 26, 2001.

[2. "Intelligence Sharing Procedures for Foreign Intelligence and Foreign

[Counterintelligence Investigations Conducted by the FBI," issued on March 6,
[2002 by the Department of Justice (DOJ).

[3. Foreign Intelligence Surveillance Court of Review's opinion issued on
[November 18, 2002, In re Sealed Case, 310 F.3d 717 (FISCR 2002).

[(U) These developments removed the "walls" that were historically erected
[between "criminal" and "intelligence" International Terrorism investigations. They
[also permit unprecedented coordination among the FBI, DOJ, and the U. S.
[Intelligence Community (USIC).

[F. (U)
[
[

b2
b7E

[G. (U) The FBI shall conduct its International Terrorism investigations in compliance with the
[Attorney General's Guidelines for FBI National Security Investigations and Foreign
[Intelligence Collection (National Security Investigations Guidelines, or NSIG), which were
[issued October 31, 2003. The general objective of the NSIG is the full utilization of all
[authorities and investigative techniques, consistent with the Constitution and laws of the
[United States, so as to protect the United States and its people from terrorism and other
[threats to the national security.

[(U) The NSIG permits more aggressive investigation and analysis of international
[terrorism targets than previously permitted.
[
[

[H. (U) In addition to the NSIG, the FBI shall conduct its International Terrorism
[investigations in compliance with the Constitution and all applicable statutes, executive
[orders, DOJ regulations and policies, and other Attorney General guidelines.

[I. (U) FBI Headquarters will be the national program manager and office of origin for all
[Foreign Terrorist Organizations designated by the U.S. Secretary of State. Field offices
[direct investigations on the activities of these organizations only within their respective
[areas of responsibility.]

EFFDATE: 12/01/2003 MCRT# 1314 Div: CT Cav: SecClass: Unclassified

Section 19-02 (U) Investigative Strategy in International Terrorism Investigations

A.

b2
b7E

B. (U) The strategy (or long-term) goal of an International Terrorism investigation is the development of intelligence regarding all aspects of the terrorist threat. There are several tactical resolutions that can be used in an investigation. Prosecution for a criminal offense is one tactical weapon that can be used in the arsenal available to defeat international terrorism.

C. (U) International Terrorism investigations are nationally managed by CTD. It is essential during the course of the each stage of an investigation that field offices coordinate with the appropriate CTD operational, analytical, reports dissemination, and operational support units.

D. (S)

1. Identification

(S)

b1
b2
b7E

2. (S)

(S)

[redacted]

b1
b2
b7E

(See 19-03, D.1., below.)

3. (S) [redacted]

a) (U) THREAT ASSESSMENT

(S) [redacted]

(S)

(S)

(U) Under this authority, Agents may attend public events and visit public places and conduct surveillance of individuals or groups present in these public settings for the purpose of determining the presence and extent (nature, scope) of a threat to national security. Surveillance may not be conducted for the sole purpose of monitoring the exercise of rights protected by the constitution.

(U) The retention of information acquired from visits to public places and events is allowed only if it relates to threats to the national security or potential criminal activity.

b) (U) PRELIMINARY INVESTIGATIONS:

(S)

(S)

(S)

b1
b2
b7E

b1
b2
b7E

(S)

1)
2)
3)
4)
5)
6)
7)
8)
9)
10)
11)
12)

b1
b2
b7E

(S)

13)

14)

15)

16)

(S)

b1
b2
b7E

c) (U) FULL INVESTIGATIONS:

(S)

(S)

1)

288I [redacted] b2 b7E

EFFDATE: 01/17/2003 MCRT# ~~1273~~ Div. CY Cav: ~~SecClass: Unclassified~~

Section 23-08 288A - Computer Intrusion - Criminal

A. (U) The 288A Subclassification should be utilized upon the receipt of a computer intrusion report and the initiation of a criminal investigation. Examples of criminal computer intrusions include Denial of Service attacks, network intrusions resulting in theft of proprietary or customer information, computer virus attacks which disrupt or destroy data contained on computers, and insertion of malicious computer code which impedes or impairs computer data.

B. (U) As stated in the Attorney General's Guidelines on General Crimes, Racketeering Enterprise and Domestic Security/Terrorism Investigations, "All investigations of crime or crime-related activities shall be undertaken in accordance with one or more of these guidelines." In short, criminal investigative authorities, as set forth in these guidelines, are utilized during investigations of criminal activity, suspected criminal activity, in violation of federal criminal statutes, i.e. the United States Code.

C. (U) Guidance regarding the conduct and reporting of 288A matters can be found in the Manual of Investigative and Operational Guidelines (MIOG), part 1, section 288.

EFFDATE: 01/17/2003 MCRT# ~~1273~~ Div. CY Cav: ~~SecClass: Unclassified~~

Section 23-09 (U) 288B - Threats to the National Information Infrastructure - Counterintelligence/Counterterrorism Computer Intrusion (TNII - CI/CT)

b1 b2 b7E

A. (U) General Guidelines

1. (S/NF [redacted]

b2 b7E

2. (U) Pursuant to Section II.A.,and II.B.2.F. of the Attorney General Guidelines for FBI Foreign Intelligence Collection and Foreign Counterintelligence Investigations (FCIG), the Attorney General [redacted]

3. (S/NF) [redacted]

4. (S/NF) [redacted]

5. (S/NF) [redacted]

6. (S/NF) [redacted]

b1
b2
b7E

7. (S/NF) [redacted]

8. (S/NF) [redacted]

9. (S/NF) [redacted]

10. (S/NF) [redacted]

(S) [redacted] b1 b2 b7E

11. (S/NF) [redacted]

12. (S/NF) [redacted]

B. (U) Investigative Thresholds for [redacted]

1. (U) The Computer Fraud and Abuse Act, as amended (the National Information Infrastructure Protection Act of 1996), is the principal federal statute that predicates computer intrusion investigations. The amended statute addresses the central tenets of computer and information system security, i.e., protecting the confidentiality, integrity, and availability of data and systems.

2. (U) Any investigation involving this violation could have national level consequences [redacted] b1 b2 b7E

a) (S/NF [redacted]

b) (U) [redacted]

c) (U)

b2
b7E

d) (U

3. (S/NF)

C. (U Authorities and Standards

1. (S/NF)

b1
b2
b7E

D. (U) Guidelines

1. (S/NF)

2. (S/NF)

3. (S/NF)

E. (S/NF)

1. (S/NF)

2. (S/NF)

b1
b2
b7E

b1

(S) [redacted] b1

F. (S/NF [redacted]

1. (S/NF [redacted]

[redacted]

2. (S/NF [redacted] b1 b2 b7E

[redacted]

3. (S/NF [redacted]

[redacted]

(S)

b1
b2
b7E

4. (S/NF)

5. (S/NF)

6. (S/NF)

7. (S/NF)

8. (S/NF)

9. (S/NF)

b1
b2
b7E

(S)

b1
b2
b7E

10. (S/NF)

G. (U)

b2
b7E

1. (S/NF)

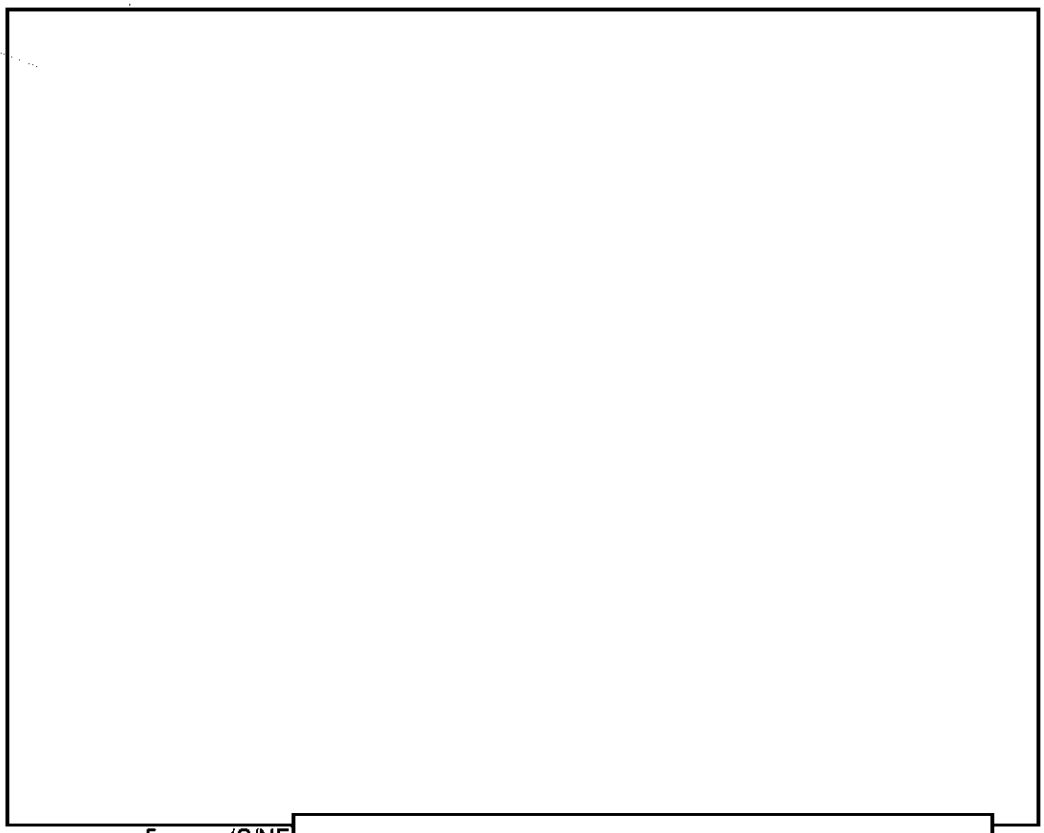
2. (S/NF)

b1
b2
b7E

3. (S/NF)

4. (S/NF)

(S)



b1
b2
b7E

5. (S/NF)

6. (S/NF)

7. (S/NF)

8. (S/NF)

H. (U)

b2
b7E

1. (S/NF)

2. (S/NF)

3. (S/NF)

4. (S/NF)

5. (S/NF)

6. (S/NF)

b1
b2
b7E

I. (U)

1. (S/NF)

2. (S/NF)

J. (U)

1. (S/NF)

2. (S/NF)

K. (U) see also Section 28, infra.)

1. (S/NF)

2. (S/NF)

L. (U) (see also Section 27, infra.)

1. (S/NF)

b1
b2
b7E

2. (S/NF)

M. (U

1. (S/NF)

b1
b2
b7E

N. (U) NIPCIP Computer Intrusion Investigation Reporting Requirements

1. (U) In addition to the reporting requirements for FCI/IT matters, described above, all field offices are reminded that all complaints/allegations of FCI/IT computer intrusions, are to be reported to the Counterintelligence/Counterterrorism Computer Intrusion Unit (C3IU), Computer Intrusion Section (CIS), Cyber Crime Branch, CyD, via Form The FD is to be sent to C3IU The submission of the will allow

2. (U) The FD should include the predication for the investigation

3. (U) Major developments during the investigation, i.e. are to be promptly reported to C3IU, via a supplemental FD

b2
b7E

4. (U) A closing FD is also to be submitted to C3IU, as the closing serial for all 288 matters. This communication should report the final disposition of the investigation/complaint.

5. (U) Reporting of the FD can be completed by fax to C3IU or sent to Unit.

6. (U) It should be noted that [redacted] b2 b7E

O. (U) Investigative Accomplishments [redacted] see also Section 2-53, supra.)

1. (S) [redacted] b1 b2 b7E

2. (U) The NIPCIP will utilize this automated system to capture additional statistical accomplishments, not already captured [redacted] system utilizes the FD-515 to capture data relative to traditional criminal statistical accomplishments, such as arrests, indictments, convictions, etc. The NIPC has found that this matrix was not sufficient to capture the work being done in the field for the NIPCIP.

3. (U) [redacted] b2 b7E

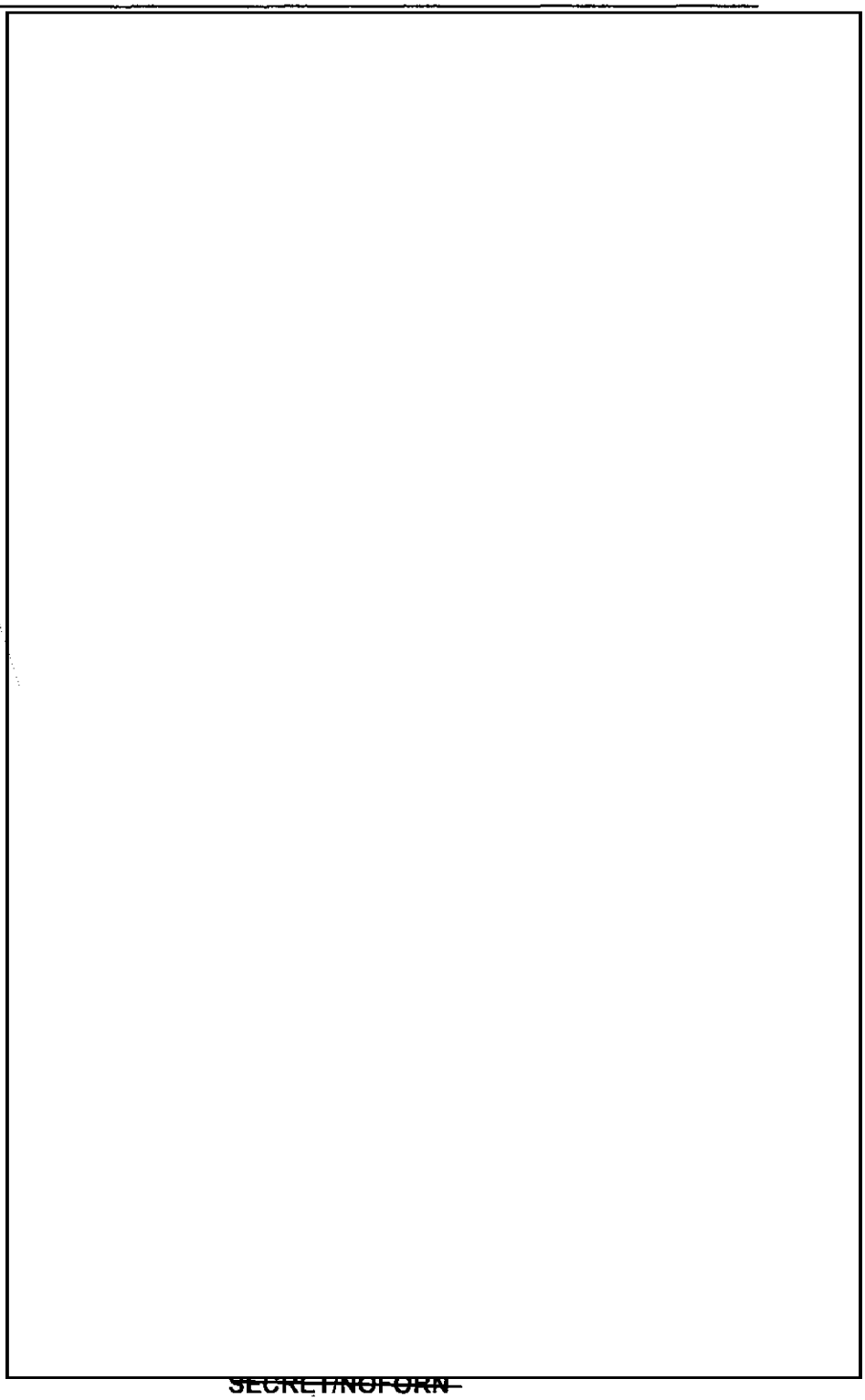
4. (U) As such, the following investigative accomplishments have been incorporated [redacted] to account for the additional accomplishments [redacted]

5. (U) Field offices should maintain a record of the statistical accomplishments, which have been performed since 10/01/1998, the start of the NIPCIP.

6. (U) [redacted]

7. (S) [redacted] b1 b2 b7E

(S)



b1
b2
b7E

(S)

b1
b2
b7E

m) (U) - Claim one accomplishment

n) (U) Claim one accomplishment

o) (U) Claim one accomplishment

p) (U) - Claim one accomplishment

q) (U) Claim one accomplishment

b2
b7E

r) (U) - Claim one accomplishment

s) (U) Claim one accomplishment

t) (U) - Claim one accomplishment

u) (U) Claim one accomplishment

v) (U) - Claim one accomplishment

w) (U) Claim one accomplishment

x) (U) Claim one accomplishment

y) (S)

z) (S)

aa) (S)

bb) (S)

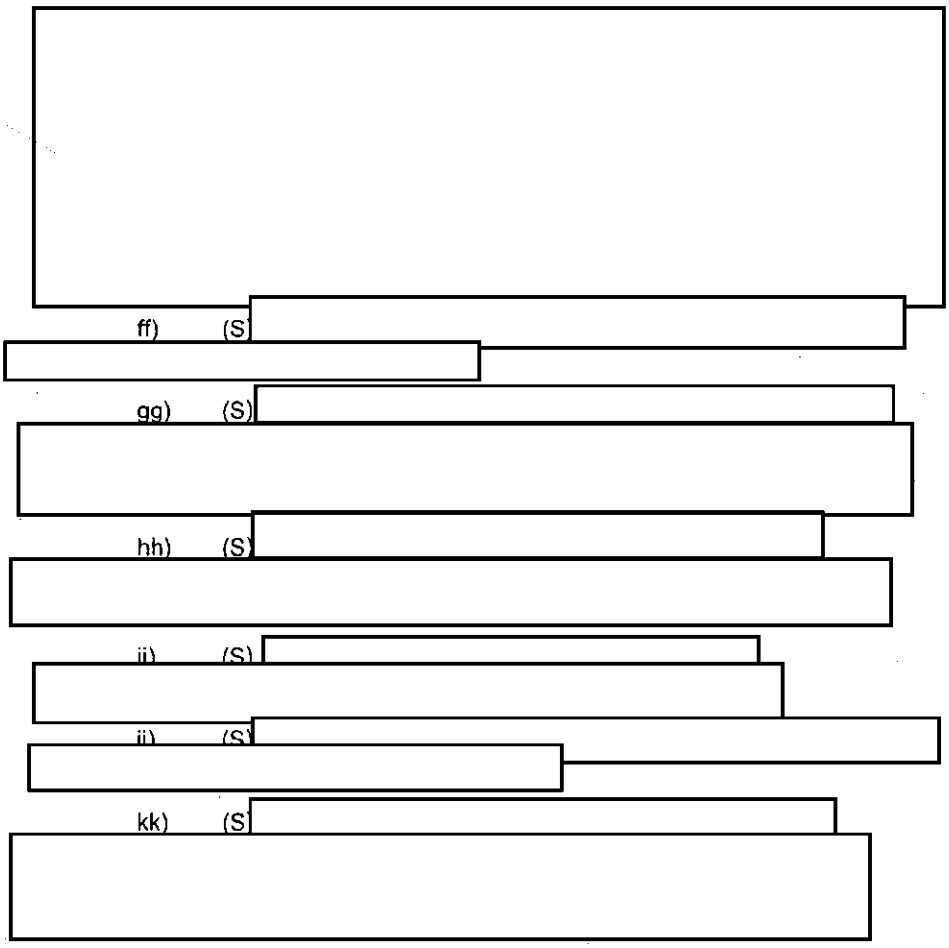
cc) (S)

dd) (S)

ee) (S)

b1
b2
b7E

(S)



ff) (S)

gg) (S)

hh) (S)

ii) (S)

jj) (S)

kk) (S)

b1
b2
b7E

EFFDATE: 01/17/2003 MCRT# 1273 Div. CY Cav: NF SecClass: Secret

Section 23-10 (U) 288C-H - Technical Assistance Matters

A. The 288C-H classifications involve NIPC and NIPCI Squad/Team technical expert assistance to other program's computer-facilitated crime. NIPCI Squad/Team members should TURK time that is spent to support noncomputer intrusion matters as follows:

288C Technical Assistance to WCC Program
288D Technical Assistance t[redacted] Program
288E Technical Assistance to OC/DP
288F Technical Assistance to CI and CT
288G Technical Assistance to DT Program
288H Technical Assistance to CR Program

b2
b7E

EFFDATE: 01/17/2003 MCRT# 1273 Div. CY Cav: SecClass: Unclassified

(U) Glossary
Terms That Have Bearing Upon the FBI's National Foreign Intelligence Program

1. (U)

2. (U)

3. (U)

4. (U)

5. (U)

b2
b7E

6. (U) Analysis: The process in which intelligence information is subjected to systematic examination in order to identify significant facts, and derive conclusions therefrom.

7. (U) Assessment: (a) An appraisal of the worth of an intelligence activity, source, information or product, in terms of its contribution to a specific goal. (b) An appraisal of the credibility, reliability, pertinency, accuracy or usefulness of information in terms of an intelligence need. (c) A judgment of motives, qualifications and characteristics of present or prospective employees, Agents or Assets.

8. (U) Asset: Any resource (human, technical or otherwise) available to an intelligence, CI, IT or security service, for operational purposes. *See, also: Established Source, Informational Asset and Operational Asset.*

9. (U)

10. (U) Asylum: An immigration status which is sought by one who seeks to remain in the U.S. because of persecution or anticipated persecution in his/her country of origin.

11. (U) (REL TO) Authorized For Release To: A control marking which is used when a limited exception to the parameters of NOFORN may be made, to allow the release of information

beyond U.S. recipients. [redacted]

12. (U) [redacted]

13. (U) [redacted]

14. (U) [redacted]

15. (U) [redacted]

16. (U) [redacted]

17. (U) Buckley Amendment: Governs the acquisition of education records from educational agencies and institutions. *See: Title 20, U.S. Code, Section 1232g.*

18. (U) [redacted]

19. (U) PROPIN (Caution--Proprietary Information Involved): A marking used, with or without a security classification, to identify information which has been provided under an express or implied understanding that the information will be protected as a proprietary trade secret, or proprietary data, believed to have actual or potential value. *See: Director of Central Intelligence Directive 1/7,* [redacted]

b1
b2
b7E

20. (U) Caveated Information: Information that is subject to an authorized control marking. *See: id., Section 3.1.*

21. (U) [redacted]

22. (S) [redacted]

23. (S) [redacted]

24. (U) Chief Of Mission: The principal officer in charge of a diplomatic mission of the U.S., or of a U.S. office abroad which is designated by the Secretary of State as diplomatic in nature. *See: Title 22, U.S. Code, Section 3902(3).*

25. (U)

26. (S)

27. (U) Cipher: Any cryptographic system in which arbitrary symbols or groups of symbols represent units of plain text, and/or in which units of plain text are rearranged.

28. (U) Cipher Pad (One Time Pad): A manual one-time cryptosystem produced in pad form. *See: id.*

29. (U) Clandestine Operation: A preplanned intelligence collection activity, or covert political, economic, propaganda, or paramilitary action, which is conducted in such a way a to assure the secrecy of the operation.

30. (C)

31. (U) Classification: The determination that official information requires, in the interest of National Security, a specific degree of protection against disclosure, coupled with a designation signifying that such a determination has been made.

32. (U) Codename: A single word which is used to disguise the identity of a covert operative.

b1
b2
b7E

33. (U) Codeword: (a) used to disguise certain covert operations; e.g., (b) used with a security classification to indicate that material so classified was derived through a sensitive source or method, constitutes a particular type of SCI, identifies a particular investigation, and/or is otherwise accorded limited distribution.

34. (U) Coercion: An expressed or implied threat, made to elicit a desired response or action from a person.

35. (U) Collection Requirement: A request for a specific collection action, in order to satisfy a general or specific intelligence information need.

36. (C)

37. (U)

[redacted]

38. (U) COMINT (Communications Intelligence): An intelligence product, derived from the collection and processing of foreign communications.

39. (U) COMSEC (Communications Security): Measures and controls taken to deny unauthorized persons information derived from telecommunications, and to ensure the authenticity of such telecommunications. COMSEC includes cryptosecurity, transmission security, emission security and physical security of COMSEC material. *See: the National Security Telecommunications and Information Systems Security Command's National Information Systems Security (INFOSEC) Glossary; and Manual of Investigative Operations and Guidelines, Section II, 16-12.*

40. (U) [redacted]

41. (S) [redacted]

b1
b2
b7E

42. (U) Compartmentation: The restriction of information to those who have a need-to-know.

43. (U) Compromise: A disclosure of information to unauthorized persons; or a violation of the security policy of a system in which unauthorized, intentional or unintentional disclosure, modification, destruction or loss of an object may have occurred. *See: the National Security Telecommunications and Information Systems Security Command's National Information Systems Security (INFOSEC) Glossary.*

44. (U) [redacted]

45. (U) [redacted]

46. (U) [redacted]

47. (U) [redacted]

48. (U) Controlled Technology: Referring to all forms of restricted and embargoed unclassified technology.

49.(U) [redacted]

50. (U) [redacted]

[redacted]

51. (U) Counterespionage: An aspect of FCI, designed to detect, destroy, neutralize, exploit and/or prevent espionage activities through identification, penetration, manipulation, deception and/or repression of individuals, groups or organizations which are conducting or suspected of conducting espionage activities.

52. (U) Counterintelligence Policy Board: Serves as the principle mechanism for (a) developing policies and procedures for the approval of the President to govern the conduct of CI activities; and (b) resolving conflicts, as directed by the President, which may arise between elements of the U.S. Government which carry out such activities.

53. (U) Countermeasure: An action taken to negate the opposition's ability to take advantage of its target's vulnerabilities.

54. (U) Counterterrorism: Measures taken to prevent, deter and respond to a terrorist act, or the threat of such an act, but not including personnel, physical, document or communications security programs. *See: Executive Order 12333, Section 3.4(a).*

55. (U) [redacted]

b2
b7E

56. (U) [redacted]

57. (U) [redacted]

58. (U) Critical Technology: Any technology, selected on the basis of its ability to (a) enhance U.S. national and economic prosperity, (b) provide for U.S. economic independence and competitiveness in the global marketplace, (c) contribute to a rising standard of living, (d) strengthen the U.S.' industrial base, and/or (e) provide for an increased National Security capability. [redacted]

59. (U) Cryptanalysis: The conversion of an encrypted message to plain text, without the knowledge of the crypto-algorithm and/or key which was employed in the encryption. *See: the National Security Telecommunications and Information Systems Security Command's National Information Systems Security (INFOSEC) Glossary.*

60. (U) Cryptographic Systems. *See: Manual of Investigative Operations and Guidelines, Section II, 16-12.1.*

61. (U) [redacted]

62. (U) [redacted]

63. (U) Damage Assessment: An evaluation of a compromise in terms of lost intelligence

information, sources, and/or methods, which may describe and/or recommend measures to minimize damage and to prevent future compromises.

64. (U) [redacted]

65. (U) Dead Drop: An unattended place to which communications, materials or equipment can be taken by one individual, and from which they can be retrieved by another individual, without the two either meeting or seeing each other.

66. (U) Debriefing: A nonhostile interview of an individual who has completed an intelligence assignment, or who has knowledge (through observation, participation or otherwise) of operational or intelligence significance.

67. (U) Deception (Disinformation): A measure designed to induce an opponent into taking an action which is prejudicial to its own interests.

b2
b7E

68. (U) [redacted]

69. (U) Defector: A person of any nationality (though usually a country whose interests are hostile or inimical to those of the U.S.) who has escaped from the control of his/her home country; who is unwilling to return to that country; and who is of special value to the U.S. government [redacted]

70. (U) Defector Source: An individual who (a) possesses intelligence information of value, who (b) has either openly, or without announcement, left the employment of his/her own country's government, and who (c) is furnishing information to another country's government.

71. (U) Delegation: A group from [redacted] country which has been admitted to the U.S. as a representative of an organization or corporation in that country.

72. (U) [redacted]

73. (U) Diplomatic Establishment: Any establishment which is directed and controlled by a foreign government, and which deals with diplomatic, commercial, cultural, educational, news-gathering and/or tourism affairs.

74. (U) Diplomatic Officials: Personnel employed by a country, who act in official capacities. E.g., (a) diplomats, attaches and consuls assigned to diplomatic missions, embassies and Consulates General; and (b) members of international organizations or establishments who are assigned to the U.S. for a period of one year or more. Immediate family members, servants and personal employees are excluded from this class unless unusual circumstances exist. [redacted]

75. (U) Diplomatic Pouch (Diplomatic Bag): A container, bearing visible marks of its

diplomatic character, and protected from opening or detention by a treaty to which the U.S. is a party. *See: AG Guidelines for FBI Foreign Intelligence Collection and FCI Investigations, Section II.B.*

76. (U) Dissemination: The timely distribution of an intelligence product, in a form suitable to intelligence consumers.

77. (U) ORCON (Dissemination and Extraction of Information Controlled by Originator): A security designation which is used to enable the originator of intelligence to control its wider distribution and use on a continuing basis. b2 b7E b1

78. (U)

79. (U)

80. (U)

81. (U)

82. (U)

83. (U) Economic Espionage: Foreign power-sponsored or coordinated intelligence activity directed at the U.S. Government, U.S. corporations, establishments or persons, which involves (a) the unlawful or clandestine targeting or acquisition of sensitive financial, trade or economic policy information, proprietary economic information, or critical technologies; or (b) the unlawful or clandestine targeting or influencing of sensitive economic policy decisions.

84. (S)

85. (U) Electronic Surveillance: (a) The acquisition (by electronic, mechanical or other surveillance device) of the contents of any wire or radio communication (sent by, or intended to be received by, a U.S. person in the U.S.), if the contents are acquired by intentionally targeting that U.S. person, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes; (b) the acquisition (by electronic, mechanical or other surveillance device) of the contents of any wire or radio communication (to or from a person in the U.S.), without the consent of any party thereto, if such acquisition occurs in the U.S.; (c) the intentional acquisition (by an electronic, mechanical, or other surveillance device) of the contents of any radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, and if both the sender and all intended recipients are located within the U.S.; or (d) the installation or use of an electronic, mechanical, or other surveillance device in the U.S. for monitoring to acquire information (other than from a wire or radio communication), under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes. *See: Title 50, U.S. Code, Section 1801(f).*

86. (U) Embargoed Material: Material which is formally prohibited by U.S. law and administrative procedure from being transferred to certain recipients.

87. (U) Emigre: A person who departs from his/her country for any lawful reason, with the intention of permanently resettling elsewhere. *See: Director of Central Intelligence Directive 4/1, Section 2(g).*

88. (U) Espionage: Intelligence activity directed toward the acquisition of intelligence through clandestine means. *See: Director of Central Intelligence Directive 5/1, Section 2.*

89. (U) Established Source: A person who, as a result of his/her employment or position in a community or organization, is in possession of information relevant to an FCI, IT or foreign intelligence investigation, and who is willing to furnish this information to the FBI on an occasional/intermittent/ irregular basis.

90. (U) Fair Credit Reporting Act: Governs the acquisition of consumer reports from consumer reporting agencies. *See: Title 15, U.S. Code, Sections 1681-1681f.*

91. (U)

92. (U)

93. (U) For Or On Behalf Of A Foreign Power: Referring to a determination of the extent to which a foreign power is involved in the (a) control, leadership or policy direction; (b) financial or material support; or (c) leadership, assignments or discipline of an individual or group. *See: AG Guidelines for FBI Foreign Intelligence Collection and FCI Investigations, Section II.L.*

94. (U) FCI (Foreign Counterintelligence): Information gathered, and activities conducted, to protect against espionage and other intelligence activities, sabotage, or assassinations conducted by, for or on behalf of foreign powers, organizations or persons, or IT activities--but not including personnel, physical, document or communications security programs. *See: Executive Order 12333, Section 3.4(a) and AG Guidelines for FBI Foreign Intelligence Collection and FCI Investigations, Section II.D.*

b1
b2
b7E

95. (S)

96. (U) Foreign Diplomatic Establishment: An embassy, mission, consulate, residential compound or other premises owned or leased and used for official purposes by a foreign government, whether or not recognized by the U.S.; premises of international organizations, as defined by Title 22, USC, Section 288; premises of establishments authorized to be treated as international organizations or diplomatic missions by specific statute (e.g., Title 22, USC, Section 288f-1 through 288i); and the premises of establishments of foreign representatives to such international organizations. *See: AG Guidelines for FBI Foreign Intelligence Collection and FCI Investigations, Section II.E.*

97. (U) Foreign Intelligence: Information relating to the capabilities, intentions and activities

of foreign powers, organizations or persons--but not including counterintelligence except for information on IT activities. *See: Executive Order 12333, Section 3.4(d).*

98. (U) Foreign Intelligence Agent: A person (other than a foreign IO) who is engaged in intelligence activities or sabotage for or on behalf of a foreign power, or IT activities, or who knowingly conspires with or aids or abets such a person in such activities. *See: AG Guidelines for FBI Foreign Intelligence Collection and FCI Investigations, Section II.G.*

99. (U) Foreign Intelligence Officer: A member of a foreign intelligence service. *See: id. Section II.H.*

100. (U) (FISA) Foreign Intelligence Surveillance Act: Governs electronic surveillances and physical searches in FCI, international terrorism and foreign intelligence investigations. *See: Title 50, U.S. Code, Sections 1801-1829, 1841-1846 and 1861-1863.*

101. (U) Foreign Intelligence Surveillance Court: A body of seven federal district court judges who have jurisdiction to hear applications, and to grant orders for, electronic surveillances and physical searches under the FISA.

102. (U) [redacted]

103. (U) Foreign Liaison Officer: A government official who has been accredited to represent that government in the exchange and/or discussion of intelligence.

104. (U) [redacted] b2 b7E

105. (U) Foreign Official: A foreign national in the U.S. who is (a) acting in an official capacity for a foreign power, (b) attached to a foreign diplomatic establishment or an establishment under the control of a foreign power, or (c) employed by an international organization established under an agreement to which the U.S. is a party.

106. (U) Foreign Power: (a) A foreign government or any component thereof, whether or not recognized by the U.S. (b) A faction of a foreign nation or nations, not substantially composed of USPERs. (c) An entity that is openly acknowledged by a foreign government or governments to be directed and controlled by such foreign government or governments. (d) A group engaged in IT or activities in preparation therefor. (e) A foreign-based political organization, not substantially composed of USPERs. (f) An entity that is directed and controlled by a foreign government or governments. *See: Title 50, U.S. Code, Section 1801.*

107. (U) Foreign Visitor: A foreign national in the U.S. who is not a PRA of the U.S. *See: AG Guidelines for FBI Foreign Intelligence Collection and FCI Investigations, Section II.K.*

108. (U) FOUO: A marking, used on classified intelligence, [redacted]

109. (U) Front: An organization or company which is used by an FIS or IT group as a guise, to protect clandestine intelligence or terrorist activities.

110. (S) [redacted]

b1
b2
b7E

111. (U) HUMINT (Human Intelligence): Intelligence information that is collected from human sources, in either an overt or clandestine manner. [redacted]

112. (U) Illegal: An officer or employee of an intelligence service, who has no overt connection with either the service or the government which controls it, and who is dispatched abroad for covert purposes.

113. (U) Illegal Transfer: The transfer of controlled, but unclassified technology.

114. (S) [redacted]

115. (U) [redacted]

116. (U) Informational Asset: A person who obtains information of value to the FBI as a result of his/her normal daily and/or business routine.

117. (U) Inspectors: Within the Arms Control Treaty arena, officials who, at U.S. locations described in the Intermediate-Range Nuclear Forces Treaty Protocol [redacted]

118. (U) INTELINK: A transposition of public domain, Internet technology to a secure communications and processing environment. An intelligence dissemination and collaboration service.

119. (U) Intelligence: (a) Referring, collectively, to the functions, activities or organizations that are involved in the process of planning, gathering and analyzing information of potential value to decision makers. (b) The product which results from the collection, collation, evaluation, analysis, integration and interpretation of collected information.

120. (U) Intelligence Activity: An activity conducted by, for or on behalf of a foreign power, for intelligence purposes, or to affect political or governmental processes. *See: AG Guidelines for FBI Foreign Intelligence Collection and FCI Investigations, Section II.M.*

121. (U) Intelligence Community: All components of a government which cooperate in the production of intelligence and CI. Within the U.S., it includes: (a) the CIA; (b) the NSA; (c) the DIA; (d) reconnaissance program offices within the DOD; (e) DOS's Bureau of Intelligence and Research; intelligence elements of (f) the Army, (g) the Navy, (h) the Air Force, (i) the Marine Corps, (j) the FBI, (k) the Department of the Treasury and (l) the DOE; and (m) staff elements of the DCI. *See: Executive Order 12333, Section 3.4(f).* b1 b2 b7E

122. (U) [redacted]

123. (U) Intelligence Officer: A professionally trained member of an intelligence service.

124. (U) Intelligence Oversight Board: An organization which: (a) reports to the President and the AG on USIC activities which may be unlawful, or contrary to EO or Presidential Directive; (b) reviews the internal guidelines of agencies within the USIC which concern intelligence activities and the law; (c) reviews the practices and procedures of agencies within the USIC for discovering and reporting intelligence activities that may be unlawful or contrary to EO or Presidential Directive; and (d) conducts such investigations as it deems necessary to carry out the aforementioned functions. *See: Executive Order 12863.*

125. (S) [redacted]

126. (U) International Terrorism: Activities that (a) involve violent acts or acts dangerous to human life that are a violation of the criminal laws of the U.S. or of any State, or that would be a criminal violation if committed within the jurisdiction of the U.S. or any State; (b) appear to be intended to intimidate or coerce a civilian population, to influence the policy of a government by intimidation or coercion, or to affect the conduct of a government by assassination or kidnapping; and (c) occur totally outside the U.S., or transcend national boundaries in terms of the means by which they are accomplished, the persons they appear intended to coerce or intimidate, or the locale in which their perpetrators operate or seek asylum. *See: AG Guidelines for FBI Foreign Intelligence Collection and FCI Investigations, Section II.N.*

127. (U) International Terrorist: An individual or group that knowingly engages in IT or activities in preparation therefore, or knowingly aids or abets any person engaged in such activities. *See: id. Section II.O.*

128. (U) Inviolable Premises: Diplomatic or consular premises, including the residences of diplomatic agents, administrative and technical personnel, consular officers or consular employees,

and any international organization premises, including residences. *See: MOU Between the DOS and the FBI on Liaison for CI Investigations.*

129. (U) Issue Threat: A category of activity which, when engaged in by any foreign power or entity, is considered to be of such concern to U.S. National Security interests that CI or monitoring actions directed against such activities are warranted.

130. (U)

131. (S)

132. (U)

133. (U)

134. (S)

135. (S)

136. (U)

137. (U)

b1
b2
b7E

138. (U) National Counterintelligence Operations Board: An entity composed of personnel on the National Counterintelligence Policy Board, which operates closely with NACIC in resolving specific issues which are brought before it by the NACIPB.

139. (U) National Counterintelligence Policy Board: A senior CI policy coordination body, composed of senior executives from: the FBI; DOD; the CIA; DOS; DOJ; the NSC; and OMB.

140. (U)

exchanges of foreign intelligence information; (c) arrangements with foreign governments on intelligence matters; (d) protection of intelligence sources and methods; (e) activities of common concern; and (f) such other matters as may be referred to it by the DCI. *See: Director of Central Intelligence Directive 3/1.*

141. (U) National Foreign Intelligence Program: Includes (a) the programs of the CIA; (b) the programs of the Consolidated Cryptologic Program; (c) the General Defense Intelligence Program, (d) the programs of offices within the DOD for the collection of specialized national foreign intelligence through reconnaissance (except such elements as the DCI and the Secretary of Defense agree should be excluded); (e) the foreign intelligence and FCI programs of other agencies within the USIC; (f) activities of the staff elements of the DCI. Activities to acquire the intelligence required for the planning and conduct of tactical operations by the U.S. military forces are not included in the NFIP. *See: Executive Order 12333, Section 3.4(g).*

142. (C) National HUMINT Requirements Tasking Center: A body which provides a mechanism to support the DCI in the effective oversight, management, coordination, integration and allocation of IC resources for the collection of intelligence information through the use of human sources. *See: Director of Central Intelligence Directive 3/7.*

143. (S)

144. (S)

145. (U) National Security Letter: A process used to obtain telephone toll records, subscriber information, financial records, and consumer credit reports on subjects of FCI, foreign intelligence, and IT investigations, where the appropriate statutory predicates have been met.

146. (U) National Security Telecommunications and Information Systems Security Committee: An organization which operates under the direction of the U.S. Government's System Security Steering Committee; which consists of the Secretaries of Defense, State, and the Treasury, the AG, the Director of the Office of Management and Budget, and the DCI. Consisting of representatives from the Departments of Defense, State, Treasury, Commerce, Transportation, and Energy; the Joint Chiefs of Staff, GSA, FBI, Army, Navy, Air Force, Marine Corps, DIA, CIA and NSA. The NSTISSC develops operations policies, and provides guidance to government agencies as respects computer security.

b1
b2
b7E

147. (U) Need-to-Know: A determination by an authorized holder of classified information that access to that material is required by another person to perform a specific and authorized function. The recipient must possess an appropriate security clearance, and approvals in accordance with DCID 1/14. *See: Director of Central Intelligence Directive 1/19, Section 1.1.12.*

148. (U) No Foreign Policy Objection: A statement that the DOS does not pose a foreign policy objection to an FCI, IT or foreign intelligence activity proposed by the FBI. *See: 1992 MOU Between the DOS and the FBI on Liaison for CI Investigations, Section I.H.*

149. (U)

[redacted]

150. (U) Non-U.S. Person: An undocumented alien, or a foreign national lawfully in the U.S. who is not a PRA. *See: AG Guidelines for FBI Foreign Intelligence Collection and FCI Investigations, Section II.P.*

151. (U) NOFORN (Not Releasable To Foreign Nationals): A security designation which is used to identify classified intelligence which may not be released, in any form, to foreign governments, foreign nationals or non-U.S. citizens, without the originator's permission. *See: Director of Central Intelligence Directive 1/7, Section 9.4.*

152. (U) [redacted]

153. (U) [redacted]

154. (U) Official Establishment: Any establishment controlled by a foreign government, regardless of its diplomatic or non-diplomatic status.

155. (U) Open Storage: The storage of classified information within an accredited facility (though not within GSA-approved containers) while the facility is unoccupied by authorized personnel. *See: the National Security Telecommunications and Information Systems Security Command's National Information Systems Security (INFOSEC) Glossary.*

b2
b7E

156. (U) Operational Asset: A person who is directed by the FBI to undertake activities outside the normal course of his/her daily or business routine. All [redacted] should be designated OAs.

157. (U) OPSEC (Operations Security): The process of detecting activities which, by themselves or combined with other data, may reveal the existence of sensitive information or operations.

158. (U) Otherwise Illegal Activity: Any activity which would be illegal but for the fact of its having been appropriately authorized. *See: AG Procedure for Reporting and Use of Information Concerning Violations of Law and Authorization for Participation in Otherwise Illegal Activity in FBI Foreign Intelligence, CI or IT Intelligence Investigations.*

159. (U) [redacted]

160. (U) [redacted]

161. (U) [redacted]

162. (U) [redacted]

163. (U) Permanent Resident Alien: A person who has received lawful permanent resident status in the U.S., but who is not yet a U.S. citizen.

164. (U) Persona Non Grata: An official act, declaring a foreign national unacceptable or

unwelcome--usually when found to have been engaging in intelligence activities, or otherwise violating the law.

165. (U) Physical Search: Any physical intrusion within the U.S. into premises or property (including an examination by technical means) that is intended to result in a seizure, reproduction, inspection, or alteration of information, material, or property, under circumstances in which a person has a reasonable expectation of privacy, and a warrant would be required for law enforcement purposes. *See: Title 50, U.S. Code, Section 1821(5).*

166. (U) PL 110 (Public Law 110): A law whereby vetted Defectors are granted PRA status through agreement between the DCI, the Commissioner of INS and the AG.

167. (S)

b1
b2
b7E

168. (U) President's Foreign Intelligence Advisory Board: An entity which (a) assesses the quality, quantity and adequacy of U.S. intelligence and CI activities; (b) reports to the President regarding the USIC's objectives, conduct, management and efforts at coordination; and (c) makes such recommendations as may be appropriate. *See: Executive Order 12863, Sections 1.2 through 104.*

169. (U) Proprietary Economic Information: Any economic, scientific or technical information, design, process, procedure, formula, strategy or improvement (whether represented in a tangible or intangible form) which is not generally accessible or known in the trade, business or scientific communities, and concerning which the owners have taken affirmative measures to prevent its entry into the public domain.

170. (U)

171. (U) Proprietary Information and Technology: Sensitive material that is not yet embargoed or classified.

172. (U) Publicly Available: Information which (a) has been published or broadcast for general public consumption, (b) is available on request to any member of the general public, (c)

could lawfully be seen or heard by any casual observer, or (d) is made available at a meeting open to the general public. *See: AG Guidelines for FBI Foreign Intelligence Collection and FCI Investigations, Section II.B.*

173. (U)

174. (U)

175. (U)

176. (U)

177. (U)

178. (U) Refugee: A person who (a) has departed his/her country of nationality or habitual residence; who (b) is unable to return to that country because of a well-founded fear of being persecuted for reasons of race, religion, nationality, membership in a particular social group, or political opinion; who (c) does not possess another citizenship; and who (d) has not acquired resident status in the country of present domicile.

b2
b7E
b1

179. (U) Reliability: Referring to whether an Asset is controllable, dependable, and whether the information he/she provides is correct.

180. (U) Residency--Illegal: An intelligence establishment, which has no overt connection with government.

181. (U) Residency--Legal: An intelligence establishment, which is overtly linked to its government.

182. (U) Right to Financial Privacy Act: Governs the acquisition of financial records of customers of financial institutions. *See: Title 12, U.S. Code, Sections 3401-3414.*

183. (U)

184. (U) Sanitization: The process of editing or otherwise altering intelligence products, to conceal sensitive sources, methods, capabilities, analytical procedures and/or privileged information, in order to permit wider dissemination.

185. (S)

(S) [redacted]

186. (U) [redacted]

187. (U) SCI (Sensitive Compartmented Information): Classified information (concerning or derived from intelligence sources, methods, or analytical processes) which is required to be handled within formal access control systems established by the DCI. [redacted]

188. (U) SCIF (Sensitive Compartmented Information Facility): An accredited area, room, group of rooms, building or installation where SCI may be stored, used, discussed and/or processed. [redacted]

189. (U) Sensitive Financial, Trade And Economic Policy Information: Data, details, facts and/or knowledge, concerning strategy, methods, tactics and/or procedures; which pertain to productivity, strategic goals, financial planning and allocation of resources, of the U.S. government, U.S. corporations, establishments and/or persons; which is not generally accessible or known in the financial, trade, business or scientific community, the owners of which have taken affirmative measures to prevent its entry into the public domain.

190. (U) SIGINT (Signals Intelligence): An intelligence product, derived from the monitoring of radio transmissions of all kinds; e.g., teletype; Morse code; radiophone; radar emissions; and signals from missiles, satellites and spacecraft.

191. (U) Sleeper: An Illegal or Agent, residing in a foreign country, and under orders to engage in no intelligence activities until a specific need arises.

192. (U) SAP (Special Access Program): Any program, established under EO 12356, which imposes controls governing access to classified information above and beyond those required by normal management and safeguarding practices.

193. (U) [redacted]

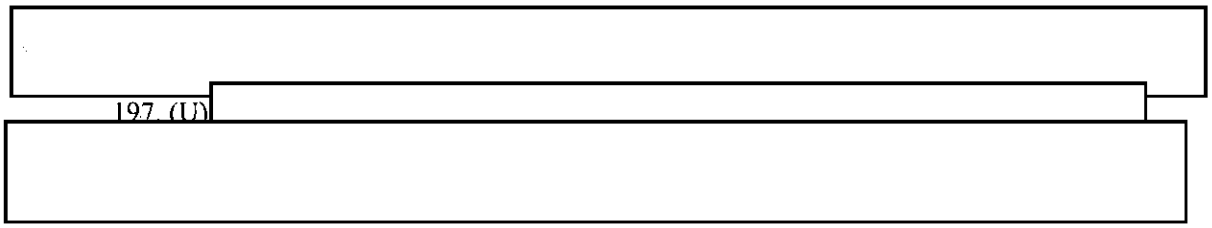
194. (U) Substantially Composed Of U.S. Persons: In determining whether a group or organization is substantially composed of USPERs, the FBI should consider not only the citizenship or resident alien status of members of the group or organization in the U.S.; but also the relationship of that group or organization to a foreign-based international organization. If the group or organization in the U.S. operates directly under the control of the international organization and has no independent program or activities in the U.S., membership of the entire international organization should be considered in determining if it is substantially composed of USPERs. If, however, the U.S.-based group or organization has programs or activities separate from, or in addition to, those directed by the international organization, only the U.S. membership should be considered in determining whether it is substantially composed of USPERs. *See: AG Guidelines for FBI Foreign Intelligence Collection and FCI Investigations, Section II.T.*

195. (U) [redacted]

196. (S) [redacted]

b1
b2
b7E

(S)



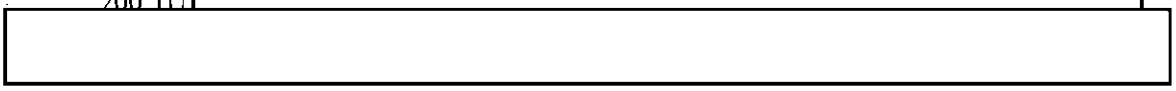
b1
b2
b7E

197. (U)

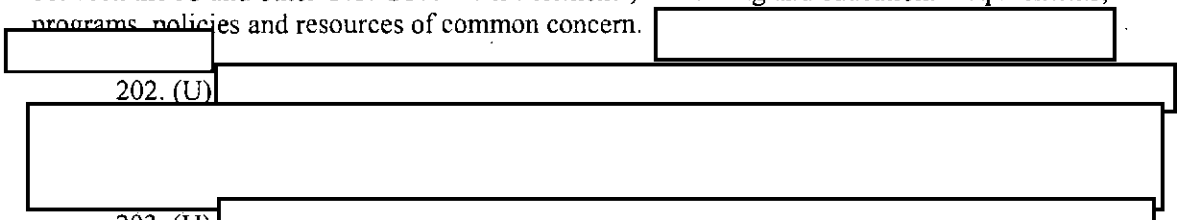
198. (U) Terrorist: An individual who engages in terrorist activities which are intended to (a) intimidate or coerce a civilian population; (b) influence the policy of a government by intimidation or coercion; or (c) affect the conduct of a government by assassination or kidnapping.

199. (U) Threat Analysis: A comprehensive assessment of the threat posed not only by an opposition intelligence service, but also those organizations and individuals whose interests are inimical to thos

200. (U)

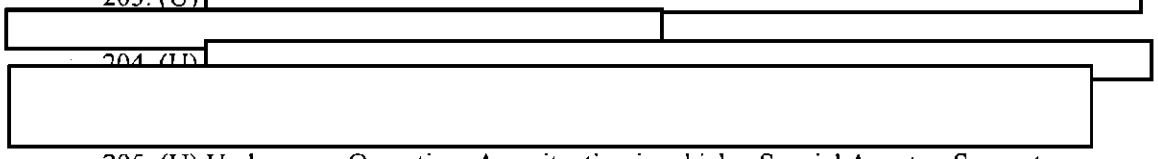


201. (U) Training Directors' Consortium: Serves as the focal point within the IC, and between the IC and other U.S. Government elements, on training and educational requirements, programs, policies and resources of common concern.



202. (U)

203. (U)

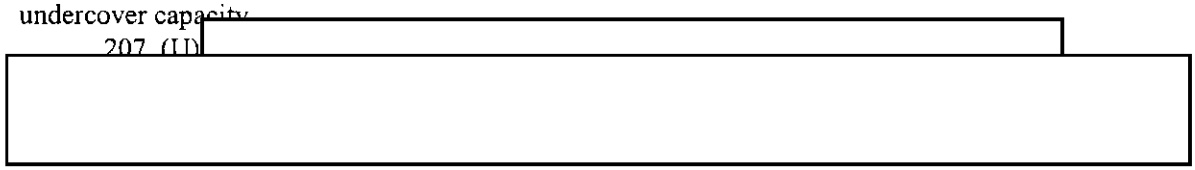


204. (U)

205. (U) Undercover Operation: Any situation in which a Special Agent or Support Employee is engaged in a relationship with the target of a FCI, IT or foreign intelligence investigation, where the contact is expected to continue over a period of time, and where FBI employment is concealed. A "Group I" operation involves sensitive circumstances; whereas a "Group II" operation is non-sensitive.

206. (U) Undercover Special Agent/Support Person: An FBI employee who is acting in an undercover capacity.

207. (U)



208. (U) United States: All areas under the territorial sovereignty of the U.S. *See: AG Guidelines for FBI Foreign Intelligence Collection and FCI Investigations, Section II.V.*

209. (U) U.S. Arms Control and Disarmament Agency: Within the Arms Control Treaty

arena, is responsible for: (i) formulating, coordinating and carrying out arms control policies; (ii) conducting and coordinating research; (iii) preparing and managing U.S. participation in negotiations; and (iv) disseminating information regarding arms control matters to the general public.

210. (U) U.S. Economic Interests: Those financial, trade, research and development, technological and policy issues which define U.S. strategic economic goals, including: (a) the maintenance of U.S. economic health, (b) providing a higher standard of living, and (c) organizing a sustainable economic order.

211. (S)

212. (U)

213. (U) U.S. On-Site Inspection Agency: Within DOD, in connection with Arms Control Treaty matters, is responsible for: (i) providing overall management and support for implementation of the Intermediate Range Nuclear Forces, the Conventional Forces in Europe, the Threshold Test Ban and the Peaceful Nuclear Explosions treaties; (ii) protecting U.S. personnel serving on Agency inspection and escort teams from exploitation by foreign intelligence services; (iii) denying foreign nationals who participate in the verification process from gaining access to sensitive information not required under treaty provisions; and (iv) planning for future treaties--including such matters as scheduling, housing, security, transportation, linguistic needs, and communications. The Agency draws its Principal Deputy, International Affairs, and CI deputy director from the Arms Control Disarmament Agency, DOS and the FBI, respectively. The CI Deputy Director is responsible for preparing a CI operational plan as respects each treaty, specifically identifying all USIC agencies which have interests in same, and their responsibilities. Military and civilian DOD personnel permanently staff the Agency, and personnel are detailed to it from other agencies (including the FBI), as needed.

214. (U) USPER (U.S. Person): A U.S. citizen; a PRA; an unincorporated association, substantially composed of U.S. citizens or permanent resident aliens; or a corporation incorporated in the U.S., except for a corporation directed and controlled by a foreign government or governments. *See: Executive Order 12333, Section 3.4(i); and AG Guidelines for FBI Foreign Intelligence Collection and FCI Investigations, Section II.W.*

215. (U)

216. (U)

b2
b7E
b1

217. (U)

218. (S)

219. (U)

b1
b2
b7E

EFFDATE: 04/19/2002 MCRT# 1262 Div: D5 Cav: NF SecClass: ~~Secret~~

13. (U) See: id., Section V(a)(1). The words "targeted non-United States person agent of a foreign power" are substituted for the words "targeted foreign power."

14. (U) See: id., Section V(a)(2). The words "targeted non-United States person agent of a foreign power" are substituted for the words "targeted foreign power."

15. (U) See: id., Section V(b). The words "targeted non-United States person agent of a foreign power" are substituted for the words "targeted foreign power."

16. (U) See: id., Section V(c). The words "targeted non-United States person agent of a foreign power" are substituted for the words "targeted foreign power."

17. (U) See: id., Section V(d). The words "targeted non-United States person agent of a foreign power" are substituted for the words "targeted foreign power."

~~EFFDATE: 04/29/2002 MCRT# 1262 Div. D5 Cav: SecClass: Secret~~

==========

[E-11 (U) [The Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection, Effective 10/31/2003]

[PREAMBLE (U)

The following Guidelines on national security investigations and foreign intelligence collection by the Federal Bureau of Investigation (FBI) are issued under the authority of the Attorney General as provided in sections 509, 510, 533, and 534 of title 28, United States Code. They apply to activities of the FBI pursuant to Executive Order 12333 and other activities as provided herein. (U)

TABLE OF CONTENTS (U)

II. NATIONAL SECURITY INVESTIGATIONS

A. THREAT ASSESSMENTS
B. COMMON PROVISIONS FOR PRELIMINARY AND FULL INVESTIGATIONS
C. PRELIMINARY INVESTIGATIONS
D. FULL INVESTIGATIONS
E. EXTRATERRITORIAL OPERATIONS

III. INVESTIGATIVE ASSISTANCE TO STATE, LOCAL, AND FOREIGN GOVERNMENTS

A. STATE AND LOCAL GOVERNMENTS
B. FOREIGN GOVERNMENTS

IV. FOREIGN INTELLIGENCE COLLECTION AND ASSISTANCE TO INTELLIGENCE AGENCIES

A. FOREIGN INTELLIGENCE COLLECTION
B. OPERATIONAL SUPPORT
C. CENTRAL INTELLIGENCE AGENCY AND DEPARTMENT OF DEFENSE ACTIVITIES WITHIN THE UNITED STATES

V. INVESTIGATIVE TECHNIQUES

VI. STRATEGIC ANALYSIS

VII. RETENTION AND DISSEMINATION OF INFORMATION

A. INFORMATION SYSTEMS AND DATABASES
B. INFORMATION SHARING
C. SPECIAL STATUTORY REQUIREMENTS

VIII. DEFINITIONS

INTRODUCTION (U)

Following the September 11, 2001, terrorist attack on the United States, the Department of Justice carried out a general review of existing guidelines and procedures relating to national security and criminal matters. These Guidelines reflect the result of that review. (U)

These Guidelines generally authorize investigation by the FBI of threats to the national security of the United States; investigative assistance by the FBI to state, local, and foreign governments in relation to matters affecting the national security; the collection of foreign intelligence by the FBI; the production of strategic analysis by the FBI; and the retention and dissemination of information resulting from the foregoing activities. This includes guidance for the activities of the FBI pursuant to Executive Order 12333, "United States Intelligence Activities" (Dec. 4, 1981). (U)

The general objective of these Guidelines is the full utilization of all authorities and investigative techniques, consistent with the Constitution and laws of the United States, so as to protect the United States and its people from terrorism and other threats to the national security. As Executive Order 12333 provides, "[t]imely and accurate information about the activities, capabilities, plans, and intentions of foreign powers, organizations, and persons and their agents, is essential to the national security of the United States" and "[a]ll reasonable and lawful means must be used to ensure that the United States will receive the best intelligence available." At the same time, intelligence gathering activities must be carried out in a "responsible manner that is consistent with the Constitution and applicable law" and information concerning United States persons may be collected, retained, and disseminated "only in accordance with procedures . . . approved by the Attorney General." Executive Order 12333, Preamble, Sections 2.1, 2.3. These guidelines should be implemented and interpreted so as to realize as fully as possible the critical objectives of the Executive Order. (U)

The activities of the FBI under these Guidelines are part of the overall response of the United States to threats to the national security, which includes cooperative efforts and sharing of information with other agencies, including other entities in the Intelligence Community and the Department of Homeland Security. The overriding priority in these efforts is preventing, preempting, and disrupting terrorist threats to the United States. In some cases, this priority will dictate the provision of information to other agencies even where doing so may affect criminal prosecutions or ongoing law enforcement or intelligence operations. To the greatest extent possible that is consistent with this overriding priority, the FBI shall also act in a manner to protect other significant interests, including the protection of intelligence and sensitive law enforcement sources and methods, other classified information, and sensitive operational and prosecutorial information. (U)

A. NATIONAL SECURITY INVESTIGATIONS (U)

These Guidelines authorize the investigation by the FBI of threats to the national security. Matters constituting threats to the national security, including international terrorism and espionage, are identified in Part I.A1. Parts II and V of the Guidelines contain the specific provisions governing the conduct of investigations of these threats. (U)

The investigations authorized by these Guidelines serve to protect the national security by providing the basis for, and informing decisions concerning, a variety of measures to deal with threats to the national security. These measures may include, for example, recruitment of double agents and other assets; excluding or removing persons involved in terrorism or espionage from the United States; freezing assets of organizations that engage in or support terrorism; securing targets of terrorism or espionage; providing threat information and warnings to other federal agencies and officials, state and local governments, and private entities; diplomatic or military actions; and actions by other intelligence agencies to counter international terrorism or other national security threats. In addition, the matters identified by these Guidelines as threats to the national security, including international terrorism and espionage, almost invariably involve possible violations of criminal statutes. Detecting, solving, and preventing these crimes – and in many cases, arresting and prosecuting the perpetrators – are crucial objectives of national security investigations under these Guidelines. Thus, these investigations are usually both "counterintelligence" investigations and "criminal" investigations. (U)

The authority to conduct national security investigations under these Guidelines does not supplant or limit the authority to carry out activities under other Attorney General guidelines or pursuant to other lawful authorities of the FBI. Thus, matters within the scope of these Guidelines, such as crimes involved in international terrorism and the activities of groups and organizations that aim to commit such crimes, may also be investigated under the guidelines for general crimes investigations and criminal intelligence investigations. See the Attorney General's Guidelines on General Crimes, Racketeering Enterprise and Terrorism Enterprise Investigations, Part II (general crimes investigations) and Part III.B (terrorism enterprise investigations). Likewise, the authorization of extraterritorial activities under Part II.E of these Guidelines overlaps at a practical level with other guidelines the Attorney General has issued for extraterritorial criminal investigations and use of extraterritorial criminal informants. The requirements under these Guidelines to notify FBI Headquarters and other Department of Justice components and officials concerning the initiation and progress of investigations are intended in part to ensure that activities pursuant to these Guidelines are fully coordinated with investigations and activities under other authorities of the FBI. (U)

Part II of these Guidelines authorizes three levels of investigative activity in national security investigations: (1) threat assessments, (2) preliminary investigations, and (3) full investigations: (U)

b2
b7E
b1

(1) Threat assessments. To carry out its central mission of preventing the commission of terrorist acts against the United States and its people, the FBI must proactively draw on available sources of information to identify terrorist threats and activities. It cannot be content to wait for leads to come in through the actions of others, but rather must be vigilant in detecting terrorist activities to the full extent permitted by law, with an eye towards early intervention and prevention of acts of terrorism before they occur. (U)

Part II.A of these Guidelines accordingly authorizes the proactive collection of information concerning threats to the national security, including information on individuals, groups, and organizations of possible investigative interest, and information on possible targets of international terrorist activities or other national security threats (such as infrastructure and computer systems vulnerabilities). This is comparable to the authorization under Part VI of the Attorney General's Guidelines on General Crimes, Racketeering Enterprise and Terrorism Enterprise Investigations to engage in information collection for counterterrorism or other law enforcement purposes without any more specific investigative predication. (S)

b1
b2
b7E

In addition to allowing proactive information collection for national security purposes, the authority to conduct threat assessments may be used in cases in which information or an allegation concerning possible terrorist (or other national security-threatening) activity by an individual, group, or organization is received, and the matter can be checked out promptly through the relatively non-intrusive techniques authorized in threat assessments. [redacted] pg 3 can avoid the need to open a formal preliminary or full investigation, if the threat assessment indicates that further investigation is not warranted. In this function, threat assessments under these Guidelines are comparable to the checking of initial leads in ordinary criminal investigations. See the Attorney General's Guidelines on General Crimes, Racketeering Enterprise and Terrorism Enterprise Investigations, Subpart A of the Introduction. (U)

(S) (2) Preliminary investigations. [redacted] Preliminary investigations may relate to individuals, groups, organizations, and possible criminal violations, as specified in Part II.B. (S)

(S) [redacted] (S)

(S) [redacted] (S) b1 b2 b7E

(S) (3) Full investigations [redacted] Like preliminary investigations, full investigations may relate to individuals, groups, organizations, and possible criminal violations, as specified in Part II.B. (S)

(S) [redacted] (S)

(S) [redacted] Part II.E of these Guidelines sets out conditions and approval requirements for extraterritorial activities. As provided in Part II.E, these activities require a request from or approval of the Director of Central Intelligence or a designee. This requirement ensures that extraterritorial activities under these Guidelines are properly coordinated with other agencies in the Intelligence Community, so that their authorities and capabilities are also brought to bear as appropriate to protect the national security, consistent with Executive Order 12333 or a successor order. (S)

The FBI may also provide assistance to state and local governments, and to foreign law enforcement, intelligence, and security agencies, in investigations relating to threats to the national security. Part III of these Guidelines specifies standards and procedures for the provision of such assistance. (U)

B. FOREIGN INTELLIGENCE COLLECTION (U)

The FBI's functions pursuant to Executive Order 12333 Sections 1.6, 1.14, 2.3, and 2.4 include engaging in foreign intelligence collection and providing operational support for other components of the U.S. Intelligence Community. This role is frequently critical in collecting foreign intelligence within the United States because the authorized domestic activities of other intelligence agencies are more constrained than those of the FBI under applicable statutory law and Executive Order 12333. (U)

Part IV of these Guidelines provides standards and procedures for the provision of such assistance by the FBI to other federal intelligence agencies and the collection of foreign intelligence by the FBI. (U)

C. STRATEGIC ANALYSIS (U)

Executive Order 12333 Section 1.14(d) states that the FBI shall "[p]roduce and disseminate foreign intelligence and counterintelligence." The Executive Order further provides, in Section 1.1(a), that "[m]aximum emphasis should be given to fostering analytical competition among appropriate elements of the Intelligence Community." Given the magnitude and potential consequences of terrorist threats and other threats to the national security, it is imperative that the FBI develop and maintain a strong analytic capacity to identify, examine, assess, and appropriately disseminate information concerning terrorist threats and to produce and disseminate other analysis relating to national security matters. (U)

Part VI of these Guidelines accordingly authorizes the FBI to examine and analyze information to produce and disseminate foreign intelligence and counterintelligence. Part VI provides that the FBI may draw on information from any source permitted by law in carrying out this analytic function, and may supplement the information in its possession, for purposes of these analytic activities, through the use of the methods authorized in threat assessments, such as obtaining publicly available information and checking government records. (U)

D. RETENTION AND DISSEMINATION OF INFORMATION (U)

Part VII of these Guidelines requires the maintenance of adequate records and information relating to investigations and other activities under these Guidelines, and provides standards for the sharing and dissemination of information obtained in such investigations and activities. (U)

Part VII includes, in Subpart B.2, provisions for sharing of information and consultation with other Department of Justice components, which reflect legal reforms and policies adopted by the Attorney General following the September 11, 2001, terrorist attack. Consistent with legal norms and standards of effective management, all relevant components, including the Criminal Division, relevant United States Attorneys' offices, and the Office of Intelligence Policy and Review, must be fully informed about the nature, scope, and conduct of national security investigations and other activities under these Guidelines. The Attorney General can most effectively direct and control such investigations and activities only if all relevant Department of Justice components are able to offer advice and recommendations, both strategic and tactical, about their conduct and goals. The overriding need to protect the United States and its people from terrorism and other threats to the national security requires a full and free exchange of information and ideas. (U)

I. GENERAL AUTHORITIES AND PRINCIPLES (U)

A. GENERAL AUTHORITIES (U)

1. The FBI is authorized to conduct investigations to obtain information concerning or to protect against threats to the national security, including investigations of crimes involved in or related to threats to the national security, as provided in Parts II and V of these Guidelines. Threats to the national security are:

a. International terrorism.

b. Espionage and other intelligence activities, sabotage, or assassination, conducted by, for, or on behalf of foreign powers, organizations, or persons.

1. The FBI may conduct background inquiries concerning consenting individuals when requested by foreign governments or agencies. (U)

2. At the request of foreign law enforcement, intelligence, or security agencies, the FBI may, within the United States, conduct intelligence or security related investigations or provide assistance to such investigations by such agencies, consistent with the national security interests of the United States and with due consideration of the effect on any identifiable United States person. Such requests must be in writing and must identify the information sought and specify the purpose of the investigation. Investigations or assistance under this paragraph must be approved by FBI Headquarters (S)

b1
b2
b7E

(S)

3. The FBI may not provide assistance to foreign law enforcement, intelligence, or security officers conducting investigations within the United States unless such officers have provided prior notification to the Department of State as required by 18 U.S.C. 951. (U)

4. The FBI may provide other material and technical assistance to foreign governments to the extent not otherwise prohibited by law. (U)

IV. FOREIGN INTELLIGENCE COLLECTION AND ASSISTANCE TO INTELLIGENCE AGENCIES (U)

A. FOREIGN INTELLIGENCE COLLECTION (U)

1. The FBI may collect foreign intelligence in response to requirements of topical interest published by an entity authorized by the Director of Central Intelligence to establish such requirements, including, but not limited to, the National HUMINT Requirements Tasking Center. When approved by the Attorney General, the Deputy Attorney General, or an official designated by the Attorney General, the FBI may collect other foreign intelligence in response to tasking specifically levied on the FBI by an official of the Intelligence Community designated by the President. Upon a request by an official of the Intelligence Community designated by the President, the FBI may also collect foreign intelligence to clarify or complete foreign intelligence previously disseminated by the FBI. Copies of such requests shall be provided to the Office of Intelligence Policy and Review. (U)

2. The FBI may also collect foreign intelligence, if consistent with Executive Order 12333 or a successor order, as directed by the Attorney General, the Deputy Attorney General, or an official designated by the Attorney General. (U)

(S) 3.

B. OPERATIONAL SUPPORT (U)

1. When approved by the Attorney General, the Deputy Attorney General, or an official designated by the Attorney General, the FBI may provide operational support to authorized intelligence activities of other entities of the Intelligence Community upon a request made or confirmed in writing by an official of the Intelligence Community designated by the President. The request shall describe the type and duration of support required, the reasons why the FBI is being requested to furnish the assistance, and the techniques that are expected to be utilized, and shall certify that such assistance is necessary to an authorized activity of the requesting entity. (U)

2. The support may include techniques set forth in the approved request and, with the approval of FBI Headquarters, any other technique that does not substantially alter the character of the support. The FBI shall promptly notify the Office of Intelligence Policy and Review of the utilization of any such additional techniques. (U)

3. The FBI may recruit new assets to obtain information or services needed to furnish the requested support, subject to the same standards and procedures applicable to other FBI assets. (U)

C. CENTRAL INTELLIGENCE AGENCY AND DEPARTMENT OF DEFENSE ACTIVITIES WITHIN THE UNITED STATES (U)

(S) 1.

(S)

b1
b2
b7E

(S) 2.

(S)

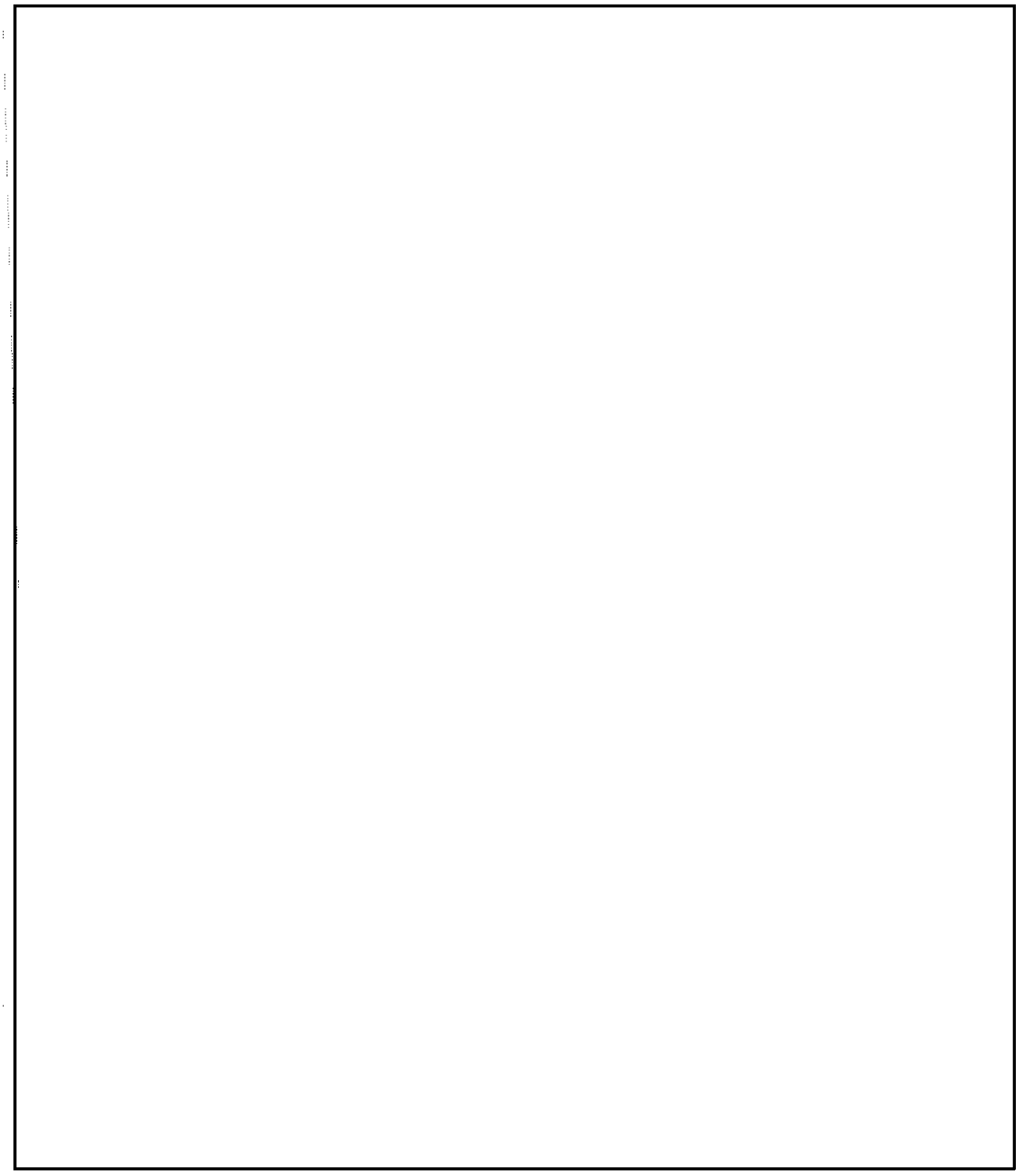
(S)

V. INVESTIGATIVE TECHNIQUES (U)

(S)

b1
b2
b7E

(S)



b1
b2
b7E

VI. [redacted] (U)

[redacted]

b2
b7E

(U)

VII. RETENTION AND DISSEMINATION OF INFORMATION (U)

A. INFORMATION SYSTEMS AND DATABASES (U)

1. The FBI shall retain records relating to preliminary and full investigations, foreign intelligence collection and support activities, and other activities under these Guidelines in accordance with a records retention plan approved by the National Archives and Records Administration. All such records shall be available for review upon request by the Office of Intelligence Policy and Review, including all information in the database or records system described in paragraph 2. (U)

2. The FBI shall maintain a database or records system that permits the prompt retrieval of the following information:

(S) a. The identity and status of each preliminary or full investigation (open or closed). [redacted] (S)

b1
b2
b7E

(S) b. The number of preliminary investigations [redacted] (S)

(S) c. The number of full investigations [redacted] (S)

(S) d. [redacted] (S)

(S) e. [redacted] (S)

B. INFORMATION SHARING (U)

Legal rules and Department of Justice policies regarding information sharing and interagency coordination have been significantly modified since the September 11, 2001, terrorist attack by statutory reforms and new Attorney General guidelines. The general principle reflected in current laws and policies is that information should be shared as consistently and fully as possible among agencies with relevant responsibilities to protect the United States and its people from terrorism and other threats to the national security, except as limited by specific constraints on such sharing. Under this general principle, the FBI shall provide information expeditiously to other agencies in the Intelligence Community, so that these agencies can take action in a timely manner to protect the national security in accordance with their lawful functions. This Subpart provides standards and procedures for the sharing and dissemination of information obtained in national security investigations, foreign intelligence collection, and other activities under these Guidelines. (U)

1. General (U)

a. Information may be disseminated with the consent of the person whom the information concerns, or where necessary to protect life or property from threatened force or violence, otherwise necessary for the safety or security of persons or property or for the prevention of crime, or necessary to obtain information for the conduct of a lawful investigation by the FBI. (U)

b. Information that is publicly available or does not identify United States persons may be disseminated for any lawful purpose. (U)

c. Dissemination of information provided to the FBI by other Intelligence Community agencies is subject to applicable agreements and understandings with such agencies concerning the dissemination of such information. (U)

2. Department of Justice (U)

a. The FBI may share information obtained through activities under these Guidelines with other components of the Department of Justice. (U)

b. The Criminal Division and the Office of Intelligence Policy and Review shall have access to all information obtained through activities under these Guidelines except as limited by orders issued by the Foreign Intelligence Surveillance Court, controls imposed by the originators of sensitive material, or restrictions established by the Attorney General or the Deputy Attorney General in particular cases. (U)

c. The FBI shall keep the Criminal Division and the Office of Intelligence Policy and Review apprised of all information obtained through activities under these Guidelines that is necessary to the ability of the United States to investigate or protect against threats to the national security, subject to the limits noted in subparagraph b. The FBI shall also keep the Criminal Division and the Office of Intelligence Policy and Review apprised of information concerning any crime which is obtained through activities under these Guidelines. (U)

d. As part of its responsibility under subparagraphs b. and c., the FBI shall provide to the Criminal Division and the Office of Intelligence Policy and Review notices of the initiation of investigations and annual notices and summaries as provided in Part II.B.2 and .D.4 of these Guidelines, and shall make available to the Criminal Division and the Office of Intelligence Policy and Review relevant information from investigative files. The Criminal Division shall adhere to any reasonable conditions on the storage and disclosure of such documents and information that the FBI and the Office of Intelligence Policy and Review may require. The FBI and the Criminal Division may adopt by mutual agreement exceptions to the provision of notices of the initiation of investigations and annual notices and summaries to the Criminal Division, and the FBI and the Office

of Intelligence Policy and Review may adopt by mutual agreement exceptions to the provision of notices of initiation of investigations and annual notices and summaries to the Office of Intelligence and Policy Review. (U)

e. The FBI, the Criminal Division, and the Office of Intelligence Policy and Review shall consult with each other concerning national security investigations and other activities under these Guidelines, and shall meet regularly to conduct such consultations. Consultations may also be conducted directly between two or more components at any time. Consultations may include the exchange of advice and information on all issues necessary to the ability of the United States to investigate or protect against threats to the national security, including protection against such threats through criminal investigation and prosecution. Consultations are subject to any limitations in orders of the Foreign Intelligence Surveillance Court and restrictions established by the Attorney General or the Deputy Attorney General in particular cases. Disagreements arising from consultations may be presented to the Deputy Attorney General or the Attorney General for resolution. (U)

f. Subject to subparagraphs g. and h., relevant United States Attorneys' offices shall receive information and engage in consultations to the same extent as the Criminal Division. Thus, the relevant United States Attorneys' offices shall have access to information, shall be kept apprised of information necessary to protect national security, shall be kept apprised of information concerning crimes, shall receive notices of the initiation of investigations and annual summaries as provided in Part II.B.2 and .D.4 of these Guidelines, and shall have access to FBI files, to the same extent as the Criminal Division. The relevant United States Attorneys' offices shall receive such access and information from the FBI field offices. The relevant United States Attorneys' offices also may and shall engage in regular consultations with the FBI and the Office of Intelligence Policy and Review to the same extent as the Criminal Division. (U)

g. In espionage cases, dissemination of information to United States Attorneys' offices and consultations between the FBI and United States Attorneys' offices are subject to authorization by the Criminal Division. In an emergency, the FBI may disseminate information to, and consult with, a United States Attorney's office concerning an espionage investigation without the approval of the Criminal Division, but shall notify the Criminal Division as soon as possible thereafter. (U)

h. Information disseminated to a United States Attorney's office pursuant to subparagraph f. shall be disseminated only to the United States Attorney and/or any Assistant United States Attorneys designated to the Department of Justice by the United States Attorney as points of contact to receive such information. The United States Attorneys and designated Assistant United States Attorneys shall have appropriate security clearances and shall receive training in the handling of classified information and information derived from FISA, including training concerning restrictions on the use and dissemination of such information. (U)

3. Intelligence Community, Federal Law Enforcement Agencies, and Department of Homeland Security (U)

a. The FBI shall carry out the requirements of the Memorandum of Understanding Between the Intelligence Community, Federal Law Enforcement Agencies, and the Department of Homeland Security Concerning Information Sharing ("Memorandum of Understanding"), signed by the Attorney General on March 4, 2003. As provided in the Memorandum of Understanding and subject to its provisions, these requirements include timely sharing by the FBI of covered information with other covered entities having a need-to-know, based on a broad interpretation of the missions of the prospective recipients. As used in this paragraph:

1) 'covered entity' has the same meaning as in the Memorandum of Understanding, including any element of the Department of Homeland Security (and that Department itself); any element of the Intelligence Community (including the Central Intelligence Agency and the Terrorist Threat

Integration Center) or of the Department of Justice; and any other entity having federal law enforcement responsibilities;

2) 'covered information' has the same meaning as in the Memorandum of Understanding, including terrorism information, weapons of mass destruction information, and vulnerabilities information, as well as analyses based wholly or in part on such covered information;

3) 'need-to-know,' 'infrastructure,' 'terrorism information,' 'vulnerabilities information,' and 'weapons of mass destruction information' have the same meanings as in the Memorandum of Understanding; and

4) 'timely sharing' of covered information means provision by the FBI of covered information, subject to section 3(h) and other provisions of the Memorandum of Understanding, to other covered entities having a need-to-know: (i) immediately where the FBI reasonably believes that the information relates to a potential terrorism or weapons of mass destruction threat, to the United States Homeland, its infrastructure, or to United States persons or interests, and (ii) as expeditiously as possible with respect to other covered information. (U)

b. All procedures, guidelines, and mechanisms under the Memorandum of Understanding shall be designed and implemented, and all determinations with regard to sharing information covered by the Memorandum of Understanding shall be made, with the understood, overriding priority of preventing, preempting, and disrupting terrorist threats to the United States. In some cases, this priority will dictate the provision of information even where doing so may affect criminal prosecutions or ongoing law enforcement or intelligence operations. However, consistent with this overriding priority, the FBI shall act in a manner to protect, to the greatest extent possible, these other significant interests, including the protection of intelligence and sensitive law enforcement sources and methods, other classified information, and sensitive operational and prosecutorial information. (U)

c. To the greatest extent possible, information should be shared among covered entities with relevant missions and responsibilities, and there should be transparency among them with regard to their activities to preempt, prevent, and disrupt terrorist attacks against United States persons and interests. Except as otherwise specified in the Memorandum of Understanding, or mandated by relevant federal statutes or Presidential Directives, procedures and mechanisms for information sharing, use, and handling shall be interpreted and implemented consistently and reciprocally regardless of the role a particular entity plays as a provider or recipient of covered information. (U)

4. Federal Authorities (U)

The FBI may disseminate information obtained through activities under these Guidelines to other federal authorities when:

a. the information relates to a crime or other violation of law or regulation which falls within the recipient's investigative jurisdiction, or the information otherwise relates to the recipient's authorized responsibilities;

b. the recipient is a component of the Intelligence Community, and the information is provided to allow the recipient to determine whether the information is relevant to its responsibilities and can be retained or used;

c. the information is required to be furnished to another federal agency by Executive Order 10450 or its successor; or

d. the information is required to be disseminated by statute, Presidential directive, National Security Council directive, Attorney General directive, or interagency agreement approved by the Attorney General. (U)

5. State and Local Authorities (U)

The FBI may disseminate information obtained through activities under these Guidelines to state and local authorities when:

a. the information relates to a crime or other violation of law or regulation which falls within the recipient's jurisdiction, and the dissemination is consistent with national security;

b. the dissemination is for the purpose of preventing or responding to a threat to the national security, or to public safety, including a threat to the life, health, or safety of any individual or community; or

c. the information is required to be disseminated by statute, Presidential directive, National Security Council directive, Attorney General directive, or intergovernmental agreement approved by the Attorney General. (U)

6. Foreign Authorities (U)

a. The FBI may disseminate information obtained through activities under these Guidelines to foreign authorities when:

1) the dissemination of the information is in the interest of the national security of the United States, or the information is relevant to the recipient's authorized responsibilities and its dissemination is consistent with the national security interests of the United States, and the FBI has considered the effect such dissemination may reasonably be expected to have on any identifiable United States person; or

2) the information is required to be disseminated by statute or treaty, Presidential directive or executive agreement, National Security Council directive, or Attorney General directive. (U)

b. Dissemination to foreign authorities having significant implications for foreign relations shall be coordinated with the Department of State. (U)

7. Congressional Committees (U)

Except for briefings and testimony on matters of general intelligence interest, information obtained through activities under these Guidelines may be disseminated to appropriate congressional committees when authorized by the Attorney General, the Deputy Attorney General, or an official designated by the Attorney General. Any agency requesting or involved in the collection of the information shall be consulted prior to such dissemination. A request for United States person information that has been withheld from dissemination under this paragraph shall be referred to the Attorney General, the Deputy Attorney General, or an official designated by the Attorney General, for resolution. (U)

8. White House (U)

In order to carry out their responsibilities, the President, the Vice President, the Assistant to the President for National Security Affairs, the Assistant to the President for Homeland Security Affairs, the National Security Council and its staff, the Homeland Security Council and its staff, and other White House officials and offices require information from all federal agencies, including foreign intelligence, and information relating to international terrorism and other threats to the national security. The FBI accordingly may disseminate information obtained through activities under these Guidelines to the White House, subject to the following standards and procedures: (U)

a. Requests to the FBI for such information from the White House shall be made through the National Security Council staff or Homeland Security Council staff including, but not limited to, the National Security Council Legal and Intelligence Directorates and Office of Combating Terrorism. (U)

b. Compromising information concerning domestic officials or political organizations, or information concerning activities of United States persons intended to affect the political process in the United States, may be disseminated to the White House only with the approval of the Attorney General, based on a determination that such dissemination is needed for foreign intelligence purposes, for the purpose of protecting against international terrorism or other threats to the national security, or for the conduct of foreign affairs. However, such approval is not required for dissemination to the White House of information concerning efforts of foreign intelligence services to penetrate the White House, or concerning contacts by White House personnel with foreign intelligence service personnel. (U)

c. Examples of types of information that are suitable for dissemination to the White House on a routine basis include, but are not limited to:

1) information concerning international terrorism;

2) information concerning activities of foreign intelligence services in the United States;

3) information indicative of imminent hostilities involving any foreign power;

4) information concerning potential cyber threats to the United States or its allies;

5) information indicative of policy positions adopted by foreign officials, governments, or powers, or their reactions to United States foreign policy initiatives;

6) information relating to possible changes in leadership positions of foreign governments, parties, factions, or powers;

7) information concerning foreign economic or foreign political matters that might have national security ramifications; and

8) information set forth in regularly published national intelligence requirements. (U)

d. The limitations on dissemination of information by the FBI to the White House under these Guidelines do not apply to dissemination to the White House of information acquired in the course of an FBI investigation requested by the White House into the background of a potential employee or appointee, or responses to requests from the White House under Executive Order 10450. (U)

C. SPECIAL STATUTORY REQUIREMENTS (U)

1. Dissemination of information acquired under the Foreign Intelligence Surveillance Act is subject to minimization procedures approved by the Foreign Intelligence Surveillance Court and other requirements specified in that Act. (U)

2. Information obtained through the use of National Security Letters under 15 U.S.C. 1681v may be disseminated in conformity with the general standards of this Part. Information obtained through the use of National Security Letters under other statutes may be disseminated in conformity with the general standards of this Part, subject to any applicable limitations in their governing statutory provisions: 12 U.S.C. 3414(a)(5)(B); 15 U.S.C. 1681u(f); 18 U.S.C. 2709(d); 50 U.S.C. 436(e). (U)

VIII. DEFINITIONS (U)

A. AGENT OF A FOREIGN POWER:

1. any person who is not a United States person and who:

a. acts in the United States as an officer or employee of a foreign power, or as a member of a group engaged in international terrorism or activities in preparation therefor; or

b. acts for or on behalf of a foreign power which engages in clandestine intelligence activities in the United States contrary to the interests of the United States, when the circumstances of such person's presence in the United States indicate that such person may engage in such activities in the United States, or when such person knowingly aids or abets any person in the conduct of such activities or knowingly conspires with any person to engage in such activities; or

2. any person who:

a. knowingly engages in clandestine intelligence gathering activities for or on behalf of a foreign power, which activities involve or may involve a violation of the criminal statutes of the United States;

b. pursuant to the direction of an intelligence service or network of a foreign power, knowingly engages in any other clandestine intelligence activities for or on behalf of such foreign power, which activities involve or are about to involve a violation of the criminal statutes of the United States;

c. knowingly engages in sabotage or international terrorism, or activities that are in preparation therefor, for or on behalf of a foreign power;

d. knowingly enters the United States under a false or fraudulent identity for or on behalf of a foreign power or, while in the United States, knowingly assumes a false or fraudulent identity for or on behalf of a foreign power; or

e. knowingly aids or abets any person in the conduct of activities described in subparagraph a., b., or c., or knowingly conspires with any person to engage in such activities. (U)

B. CONSENSUAL MONITORING OF COMMUNICATIONS:

monitoring of oral, wire, or electronic communications for which a court order or warrant is not legally required because of the consent of a party to the communication. (U)

C. COUNTERINTELLIGENCE:

information gathered and activities conducted to protect against espionage or other intelligence activities, sabotage, or assassinations conducted by, for or on behalf of foreign powers, organizations or persons, or international terrorist activities, but not including personnel, physical, document or communications security programs. (U)

D. CRIME INVOLVED IN OR RELATED TO A THREAT TO THE NATIONAL SECURITY:

both crimes directly involved in activities constituting a threat to the national security, and crimes that are preparatory for or facilitate or support such activities. For example, if international terrorists engage in a bank robbery in order to finance their terrorist activities, the bank robbery is a crime involved in or related to a threat to the national security. (U)

(U) • **E.** [redacted] (S)

b2
b7E

F. FOR OR ON BEHALF OF A FOREIGN POWER:

the determination that activities are for or on behalf of a foreign power shall be based on consideration of the extent to which the foreign power is involved in:

1. control or policy direction;
2. financial or material support; or
3. leadership, assignments, or discipline. (U)

G. FOREIGN COMPUTER INTRUSION:

the use or attempted use of any cyber-activity or other means by, for, or on behalf of a foreign power to scan, probe, or gain unauthorized access into one or more U.S.-based computers. (U)

H. FOREIGN CONSULAR ESTABLISHMENT:

the buildings or parts of buildings and the land ancillary thereto, irrespective of ownership, used exclusively by a foreign government for the purposes of a consular post. (U)

(2) being influenced to commit or aid in the committing, or to collude in, or allow, any fraud, or make opportunity for the commission of any fraud, on the United States; or

(3) being induced to do or omit to do any act in violation of the official duty of such official or person,

shall be fined in an amount not more than 3 times the monetary equivalent of the thing of value, or imprisoned for not more than 15 years, or both. A violation of this section shall be subject to chapter 227 of title 18, United States Code, and the provisions of the United States Sentencing Guidelines.

SEC. 330. INTERNATIONAL COOPERATION IN INVESTIGATIONS OF MONEY LAUNDERING, FINANCIAL CRIMES, AND THE FINANCES OF TERRORIST GROUPS.

(a) Negotiations. It is the sense of the Congress that the President should direct the Secretary of State, the Attorney General, or the Secretary of the Treasury, as appropriate, and in consultation with the Board of Governors of the Federal Reserve System, to seek to enter into negotiations with the appropriate financial supervisory agencies and other officials of any foreign country the financial institutions of which do business with United States financial institutions or which may be utilized by any foreign terrorist organization (as designated under section 219 of the Immigration and Nationality Act), any person who is a member or representative of any such organization, or any person engaged in money laundering or financial or other crimes.

(b) Purposes of Negotiations. It is the sense of the Congress that, in

carrying out any negotiations described in paragraph (1), the President should direct the Secretary of State, the Attorney General, or the Secretary of the Treasury, as appropriate, to seek to enter into and further cooperative efforts, voluntary information exchanges, the use of letters rogatory, mutual legal assistance treaties, and international agreements to--

(1) ensure that foreign banks and other financial institutions maintain adequate records of transaction and account information relating to any foreign terrorist organization (as designated under section 219 of the Immigration and Nationality Act), any person who is a member or representative of any such organization, or any person engaged in money laundering or financial or other crimes; and

(2) establish a mechanism whereby such records may be made available to United States law enforcement officials and domestic financial institution supervisors, when appropriate.

Subtitle B--Bank Secrecy Act Amendments and Related Improvements

SEC. 351. AMENDMENTS RELATING TO REPORTING OF SUSPICIOUS ACTIVITIES.

(a) Amendment Relating to Civil Liability Immunity for Disclosures. Section 5318(g)(3) of title 31, United States Code, is amended to read as follows:

"(3) Liability for disclosures.

"(A) In general. Any financial institution that makes a voluntary