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

DATE: 06-22-2007
CLASSIFIED BY 65179/dmh/ksr/cak
REASON: 1.4 (c)
DECLASSIFY ON: 06-22-2032

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

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

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, the FD-542 macro must be used to present both required data elements and supporting narratives.

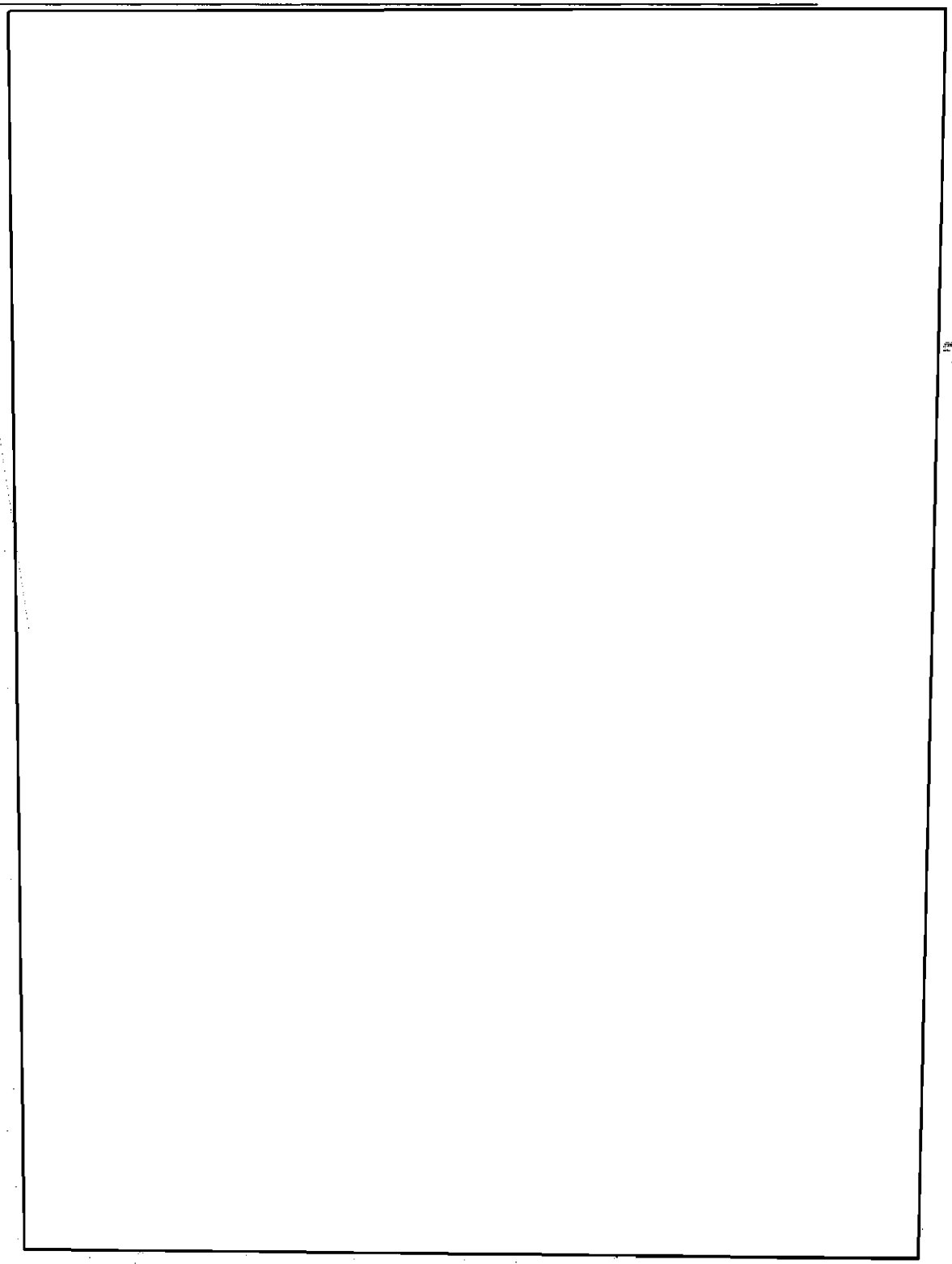
2. Data from the FD-542 is uploaded into the Electronic Case File, serialized into the electronic file, and then automatically transferred into the appropriate IIIA database. IIIA allows for ad hoc querying of data, and the printing of reports.

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

C. (S)

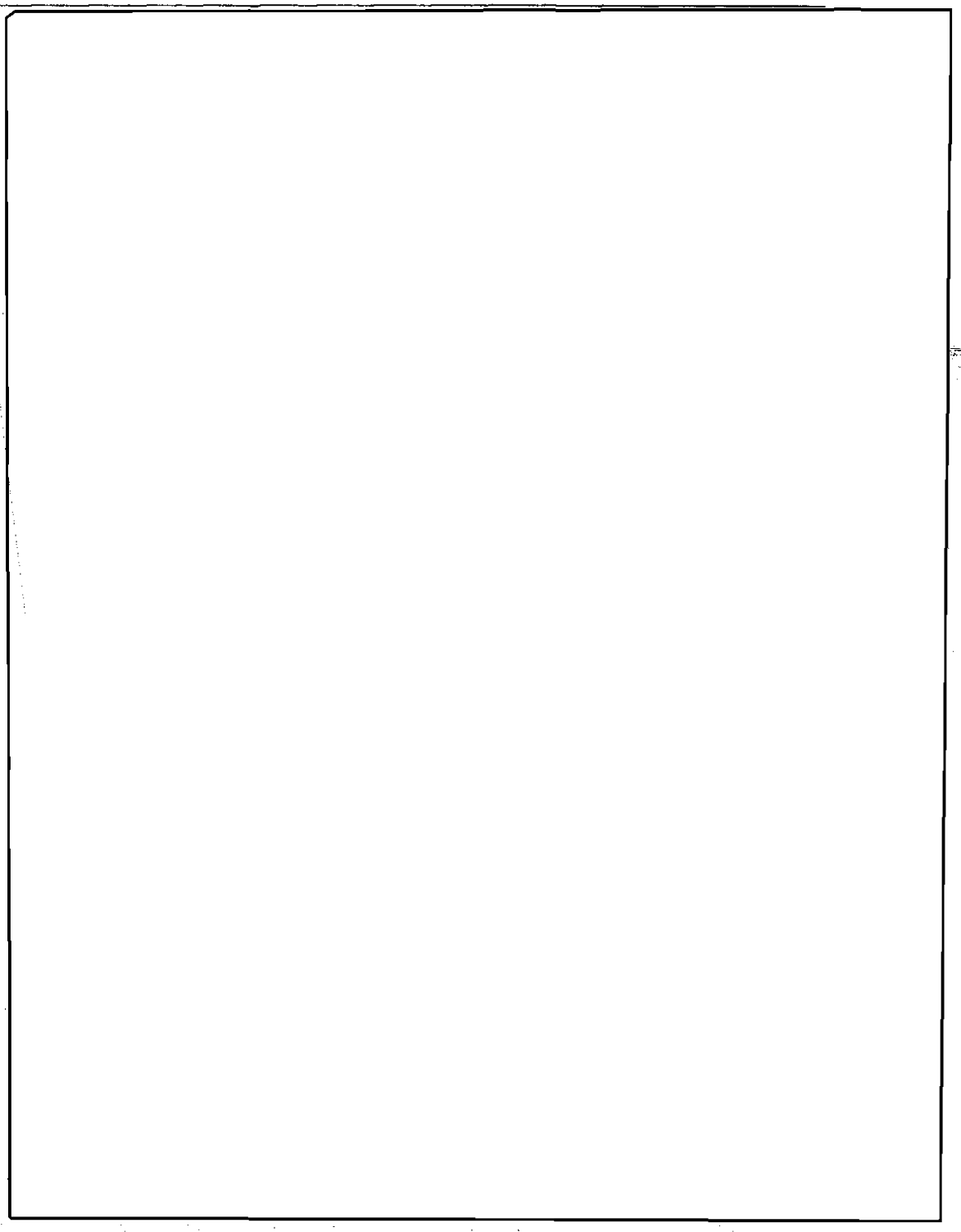
b1
b2
b7E

(S)



b1
b2
b7E

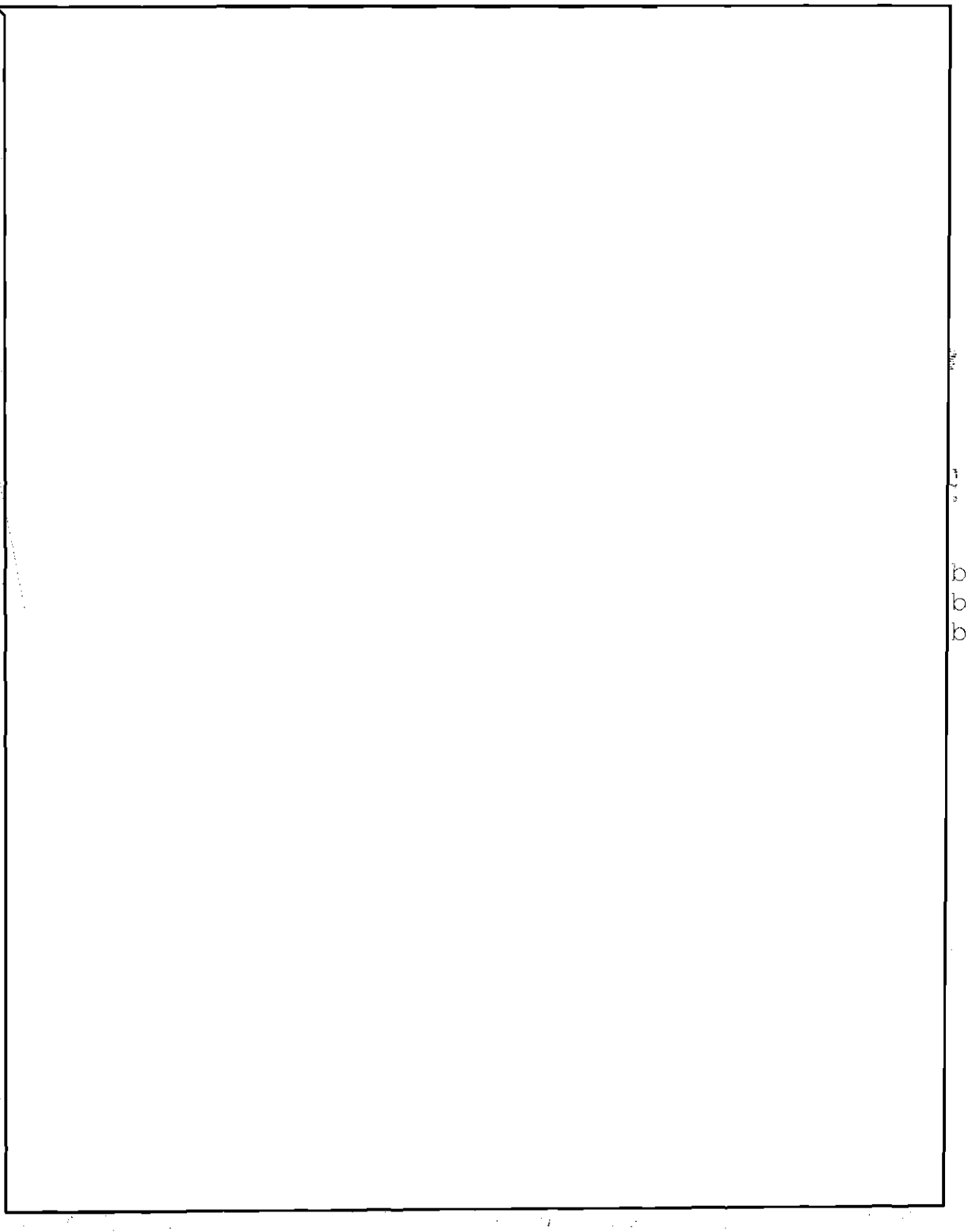
(S)



b1
b2
b7E

~~SECRET~~ /NOFORN

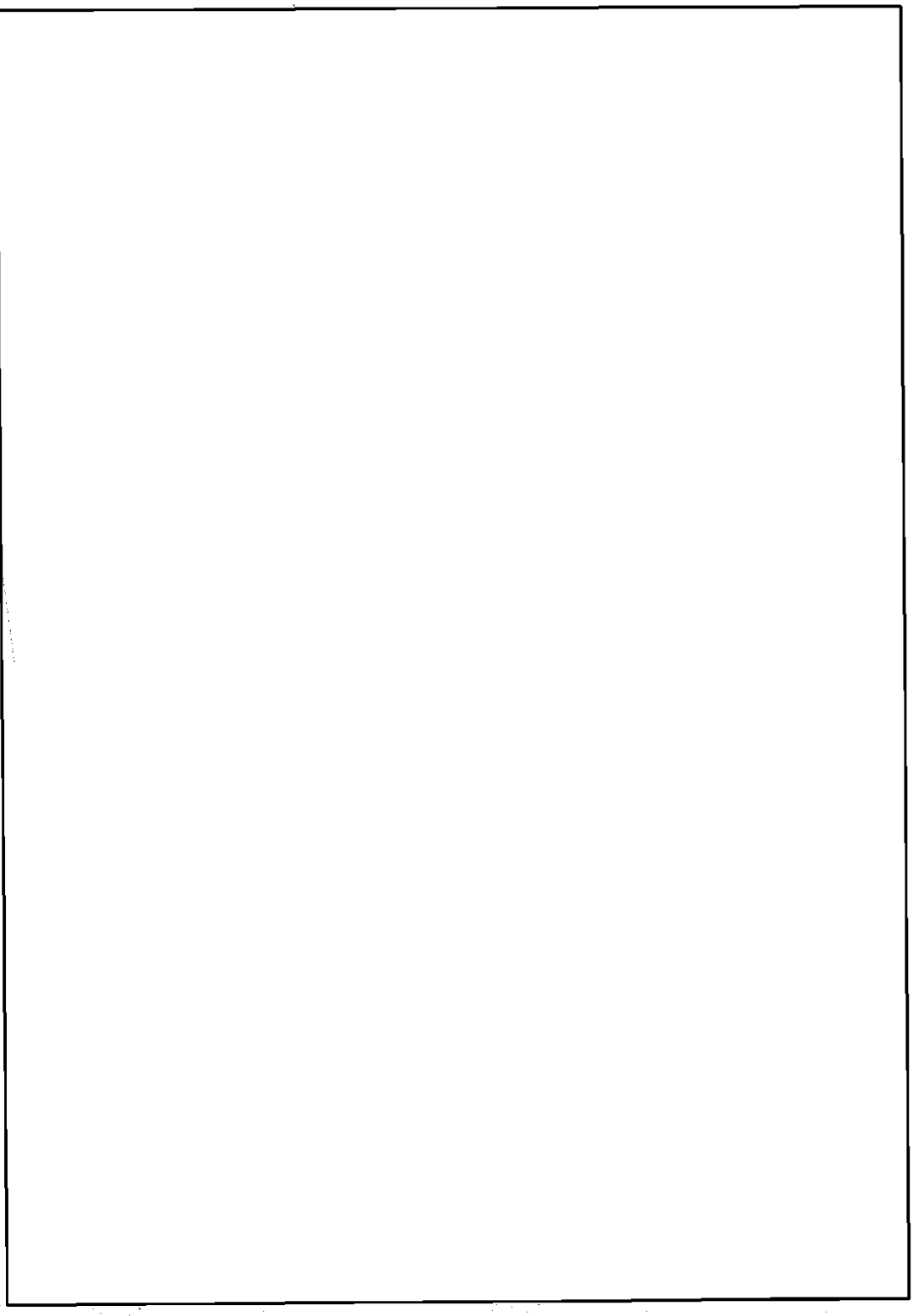
(S)



b1
b2
b7E

~~SECRET~~ /NOFORN

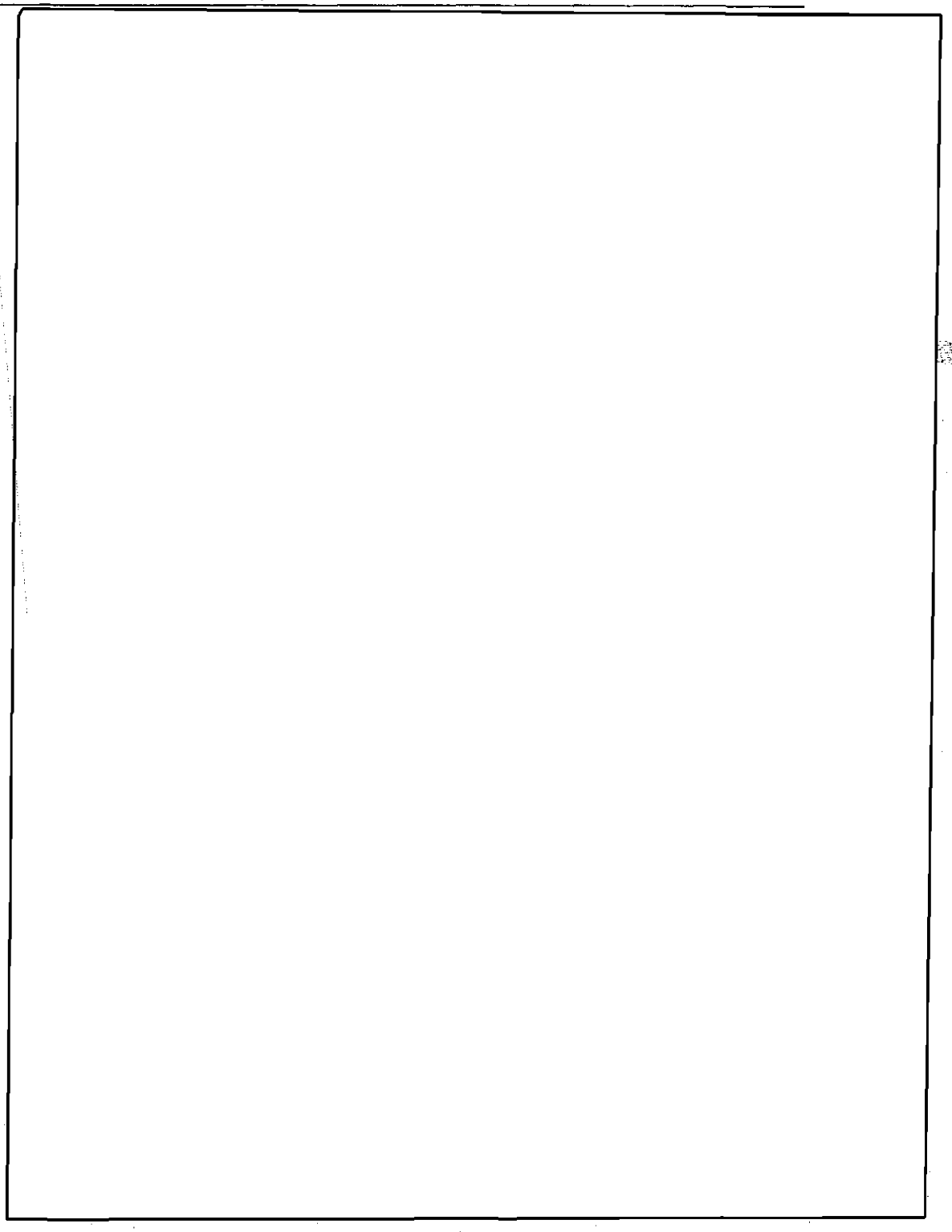
(S)



b1
b2
b7E

~~SECRET~~ /NOFORN

(S)

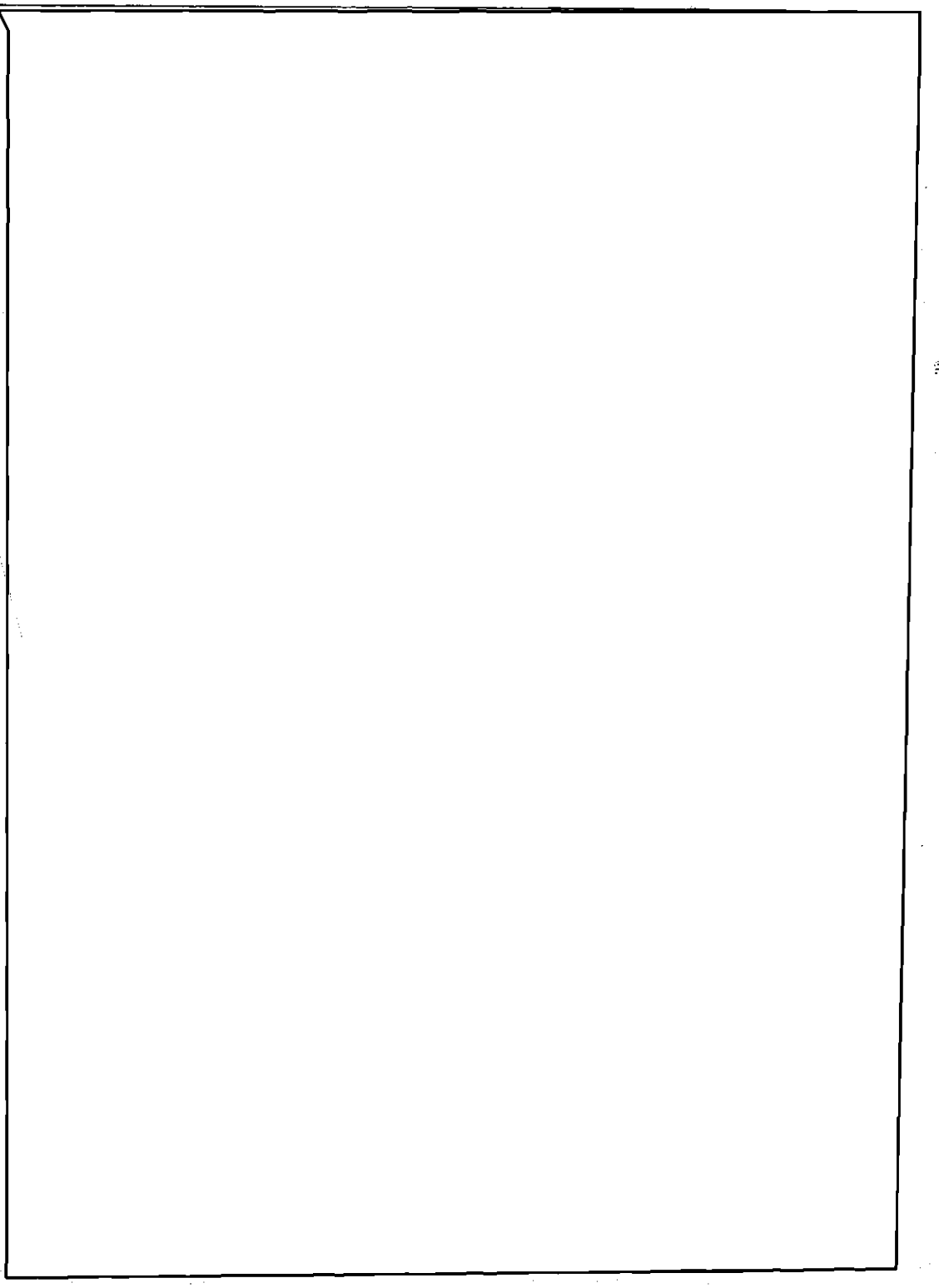


b1
b2
b7E

~~SECRET~~ /NOFORN

SECRET /NOFORN

(S)



b1
b2
b7E

SECRET /NOFORN

(S)

[redacted]

b1
b2
b7E

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

Section 2-54 (U) IIIA (Integrated Intelligence Information Application)

A. (U) IIIA is used to collate information; e.g., (a) biographic data, and information regarding (b) major cases, (c) [redacted] which is pertinent to the FBI's foreign counterintelligence, foreign intelligence, international terrorism and domestic terrorism investigations. IIIA allows [redacted] See: IIIA Manual, Part A, Section 1.

b2
b7E

B. (U) IIIA permits [redacted] thus making it possible to track information [redacted]

C. (U) IIIA signons and passwords are controlled by FBI Headquarters, and are assigned on a need-to-know basis. Access to specific sensitive case information, and even specific serial information can be restricted to specific people only.

D. (U) Additional types of data available through the IIIA include [redacted]

b2
b7E

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

b2

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.

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.

[mission.]

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

[Section 19-05 [Closing International Terrorism Investigations

[A. General

[1. Prior to closing an international terrorism investigation in the 315 classification, [Field offices must ensure all reasonable investigative techniques have been [exploited. By closing the investigation, the field office is affirming it has [exhausted all reasonable and practical intelligence collection methods with [respect to the investigation.

[2. If the investigation has uncovered criminal violations of state or federal law, then [a declination from the United States Attorney's Office must be received and [documented within the investigative case file.

[B. Closing Communication to FBIHQ

[1. The closing communication will be sent to the Counterterrorism Division to the [attention of the following:

[a) Substantive section/unit

[b) [redacted]

[c) [redacted]

[d) [redacted]

[e) Other sections or units, as appropriate

[f) Appropriate field office or Legal Attaché ("Legat"), if subject relocated

[2. An FD-930 will be enclosed [redacted] b2 b7E

[3. The Details section of the closing communication will contain the following information:

[a) The type of investigation [redacted]

[b) The date it was opened

[c) The date it was converted [redacted] [[redacted] if applicable

[d) If [redacted] then the date and serial number of the most recent

Annual Summary

e) Whether the investigation involves a United States person

f) An assessment of the extent to which the subject is (or members of the group are) aware of the terrorist aims of the foreign power

g) Any sensitive national security matters, which is defined in the NSIG as "a threat to the national security involving the activities of an official of a foreign country other than a threat country, a domestic public official or political candidate, a religious or political organization or an individual prominent in such an organization, or news media, or any other matter which, in the judgment of the official authorizing an investigation, should be brought to the attention of FBI Headquarters and other Department of Justice officials."

h) Name and all aliases of the subject and complete biographical information regarding the subject

i) Subject classification (see D, below)

j) A summary of the investigation to include a list of the investigative techniques used, to include:

(1)
(2)
(3)
(4)
(5)
(6)
(7)
(8)
(9)
(10)
(11)
(12)
(13)
(14)

b2
b7E

2. (S/NF) [redacted] b1 b2 b7D

M. (U) [redacted] CI/CT Operations b2 b7E

1. (S/NF) [redacted] 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 the Computer Investigations and [redacted] is to be sent to C3IU in as near of a realtime basis as possible. The submission of [redacted] will allow the CyD to monitor instances of computer intrusions, fully identify the scope of the crime/intelligence problem and crime/intelligence trends and seek resources, as necessary, to address these matters.

2. (U) [redacted] should include the predication for the investigation, any multi-jurisdiction victims or witnesses, an initial prosecutive opinion from the United States Attorney's Office for FCI/IT matters, contemplated investigative steps, impediments to the investigation and any actual or anticipated assistance from governmental agencies required. b2 b7E

3. (U) Major developments during the investigation, i.e., the use of innovative or sensitive investigative techniques, unusual problems encountered, searches, arrests, information/indictments/complaints or convictions are to be promptly reported to C3IU, via a supplemental [redacted]

4. (U) A closing [redacted] 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 [redacted] can be completed by fax to C3IU or sent to the CyD Watch and Warning Unit.

6. (U) It should be noted that a brief description of the complaint, case or facts of the investigation is to be included in the remarks section [redacted] The CyD will disseminate information to the appropriate government agencies from [redacted] Sensitive information, i.e. [redacted] or other concerns, is to be set forth in an administrative section of the remarks section [redacted]

O. (U) Investigative Accomplishments (FD-542) (see also Section 2-53, supra.)

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

2. (U) The NIPCIP will utilize this automated system to capture additional statistical accomplishments, not already captured in [redacted] system. [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. b2 b7E

3. (U) In working computer intrusion investigations, it is obvious that these matters do not have physical boundaries. In the beginning of an investigation, it is unknown if one computer intrusion is related to another incident or investigation. More often than not, one subject will simultaneously affect victims in multiple divisions. In the end, all of those cases are wrapped into one prosecutable case with only one division claiming statistical accomplishments. In other instances, some computer intrusion cases have foreign and/or juvenile subjects which may never be prosecuted, or the activity turns out to be state-sponsored and the case becomes a TNI - CI/CT matter.

4. (U) As such, the following investigative accomplishments have been incorporated into the FD-542 macro for NIPCIP to account for the additional accomplishments being performed by the field offices. These accomplishments captured by the FD-542 macro are an additional means by which the NIPCIP is measured. The current method of statistical accomplishments through the FD-515 form and [redacted] system will still be maintained, in addition to the FD-542 and [redacted] b2 b7E

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) The Field office claiming the statistical accomplishment should go into WordPerfect, select the FD-542 macro, and enter the appropriate statistical accomplishments. "NIPCIP" should be selected as the Investigative Technique Used (ITU), for the applicable accomplishments.

7. (S) [redacted] b1 b2 b7E

b) (S)

c) (S)

d) (S)

b1
b2
b7E

e) (S)

f) (S)

g) (S)

h) (S)

i) (S)

j) (S)

k) (S)

l) (S)

Intelligence Directive 3/1.

141. (U) National Foreign Intelligence Program: [redacted] b2 b7E

NFIP. *See: Executive Order 12333, Section 3.4(g).*

142. (C) [redacted] b1 b2 b7E

143. (S) [redacted] b1 b2 b7E

144. (S) [redacted] b1 b2 b7E

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.

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] b2 b7E

150. (U) Non-U.S. Person: An undocumented alien, or a foreign national lawfully in the U.S.

[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)

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) [redacted] and (3) [redacted] (U)

b2
b7E

(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)

(S)

b1
b2

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 This can avoid the need to 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)

b2
b7E

(S)

b1
b2
b7E

(S)

b1
b2
b7E

(S)

b1
b2
b7E