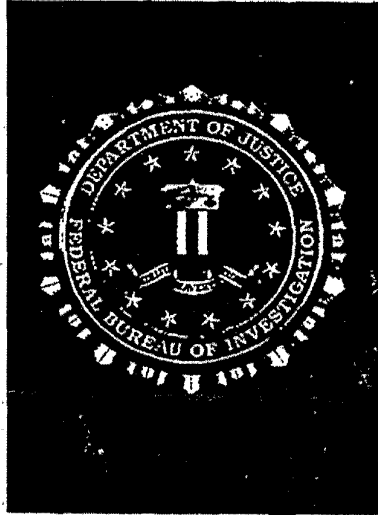


ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 07-08-2009 BY UC 60322 LP/STP/SZ

UNCLASSIFIED
FOR OFFICIAL USE ONLY

Domestic Investigations and Operations Guide



Federal Bureau of Investigation (FBI)

December 16, 2008

This is a privileged document that cannot be released in whole or in part to persons or agencies outside the Federal Bureau of Investigation, nor can it be republished in whole or in part in any written form not containing this statement, including general use pamphlets, without the approval of the Director of the Federal Bureau of Investigation.

UNCLASSIFIED
FOR OFFICIAL USE ONLY

ACLU EC-1

UNCLASSIFIED - FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

GENERAL INFORMATION: Questions or comments pertaining to the DIOG can be directed to:

The Deputy Director's Office

or

FBIHQ, Director's Office, Resource Planning Office (RPO), Division [00]

Corporate Policy Office (CPO)

Division Point of Contact:

b6
b7c

(NOTE: Document is a new publication; no previous DIOG versions are available)

PRIVILEGED INFORMATION:

Any use of this document, including direct quotes or identifiable paraphrasing, will be marked with the following statement:

This is a privileged document that cannot be released in whole or in part to persons or agencies outside the Federal Bureau of Investigation, nor can it be republished in whole or in part in any written form not containing this statement, including general use pamphlets, without the approval of the Director of the Federal Bureau of Investigation.

FOR OFFICIAL FBI INTERNAL USE ONLY—DO NOT DISSEMINATE
FOR OFFICIAL USE ONLY

UNCLASSIFIED - FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

Table of Contents

(U) Preamble..... xi

1. (U) Scope and Purpose.....1

 1.1. (U) Scope1

 1.2. (U) Purpose1

2. (U) General Authorities and Principles2

 2.1. (U) Scope of the Attorney General's Guidelines for Domestic FBI Operations2

 2.2. (U) General FBI Authorities under AGG-Dom3

 2.3. (U) FBI as an Intelligence Agency3

 2.4. (U) FBI Lead Investigative Authorities4

 2.5. (U) Status as Internal Guidance10

 2.6. (U) Departures from the AGG-Dom10

 2.7. (U) Departures from the DIOG11

 2.8. (U) Other FBI Activities Not Limited by AGG-Dom11

 2.9. (U) Use of Classified Investigative Technologies12

 2.10. (U) Application of AGG-Dom and DIOG12

3. (U) Core Values, Roles, and Responsibilities.....13

 3.1. (U) The FBI's Core Values13

 3.2. (U) Deputy Director Roles and Responsibilities14

 3.3. (U) Special Agent/Intelligence Analyst/Task Force Officer/FBI Contractor/Others
 Roles and Responsibilities.....14

 3.4. (U) Supervisor Roles and Responsibilities15

 3.5. (U) Chief Division Counsel Roles and Responsibilities18

 3.6. (U) Office of the General Counsel Roles and Responsibilities18

 3.7. (U) Corporate Policy Office Roles and Responsibilities19

 3.8. (U) Office of Integrity and Compliance Roles and Responsibilities19

 3.9. (U) Operational Program Manager Roles and Responsibilities19

 3.10. (U) Division Compliance Officer Roles and Responsibilities20

 3.11. (U) FBI Headquarters Approval Levels20

4. (U) Privacy and Civil Liberties, and Least Intrusive Methods.....21

 4.1. (U) Civil Liberties and Privacy21

 4.2. (U) Protection of First Amendment Rights24

 4.3. (U) Equal Protection under the Law30

 4.4. (U) Least Intrusive Method34

5. (U) Assessments39

 5.1. (U) Overview39

 5.2. (U) Purpose and Scope40

 5.3. (U) Civil Liberties and Privacy43

 5.4. (U) Authorized Purposes (AGG-Dom, Part II.A.2.—Authorized Activities)44

 5.5. (U//FOUO) Standards for Initiating or Approving an Assessment45

 5.6. (U).Duration, Approval, Notice, Documentation, File Review and Responsible Entity45

UNCLASSIFIED - FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

11.4.4.	(U//FOUO) Standards for Use and Approval Requirements for Investigative Method	121
11.5.	(U) Investigative Method: Consensual Monitoring of Communications, including consensual computer monitoring.....	122
11.5.1.	(U) Summary	122
11.5.2.	(U) Legal Authority	122
11.5.3.	(U) Definition of Investigative Method	122
11.5.4.	(U) Standards for Use and Approval Requirements for Investigative Method ..	123
11.5.5.	(U) Duration of Approval	127
11.5.6.	(U//FOUO) Specific Procedures	128
11.5.7.	(U//FOUO) Compliance and Monitoring.....	129
11.6.	(U) Investigative Method: Use of closed-circuit television, direction finders, and other monitoring devices (Not needing a Court Order).....	130
11.6.1.	(U) Summary	130
11.6.2.	(U) Legal Authority	130
11.6.3.	(U//FOUO) Definition of Investigative Method	130
11.6.4.	(U//FOUO) Standards for Use and Approval Requirements for Investigative Method	131
11.6.5.	(U) Duration of Approval	132
11.6.6.	(U//FOUO) Specific Procedures	132
11.6.7.	(U//FOUO) Compliance and Monitoring.....	133
11.7.	(U) Investigative Method: Polygraph	134
11.7.1.	(U) Summary	134
11.7.2.	(U) Legal Authority	134
11.7.3.	(U//FOUO) Definition of Investigative Method	134
11.7.4.	(U//FOUO) Standards for Use and Approval Requirements for Investigative Method	134
11.7.5.	(U) Duration of Approval	134
11.7.6.	(U//FOUO) Specific Procedures	135
11.7.7.	(U//FOUO) Compliance and Monitoring.....	135
11.8.	(U) Investigative Method: Undercover Operations	136
11.8.1.	(U) Summary	136
11.8.2.	(U) Legal Authority	136
11.8.3.	(U//FOUO) Definition of Investigative Method	136
(U//FOUO)	Distinction Between Sensitive Circumstance and Sensitive Investigative Matter:	137
11.8.4.	(U//FOUO) Standards for Use and Approval Requirements for Investigative Method	137
11.8.5.	(U) Duration of Approval	139
11.8.6.	(U) Additional Guidance.....	139
11.8.7.	(U//FOUO) Compliance and Monitoring, and Reporting Requirements.....	139
11.9.	(U) Investigative Method: Compulsory process as authorized by law, including grand jury subpoenas and other subpoenas, National Security Letters	140
11.9.1.	(U) Federal Grand Jury Subpoena	140
11.9.2.	(U) Administrative Subpoena	152
11.9.3.	(U) National Security Letter	158
11.9.4.	(U) Business Record Under FISA.....	165

UNCLASSIFIED - FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

11.10. (U) Investigative Method: Accessing stored wire and electronic communications and transactional records in conformity with chapter 121 of title 18, United States Code	167
11.10.1. (U) Summary	167
11.10.2. (U) Legal Authority	168
11.10.3. (U) Definition of Investigative Method	168
11.10.4. (U) Approval Requirements for Investigative Method	179
11.10.5. (U) Duration of Approval	179
11.10.6. (U//FOUO) Specific Procedures	179
11.10.7. (U) Notice and Reporting Requirements	180
11.10.8. (U) Other Applicable Policies	180
(U) Stored Communications Quick Reference Guide 5/1/2008	180
11.11. (U) Investigative Method: Pen Registers and Trap and Trace devices in conformity with chapter 206 of Title 18, United States Code, and the Foreign Intelligence Surveillance Act	181
11.11.1. (U) Summary	181
11.11.2. (U) Legal Authority	181
11.11.3. (U) Definition of Investigative Method	181
11.11.4. (U) Standards for Use and Approval Requirements for Investigative Method	181
11.11.5. (U) Duration of Approval	184
11.11.6. (U//FOUO) Specific Procedures	184
11.11.7. (U) Use and Dissemination of Information Derived from Pen Register/Trap and Trace Authorized Pursuant to FISA	185
11.11.8. (U) Notice and Reporting Requirements	186
11.11.9. (U) Special Circumstances	186
11.12. (U) Investigative Method: Electronic Surveillance under Title III and under FISA	193
11.12.1. (U) Summary	193
11.12.2. (U) Legal Authority	193
11.12.3. (U) Definition of Investigative Method	193
11.12.4. (U) Standards for Use and Approval Requirements for Investigative Method	193
11.12.5. (U) Duration of Approval	196
11.12.6. (U) Specific Procedures	196
11.12.7. (U) Notice and Reporting Requirements	199
11.12.8. (U) Compliance and Monitoring	200
11.12.9. (U) Special Circumstances	200
11.12.10. (U) Other Applicable Policies	200
11.13. (U) Investigative Method: Physical searches, including mail openings, requiring judicial order or warrant	201
11.13.1. (U) Summary	201
11.13.2. (U) Legal Authority	201
11.13.3. (U) Definition of Investigative Method	201
11.13.4. (U) Approval Requirements for Investigative Method	204
11.13.5. (U) Duration of Approval	204
11.13.6. (U) Specific Procedures	204
11.14. (U) Investigative Method: Acquisition of foreign intelligence information in conformity with Title VII of the Foreign Intelligence Surveillance Act	213
11.14.1. (U) Summary	213

UNCLASSIFIED - FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

11.14.2. (U) Legal Authority	213
11.14.3. (U) Definition of Investigative Method	213
11.14.4. (U//FOUO) Standards for Use and Approval Requirements for Investigative Method	213
11.14.5. (U) Duration of Approval	213
11.14.6. (U//FOUO) Specific Collection Procedures for Title VII	213
12. (U) Assistance to Other Agencies	216
12.1. (U) Overview	216
12.2. (U) Purpose and Scope	216
12.3. (U//FOUO) Standards for Providing and Approving Investigative Assistance to Other Agencies	217
12.4. (U) Documentation and Record Retention	217
12.5. (U) Duration, Approval and Notice for Investigative Assistance to Other Agencies ..	217
12.6. (U//FOUO) Standards for Providing and Approving Technical Assistance to Foreign, State, Local and Tribal Agencies	225
13. (U) Extraterritorial Provisions	227
13.1. (U) Overview	227
13.2. (U) Purpose and Scope	227
13.3. (U) Legal Attache Program	228
14. (U) Retention and Sharing of Information	229
14.1. (U) Purpose and Scope	229
14.2. (U) The FBI's Records Retention Plan, and Documentation	229
14.3. (U) Information Sharing	230
14.4. (U) Information Related to Criminal Matters	231
A. (U) Coordinating with Prosecutors	231
B. (U) Criminal Matters Outside FBI Jurisdiction	231
C. (U) Reporting of Criminal Activity	232
14.5. (U) Information Related to National Security and Foreign Intelligence Matters	232
(U) Department of Justice	232
(U) White House	233
14.6. (U) Special Statutory Requirements	235
15. (U) Intelligence Analysis and Planning	236
15.1. (U) Overview	236
15.2. (U) Purpose and Scope	236
15.3. (U) Civil Liberties and Privacy	237
15.4. (U) Legal Authority	237
15.5. (U//FOUO) Standards for Initiating or Approving Intelligence Analysis and Planning	238
15.6. (U//FOUO) Standards for Initiating or Approving the Use of an Authorized Investigative Method in Intelligence Analysis and Planning	238
15.7. (U) Authorized Activities in Intelligence Analysis and Planning	238
16. (U) Undisclosed Participation (UDP)	242
16.1. (U) Overview	242
16.2. (U) Purpose, Scope, and Definitions	243

UNCLASSIFIED - FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

List of Appendices

Appendix A: The Attorney General's Guidelines for Domestic FBI Operations A-1
Appendix B: Executive Order 12333.....B-1
Appendix C: Sensitive Operations Review Committee..... C-1
Appendix D: Superseded Documents and NFIP, MIOG, and MAOP Sections..... D-1
Appendix E: Key Words, Definitions, and LinksE-1
Appendix F: Acronyms..... F-1
Appendix G: Investigations Manual – Classified Provisions..... G-1

UNCLASSIFIED - FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

(U) Preamble

December 1, 2008

(U) As the primary investigative agency of the federal government, the FBI has the authority and responsibility to investigate all violations of federal law that are not exclusively assigned to another federal agency. The FBI is further vested by law and by Presidential directives with the primary role in carrying out criminal investigations and investigations of threats to the national security of the United States. This includes the lead domestic role in investigating international terrorist threats to the United States, and in conducting counterintelligence activities to counter foreign entities' espionage and intelligence efforts directed against the United States. The FBI is also vested with important functions in collecting foreign intelligence as a member agency of the United States Intelligence Community (USIC). (AGG-Dom, Introduction)

(U) While investigating crime, terrorism, and threats to the national security, and collecting foreign intelligence, the FBI must fully comply with all laws and regulations, including those designed to protect civil liberties and privacy. Through compliance, the FBI will continue to earn the support, confidence and respect of the people of the United States.

(U) To assist the FBI in its mission, the Attorney General signed *The Attorney General's Guidelines for Domestic FBI Operations* (AGG-Dom) on September 29, 2008. The primary purpose of the AGG-Dom and the Domestic Investigations and Operations Guide (DIOG) is to standardize policy so that criminal, national security, and foreign intelligence investigative activities are accomplished in a consistent manner, whenever possible (e.g., same approval, notification, and reporting requirements). In addition to the DIOG, each FBIHQ substantive Division has a policy implementation guide (PG) that supplements this document. Numerous FBI manuals, electronic communications, letterhead memoranda, and other policy documents are incorporated into the DIOG and the substantive Division policy implementation guides, thus, consolidating the FBI's policy guidance. The FBIHQ Corporate Policy Office (CPO) plays an instrumental role in this endeavor. Specifically, the CPO maintains the most current version of the DIOG on its website. As federal statutes, executive orders, Attorney General guidelines, FBI policies, or other relevant authorities change, CPO will electronically update the DIOG after appropriate coordination and required approvals.

(U) The changes implemented by the DIOG should better equip you to protect the people of the United States against crime and threats to the national security and to collect foreign intelligence. This is your document, and it requires your input so that we can provide the best service to our nation. If you discover a need for change, please forward your suggestion to FBIHQ CPO.

(U) Thank you for your outstanding service!

Robert S. Mueller, III
Director

UNCLASSIFIED - FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

1. (U) Scope and Purpose

1.1. (U) Scope

(U) The DIOG applies to all investigative activities and intelligence collection activities conducted by the FBI within the United States or outside the territories of all countries. This policy document does not apply to investigative and intelligence collection activities of the FBI in foreign countries; those are governed by *The Attorney General's Guidelines for Extraterritorial FBI Operations*.

1.2. (U) Purpose

(U) The purpose of the DIOG is to standardize policy so that criminal, national security, and foreign intelligence investigative activities are consistently and uniformly accomplished whenever possible (e.g., same approval, notification, and reporting requirements).

(U) This policy document also stresses the importance of oversight and self-regulation to ensure that all investigative and intelligence collection activities are conducted within Constitutional and statutory parameters and that civil liberties and privacy are protected.

(U) In addition to this policy document, each FBIHQ substantive Division has a PG that supplements the DIOG. As a result, numerous FBI manuals, electronic communications, letterhead memoranda, and other policy documents are incorporated into the DIOG and Division PGs, thus, consolidating FBI policy guidance.

UNCLASSIFIED - FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

11.5. (U) Investigative Method: Consensual Monitoring of Communications, including consensual computer monitoring

11.5.1. (U) Summary

(U) Consensual monitoring of communications may be used in predicated investigations. Its use, including consensual computer monitoring, requires review by the CDC or the OGC. (AGG-Dom, Part V.A.4)

(U//FOUO) **Application:** This investigative method may be used in national security investigations, criminal investigations and positive foreign intelligence collection cases, and for assistance to other agencies when it is not otherwise prohibited by AGG-Dom, Part III.B.2-3. This method cannot be used during an assessment

(U//FOUO) **Note:** For those state, local and tribal governments that do not sanction or provide a law enforcement exception available to the FBI for one-party consensual recording of communications with persons within their jurisdiction; the SAC must approve the consensual monitoring of communications as an OIA. Prior to the SAC authorizing the OIA, one-party consent must be acquired. The SAC may delegate the OIA approval authority to an ASAC or SSA.

11.5.2. (U) Legal Authority

- A. (U) The Fourth Amendment to the United States Constitution and case law interpreting the same;
- B. (U) 18 U.S.C. § 2511(2)(b) & (c);
- C. (U) The Foreign Intelligence Surveillance Act of 1978 (FISA), 50 U.S.C. §§ 1801 et seq., defines "electronic surveillance" to include only those communications "in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes." 50 U.S.C. § 1801(f). If a party to the communication has consented to monitoring, a Title III or FISA court order is not required to monitor those consensual communications; and
- D. (U) Computer Trespasser Exception - 18 U.S.C. § 2511(2)(i).

11.5.3. (U) Definition of Investigative Method

(U) Consensual monitoring is: "monitoring of communications for which a court order or warrant is not legally required because of the consent of a party to the communication." (AGG-Dom, Part VII.A.) Consensual monitoring includes the interception of the content of communications that typically fall into one of three general categories:

- A. (U) Conventional telephone communications or other means of transmitting the human voice through cable, wire, radio frequency (RF), or other similar connections;
- B. (U) Oral communications, typically intercepted through the use of devices that monitor and record oral conversations (e.g., where a body transmitter or recorder or a fixed location transmitter or recorder is used during a face-to-face communication in which a person would have a reasonable expectation of privacy but for the consent of the other party); and

UNCLASSIFIED - FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

C. (U) Communications transmitted between parties using computer protocols, such as e-mail, instant message, chat sessions, text messaging, peer-to-peer communications, or other "electronic communications," as that term is defined in 18 U.S.C. § 2510(12).

(U) The consensual monitoring of communications, including consensual computer monitoring, is subject to legal review by the CDC or the OGC. (AGG-Dom, Part V.A.4)

(U) The computer trespasser exception to the wiretap statute, 18 U.S.C. § 2511(2)(i), relies on the consent of the computer owner-operator and limits the monitoring to only the communications of the trespasser. The statute includes additional limitations on the use of this provision.

11.5.4. (U) Standards for Use and Approval Requirements for Investigative Method

A. (U) General Approval Requirements

(U//FOUO) Except as provided below in Section 11.5.4.B, an SSA may approve the consensual monitoring of communications, including consensual computer monitoring of communications, if the information likely to be obtained is relevant to an ongoing investigation. SSA approval is conditioned on the following criteria being met and documented using the FD-759:

1. (U//FOUO) **Reasons for Monitoring:** There is sufficient factual information supporting the need for the monitoring and that the monitoring is related to the investigative purpose, including, if applicable, a citation to the principal criminal statute involved;
2. (U//FOUO) **Legal Review:** Prior to the initiation of the consensual monitoring, the CDC or the OGC concurred that consensual monitoring under the facts of the investigation is legal. Whenever the monitoring circumstances change substantially, a new FD-759 must be executed and the CDC or OGC must be recontacted to obtain a new concurrence. (AGG-Dom, Part V.A.4.) The following are examples of substantial changes in monitoring circumstances which require a new FD-759: a different consenting party, new interceptees, or a change in the location of a fixed monitoring device.
3. (U) **Consent:** A party to the communication has consented to the monitoring and that consent has been documented according to the below-procedures. Consent may be express or implied. In consensual computer monitoring, for example, implied consent to monitor may exist if users are given notice through a sign-on banner that all users must actively acknowledge (by clicking through) or through other means of obvious notice of possible monitoring. Consent to monitor pursuant to the computer trespasser exception is not provided by a party to the communication per se, but is instead provided by the owner, operator, or systems administrator of the computer to be monitored.
4. (U//FOUO) **Subject:** The monitoring will not intentionally include a third-party who is not of interest to the investigation, except for unavoidable or inadvertent overhears.
5. (U//FOUO) **Location of device:** Appropriate safeguards exist to ensure that the consenting party remains a party to the communication throughout the course of monitoring. If a fixed-location monitoring device is being used, the consenting party

UNCLASSIFIED - FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

has been admonished and agrees to be present during the duration of the monitoring and, if practicable, technical means are being used to activate monitoring only when the consenting party is present.

6. (U//FOUO) **Location of monitoring:** If monitoring will occur outside a Field Office's territory, notice has been provided to the SAC or ASAC of each Field Office where the monitoring is to occur, and that notice has been documented in the case file.
7. (U//FOUO) **Duration:** The request states the length of time needed for monitoring. Unless otherwise warranted, approval may be granted for the duration of the investigation subject to a substantial change of circumstances, as described in Section 11.5.4.A.2, above. When a "sensitive monitoring circumstance" is involved, DOJ may limit its approval to a shorter duration.

B. (U//FOUO) **Exceptions Requiring Additional Approval**

1. (U//FOUO) **Party Located Outside the United States:**

(U//FOUO)

b2
b7E

a. (U//FOUO)

b2
b7E

b. (U//FOUO)

b2
b7E

c. (U//FOUO)

b2
b7E

UNCLASSIFIED - FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

2. (U) Consent of More than One Party Required:

(U//FOUO) For those states or tribes that do not sanction or provide a law enforcement exception available to the FBI for one-party consent recording of communications with persons within their jurisdiction, the SAC must approve the consensual monitoring of communications as an OIA. Prior to the SAC authorizing the OIA, one-party consent must be acquired. The SAC may delegate the OIA approval authority to an ASAC or SSA.

3. (U) Sensitive Monitoring Circumstance:

(U) Requests to consensually monitor communications when a sensitive monitoring circumstance is involved must be approved by the DOJ Criminal Division, or if the investigation concerns a threat to the national security or foreign intelligence collection, by the DOJ NSD. (AGG-Dom, Part V.A.4) A "sensitive monitoring circumstance" is defined in the AGG-Dom, Part VII.O, to include the following:

- a. (U) Investigation of a member of Congress, a federal judge, a member of the Executive Branch at Executive Level IV or above, or a person who has served in such capacity within the previous two years (Note: Executive Levels I through IV are defined in 5 U.S.C. §§ 5312-5315);
- b. (U) Investigation of the Governor, Lieutenant Governor, or Attorney General of any state or territory, or a judge or justice of the highest court of any state or territory, concerning an offense involving bribery, conflict of interest, or extortion related to the performance of official duties;
- c. (U) The Attorney General, the Deputy Attorney General, or an Assistant Attorney General has requested that the FBI obtain prior approval for the use of consensual monitoring in a specific investigation;
- d. (U) A party to the communication is in the custody of the Bureau of Prisons or the United States Marshal Service or is being or has been afforded protection in the Witness Security Program.

(U//FOUO) [REDACTED]

b2
b7E

(1) (U//FOUO) [REDACTED]

(2) (U//FOUO) [REDACTED]

b2
b7E

UNCLASSIFIED - FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

(3) (U//FOUO) [redacted]

(4) (U//FOUO) [redacted]

(5) (U//FOUO) [redacted]

(6) (U//FOUO) [redacted]

(7) (U//FOUO) [redacted]

(8) (U//FOUO) [redacted]

(9) (U//FOUO) [redacted]

(10) (U//FOUO) [redacted]

(11) (U//FOUO) [redacted]

(12) (U//FOUO) [redacted]

(13) (U//FOUO) [redacted]

(14) (U//FOUO) [redacted]

(15) (U//FOUO) [redacted]

(16) (U//FOUO) [redacted]

(17) (U//FOUO) [redacted]

(U//FOUO) [redacted]

(1) (U//FOUO) [redacted]

(2) (U//FOUO) [redacted]

b2
b7E

b2
b7E

b2
b7E

UNCLASSIFIED - FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

(U//FOUO) Note: See classified Appendix G for additional information regarding consensual monitoring.

e. (U//FOUO) Procedure for Obtaining DOJ Approval For a Sensitive Monitoring Circumstance:

[Redacted]

b2
b7E

f. (U//FOUO) Note: Emergency requests involving Sensitive Monitoring Circumstances:

[Redacted]

b2
b7E

(1) (U//FOUO)

[Redacted]

b2
b7E

(2) (U//FOUO)

[Redacted]

b2
b7E

(3) (U//FOUO)

[Redacted]

b2
b7E

(U//FOUO)

[Redacted]

b2
b7E

(U//FOUO)

[Redacted]

b2
b7E

11.5.5. (U) Duration of Approval

(U//FOUO) [Redacted]

b2
b7E

UNCLASSIFIED - FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

[Redacted]

b2
b7E

11.5.6. (U//FOUO) Specific Procedures

(U//FOUO) The following procedures apply when obtaining consent.

A. (U//FOUO) Documenting consent

[Redacted]

b2
b7E

B. (U//FOUO) Retention of the consent form:

[Redacted]

b2
b7E

C. (U//FOUO) Documenting review and approval:

[Redacted]

b2
b7E

D. (U//FOUO) Multiple communications:

[Redacted]

b2
b7E

E. (U//FOUO) Case specific approval:

[Redacted]

b2
b7E

UNCLASSIFIED - FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

11.5.7. (U//FOUO) Compliance and Monitoring

(U//FOUO) ELSUR program personnel must conduct regularly scheduled reviews of the FD-759s approved within the Field Office to determine whether approval was obtained prior to initiation of consensual monitoring and to ensure that the monitoring occurred in compliance with the approvals. The ELSUR Program is also responsible for indexing all individuals or identifiers of persons intercepted during consensual monitoring and cross-referencing their names or identifiers to the approved FD-759 in the investigative case file.

UNCLASSIFIED - FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

- d. (U//FOUO) The administrative subpoena must be approved by an authorized official;
- e. (U//FOUO) The administrative subpoena must be uploaded into the Automated Case Support (ACS) system to the Subpoena ("SBP") subfile of the substantive case file for record purposes;
- f. (U//FOUO) The return of service information must be completed on the back of the original administrative subpoena;
- g. (U//FOUO) The original administrative subpoena and completed return of service must be maintained in a "SBP" subfile of the substantive investigation; and
- h. (U//FOUO) The records provided in response to the administrative subpoena must be reviewed to ensure that the FBI is authorized to collect the records provided. If an over-production has occurred, steps must be taken to correct the error.

11.9.3. (U) National Security Letter

A. (U) Legal Authority

(U) 15 U.S.C. §§ 1681u, 1681v; 18 U.S.C. § 2709;

(U) 12 U.S.C. § 3414(a)(5)(A); 50 U.S.C. § 436;

(U) AGG-Dom, Part V

(U) A National Security Letter (NSL) may be used only to request:

- 1. (U) **Financial Records: The Right to Financial Privacy Act (RFPA)**, 12 U.S.C. § 3414(a)(5);
- 2. (U) **Identity of Financial Institutions: Fair Credit Reporting Act (FCRA)**, 15 U.S.C. § 1681u(a);
- 3. (U) **Consumer Identifying Information: FCRA**, 15 U.S.C. § 1681u(b);
- 4. (U) **Identity of Financial Institutions and Consumer Identifying Information: FCRA**, 15 U.S.C. §§ 1681u(a) & (b);
- 5. (U) **Full Credit Reports in International Terrorism Investigations: FCRA**, 15 U.S.C. § 1681v; and
- 6. (U) **Telephone Subscriber Information, Toll Billing Records, Electronic Communication Subscriber Information, and Electronic Communication Transactional Records: Electronic Communications Privacy Act (ECPA)**, 18 U.S.C. § 2709.

B. (U) Definition of Method

(U) A National Security Letter is an administrative demand for documents or records that can be made by the FBI during a predicated investigation relevant to a threat to the national security. Sample NSLs are available.

C. (U//FOUO) Approval Requirements

(U//FOUO) A request for an NSL has two parts. One is the NSL itself, and one is the EC approving the issuance of the NSL. The authority to sign NSLs has been delegated to the

UNCLASSIFIED - FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

Deputy Director, Executive Assistant Director and Assistant EAD for the National Security Branch; Assistant Directors and all DADs for CT/CD/Cyber; General Counsel; Deputy General Counsel for the National Security Law Branch; Assistant Directors in Charge in NY, DC, and LA; and all SACs.

(U//FOUO) In addition to being signed by a the statutorily-required approver, every NSL must be reviewed and approved by a CDC, ADC or attorney acting in that capacity, or an NSLB attorney.

(U) [Redacted]

b2
b7E

(U//FOUO) [Redacted]

b2
b7E

(U//FOUO) [Redacted]

b2
b7E

(U//FOUO) [Redacted]

b2
b7E

(U//FOUO) [Redacted]

b2
b7E

UNCLASSIFIED - FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

[Redacted]

b2
b7E

D. (U) Duration of Approval

[Redacted]

b2
b7E

E. (U//FOUO) Specific Procedures

(U//FOUO) [Redacted]

b2
b7E

(U//FOUO) [Redacted]

b2
b7E

(U//FOUO) [Redacted]

b2
b7E

- (U//FOUO) [Redacted]

b2
b7E

- (U//FOUO) [Redacted]

b2
b7E

- (U//FOUO) [Redacted]

b2
b7E

- (U//FOUO) [Redacted]

b2
b7E

(U//FOUO) [Redacted]

b2
b7E

UNCLASSIFIED - FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

[Redacted]

b2
b7E

(U//FOUO) [Redacted]

b2
b7E

1. (U//FOUO) Cover EC

(U//FOUO) [Redacted]

b2
b7E

a. (U//FOUO) [Redacted]

b. (U//FOUO) [Redacted]

c. (U//FOUO) [Redacted]

d. (U//FOUO) [Redacted]

b2
b7E

e. (U//FOUO) [Redacted]

f. (U//FOUO) [Redacted]

g. (U//FOUO) [Redacted]

h. (U//FOUO) [Redacted]

i. (U//FOUO) [Redacted]

j. (U//FOUO) [Redacted]

UNCLASSIFIED - FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

k. (U//FOUO) [REDACTED]

b2
b7E

l. (U//FOUO) [REDACTED]

(U//FOUO) [REDACTED]

b2
b7E

2. (U) Copy of NSL

(U//FOUO) A copy of the signed NSL must be retained in the investigative case file and uploaded under the appropriate NSL document type in ACS. Documented proof of service of NSL letters must be maintained in the case file.

3. (U//FOUO) Second Generation Information

(U//FOUO) [REDACTED]

[REDACTED]

b2
b7E

4. (U//FOUO) Emergency Circumstances

(U//FOUO) ECPA protects subscriber or transactional information regarding communications from disclosure by providers of telephone or other electronic communication services. Generally, an NSL, grand jury subpoena, or other forms of legal process must be used to compel the communication service provider to disclose subscriber or transactional information. In emergency circumstances, however, if the provider in good faith believes that a delay in disclosure could pose a danger of death or serious bodily injury, the provider may voluntarily disclose information to the FBI. As a matter of FBI policy, when there is a danger of death or serious bodily injury that does not permit the proper processing of an NSL, if approved by an ASAC, a letter to the provider citing 18 U.S.C. § 2702 may be used to request emergency disclosure. If time does not permit the issuance of an emergency letter citing 18 U.S.C. § 2702, an oral request to the provider may be made, but the oral request must be followed-up with a letter as described herein.

(U//FOUO) [REDACTED]

b2
b7E

UNCLASSIFIED - FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

[Redacted]

b2
b7E

(U//FOUO) [Redacted]

[Redacted]

b2
b7E

(U//FOUO) [Redacted]

[Redacted]

b2
b7E

F. (U//FOUO) Notice and Reporting Requirements

(U//FOUO) The National Security Law Branch at FBIHQ is required to report information about NSL usage to Congress. The data necessary for Congressional reporting is automatically recorded if the NSL is created in the NSL Subsystem (FISAMS). If the NSL is created outside the system, the EC must include all information necessary for NSLB accurately to report NSL statistics. The EC must break down the number of targeted phone numbers/e-mail accounts/financial accounts that are addressed to each and every NSL recipient. Therefore, if there are three targets, ten accounts, and six recipients of an NSL, the EC must state how many accounts are the subject of the NSL as to Recipient 1, Recipient 2, etc. It is not sufficient to only indicate that there are ten accounts and six recipients.

(U//FOUO) In addition, the FBI must report the United States person status of the subject of all NSL requests (as opposed to the target of the investigation to which the NSL is relevant), other than those seeking subscriber information. While the subject is often the target of the investigation, that is not always the case. The EC must reflect the United States person status of the subject of the request – the person whose information the FBI is seeking. If the NSL is seeking information about more than one person, the EC must reflect the United States person status of each of those persons. (See the form ECs, which make clear that the United States person status applies to the target of the request for information.)

(U//FOUO) Finally, to ensure accurate reporting, the EC must accurately state the type of information that is being sought. NSLs for toll billing records or transactional records will include subscriber information. The EC need only state that the request is for toll billing records or transactional records, and the reporting paragraph should state that toll billing or transactional records are being sought for x number of accounts, and, if multiple recipients, from each of recipients #1, #2, etc.

G. (U//FOUO) Receipt of NSL Information

(U//FOUO) [Redacted]

[Redacted]

b2
b7E

UNCLASSIFIED - FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

[Redacted]

b2
b7E

(U//FOUO) [Redacted]

[Redacted]

b2
b7E

(U//FOUO) [Redacted]

[Redacted]

b2
b7E

(U//FOUO) [Redacted]

[Redacted]

b2
b7E

H. (U//FOUO) Dissemination of NSL material

(U//FOUO) Subject to certain statutory limitations, information obtained through the use of an NSL may be disseminated according to general dissemination standards in the AGG-Dom. ECPA (telephone and electronic communications records) and the RFPA (financial records) permit dissemination if consistent with the AGG-Dom and if the information is clearly relevant to the responsibilities of the recipient agency. FCRA, 15 U.S.C. § 1681u, permits dissemination to other federal agencies as may be necessary for the approval or conduct of a foreign counterintelligence investigation. FCRA imposes no special rules for dissemination of full credit reports.

(U//FOUO) [Redacted]

[Redacted] the NSLs themselves are not classified, nor is the material received in return. [Redacted]

[Redacted]

b2
b7E

UNCLASSIFIED - FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide



b2
b7E

I. (U) Payment for NSL-Derived Information

(U//FOUO) Because there is no legal obligation for the FBI to compensate recipients of NSLs issued pursuant to ECPA, 18 U.S.C. § 2709 (toll billing records information, subscriber, electronic communication transactional records) or FCRA, 15 U.S.C. § 1681v, (full credit reports in international terrorism cases), there should not be payment in connection with those NSLs. See EC, 319X-HQ-A1487720-OGC, serial 222, for a form letter to be sent in response to demands for payment for these types of NSLs.

(U) Compensation is legally required for NSLs served to obtain financial information pursuant to RFPFA, 12 U.S.C. § 3414(a)(5), and credit information pursuant to FCRA, 15 U.S.C. § 1681u. Under 12 C.F.R. § 219.3, Appendix A, a fee schedule has been adopted under which photocopying is reimbursable at \$.25 per page and searching is reimbursable at \$11 per hour for clerical staff. Regulations governing a payment schedule for FCRA, 15 U.S.C. § 1681u, NSLs has not been promulgated.

11.9.4. (U) Business Record Under FISA

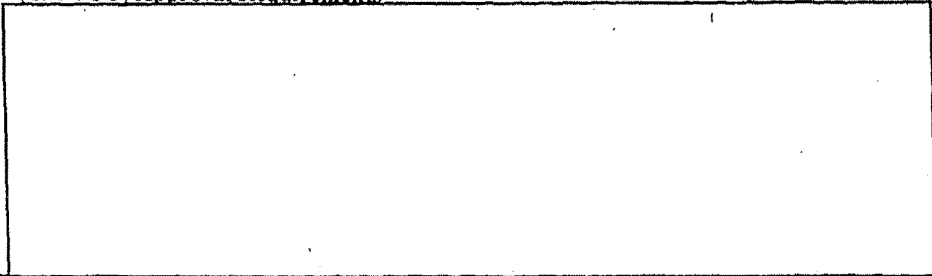
A. (U) Legal Authority

(U) 50 U.S.C. §§ 1861-63

B. (U) Definition of Method

(U) A FISA order for business records is an order for a third party to produce documents, records and other tangible information relevant to a predicated national security investigation. FISA Business Record Orders may not be used to obtain information during a positive foreign intelligence case if the material sought relates to a United States person. There is no "FISA-derived" impediment to the use of documents obtained pursuant to such orders.

C. (U//FOUO) Approval Requirements



b2
b7E

D. (U) Duration of Approval

(U) Duration is established by the court order.

E. (U) Notice and Reporting Requirements

(U) There are no special notice or reporting requirements.

UNCLASSIFIED - FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

11.10. (U) Investigative Method: Accessing stored wire and electronic communications and transactional records in conformity with chapter 121 of title 18, United States Code

11.10.1. (U) Summary

(U//FOUO) FBI employees may acquire the contents of stored wire or electronic communications and associated transactional records—including basic subscriber information—as provided in 18 U.S.C. §§ 2701-2712. Requests for voluntary disclosure under the emergency authority of 18 U.S.C. § 2702 require prior approval from the Field Office ASAC or FBIHQ Section Chief when appropriate.

(U//FOUO) **Application:** This investigative method may be used during national security investigations and criminal investigations as authorized by statute. This method may not be used for assistance to other agencies, unless relevant to an already open predicated investigation. This method cannot be used to collect positive foreign intelligence. Additionally, this method cannot be used during an assessment.

- A. (U) **Stored Data:** The Electronic Communications Privacy Act (ECPA)—18 U.S.C. §§ 2701-2712—governs the disclosure of two broad categories of information: (i) the contents of wire or electronic communications held in “electronic storage” by providers of “electronic communication service” or contents held by those who provide “remote computing service” to the public; and (ii) records or other information pertaining to a subscriber to or customer of such services. The category of “records or other information” can be subdivided further into subscriber records (listed in 18 U.S.C. § 2703[c][2]) and stored traffic data or other records.

(U) Records covered by ECPA include all records that are related to the subscriber, including buddy lists, “friend” lists (MySpace), and virtual property owned (Second Life). These other sorts of records are not subscriber records and cannot be obtained by a subpoena under 18 U.S.C. § 2703(c)(2) or an NSL under 18 U.S.C. § 2709.

- B. (U) **Legal Process:** The legal process for obtaining disclosure will vary depending on the type of information sought and whether the information is being voluntarily provided under 18 U.S.C. § 2702 (e.g., with consent or when emergency circumstances require disclosure) or the provider is being compelled to provide the information under 18 U.S.C. § 2703, as outlined below.

- C. (U) Contents held in “electronic storage” by a provider of “electronic communication service” for 180 days or less can only be obtained with a search warrant based on probable cause. Accordingly, such records may only be obtained during a full investigation.

(U) Contents held by those who provide “remote computing service” to the public and contents held in “electronic storage” for more than 180 days by an “electronic communication service” provider can be obtained with: a warrant; a subpoena; or an order issued by a court under 18 U.S.C. § 2703(d) when prior notice has been provided to the customer or subscriber (unless the court has authorized delayed notice).

(U) Title 18 United States Code Section 2705 establishes the standard to delay notice for an initial period of up to 90 days. Records or other information pertaining to a subscriber to or

UNCLASSIFIED - FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

customer of such services, including basic subscriber information can be obtained with a search warrant or an 18 U.S.C. § 2703(d) order without notice.

- D. (U) Basic subscriber information, as described in 18 U.S.C. § 2703(c)(2), can be compelled by a grand jury or administrative subpoena without notice.
- E. (U) **Preservation of Stored Data:** The government is authorized under 18 U.S.C. § 2703(f) to direct a provider to preserve records or other information (stored records or communications) in its possession for 90 days (which may be extended for an additional 90-days) pending issuance of applicable legal process for disclosure. To make a preservation request, the FBI must believe that the records will subsequently be sought by appropriate legal process.
- F. (U) **Cost reimbursement:** Title 18 United States Code Section 2706 requires the government to reimburse for costs incurred in providing the contents of communications, records, or other information obtained under 18 U.S.C. §§ 2702, 2703, or 2704, except that reimbursement is not required for records or other information maintained by a communications common carrier that relate to telephone toll records and telephone listings obtained under 18 U.S.C. § 2703. In essence, the government does not have to reimburse for the cost of producing records that the provider maintains in the ordinary course of its business..

11.10.2. (U) Legal Authority

(U) 18 U.S.C. §§ 2701-2712

(U) AGG-Dom, Part V.9

(U) ECPA—18 U.S.C. §§ 2701-2712— creates statutory privacy rights for the contents of communications in “electronic storage” and records or other information pertaining to a subscriber to or customer of an “electronic communication service” and a “remote computing service.” The statutory protections protect the privacy of an individual’s electronic data contained in a networked account—that may otherwise fall outside the scope of the protections afforded by the Fourth Amendment—when such account or its service is owned or managed by a third-party provider.

(U) ECPA generally: (i) prohibits access to the contents of wire or electronic communications while in “electronic storage” unless authorized (18 U.S.C. § 2701); (ii) prohibits a provider of service to the public from disclosing the contents of wire or electronic communications while held in “electronic storage,” and divulging to the government any information pertaining to a subscriber to or customer of such service unless authorized (18 U.S.C. § 2702); and (iii) authorizes the government to compel disclosure from a provider of stored contents of a wire or electronic communication and records or other information pertaining to a subscriber to or customer (18 U.S.C. § 2703). ECPA provides for reimbursement of costs incurred in providing the information acquired.

11.10.3. (U) Definition of Investigative Method

A. (U) Definitions:

(U) **Electronic Storage:** is “any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof,” or “any storage of such communication by an electronic communication service for purposes of backup protection of

UNCLASSIFIED - FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

such communication." 18 U.S.C. § 2510(17). In short, "electronic storage" refers only to temporary storage, made in the course of transmission, by a provider of an electronic communication service.

(U) **Remote Computing Service (RCS)**: is the "provision to the public of computer storage or processing services by means of an electronic communications system." 18 U.S.C. § 2711(2). In essence, a remote computing service is an off-site computer that stores or processes data for a customer.

(U) **Electronic Communications System**: is "any wire, radio, electromagnetic; photooptical or photoelectronic facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications." 18 U.S.C. § 2510(14).

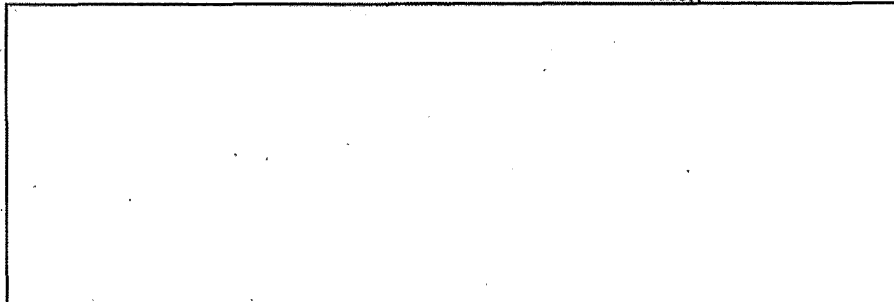
(U) **Electronic Communication Service (ECS)**: is "any service that provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15). For example, telephone companies and electronic mail companies generally act as providers of electronic communication services.

(U) ECPA authorities can be divided into two categories: (i) compelled disclosure—legal process to compel providers to disclose the contents of stored wire or electronic communications (including e-mail and voice mail—opened and unopened) and other information such as account records and basic subscriber information; and (ii) voluntary disclosure of such information from service providers. Each of these authorities is discussed below.

B. (U) Compelled Disclosure:

1. (U) Title 18 United States Code Section 2703 lists five types of legal process that the government can use to compel a provider to disclose certain kinds of information. The five mechanisms, in descending order of required threshold showing are as follows:

- (U) Search warrant;
- (U) 18 U.S.C. § 2703(d) court order with prior notice to the subscriber or customer;
- (U) 18 U.S.C. § 2703(d) court order without prior notice to the subscriber or customer;
- (U) Subpoena with prior notice to the subscriber or customer; and
- (U) Subpoena without prior notice to the subscriber or customer.



b2
b7E

UNCLASSIFIED - FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

b2
b7E

- [REDACTED]
2. (U//FOUO) **Notice—Orders Not to Disclose the Existence of a Warrant, Subpoena, or Court Order:** FBI employees may obtain a court order directing network service providers not to disclose the existence of compelled process if the government has no legal duty to notify the customer or subscriber of the process. If an 18 U.S.C. § 2703(d) order or 18 U.S.C. § 2703(a) warrant is being used, a request for a non-disclosure order can be included in the application and proposed order or warrant. If a subpoena is being used to obtain the information, a separate application to a court for a non-disclosure order must be made.
 3. (U) **Legal Standard:** A court may order an electronic communications service provider or remote computing service not to disclose the existence of a warrant, subpoena, or court order for such period as the court deems appropriate. The court must enter such an order if it determines that there is reason to believe that notification of the existence of the warrant, subpoena, or court order will result in:
 - (U) Endangering the life or physical safety of an individual;
 - (U) Flight from prosecution;
 - (U) Destruction of or tampering with evidence;
 - (U) Intimidation of potential witnesses; or
 - (U) Otherwise seriously jeopardizing an investigation or unduly delaying a trial. 18 U.S.C. § 2705(b).
 4. (U) **Search Warrant:** Investigators can obtain the full contents of a network account with a search warrant. ECPA does not require the government to notify the customer or subscriber when it obtains information from a provider using a search warrant. Warrants issued under 18 U.S.C. § 2703 must comply with either FRCP Rule 41 or an equivalent state warrant. However, all warrants issued pursuant to 18 U.S.C. § 2703 do not require personal service; those warrants issued by a federal court have nationwide jurisdiction (see below); and the warrants may only be served on an electronic communication service or a remote computing service. FRCP Rule 41 also poses the additional requirement on these warrants that a copy of the warrant be left with the provider, and a return and inventory be made.

(U) Under 18 U.S.C. § 2703(a), with a search warrant issued based on probable cause pursuant to FRCP Rule 41 or an equivalent state warrant, the government may obtain:

 - a. (U) "The contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less," and
 - b. (U) Everything that can be obtained using a 18 U.S.C. § 2703(d) court order with notice.

(U) In other words, every record and all of the stored contents of an account—including opened and unopened e-mail/voice mail— can be compelled by a search warrant based on probable cause pursuant to FRCP Rule 41. Moreover, because the warrant is issued

UNCLASSIFIED - FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

by a neutral magistrate based on probable cause, obtaining a search warrant effectively insulates the process from challenge under the Fourth Amendment.

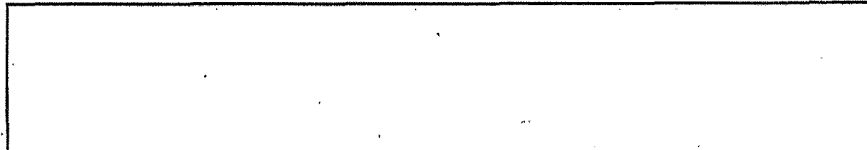
(U) **Nationwide Scope:** Search warrants under 18 U.S.C. § 2703(a) may be issued by a federal "court with jurisdiction over the offense under investigation," and may be executed outside the district of the issuing court for material responsive to the warrant. State courts may also issue warrants under 18 U.S.C. § 2703(a), but the statute does not give these warrants effect outside the issuing court's territorial jurisdiction. As with a typical FRCP Rule 41 warrant, investigators must draft an affidavit and a proposed warrant that complies with FRCP Rule 41.

(U) **Service of Process:** Title 18 United States Code Section 2703(a) search warrants are obtained just like any other FRCP Rule 41 search warrant but are typically served on the provider and compel the provider to find and produce the information described in the warrant. ECPA expressly states that the presence of an officer is not required for service or execution of a search warrant issued pursuant to 18 U.S.C. § 2703(a).

5. (U) **Court Order with Prior Notice to the Subscriber or Customer:** Investigators can obtain everything in a network account except for unopened e-mail or voice-mail stored with a provider for 180 days or less using a 18 U.S.C. § 2703(d) court order with prior notice to the subscriber unless they have obtained authority for delayed notice pursuant to 18 U.S.C. § 2705. ECPA distinguishes between the contents of communications that are in "Electronic storage" (e.g., unopened e-mail) for less than 180 days, and those that have been in "Electronic storage" for longer or that are no longer in "Electronic storage" (e.g., opened e-mail).

(U) FBI employees who obtain a court order under 18 U.S.C. § 2703(d), and either give prior notice to the subscriber or comply with the delayed notice provisions of 18 U.S.C. § 2705(a), may obtain:

- a. (U) "The contents of a wire or electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days." 18 U.S.C. § 2703(a).
- b. (U) "The contents of any wire or electronic communication" held by a provider of remote computing service "on behalf of . . . a subscriber or customer of such remote computing service," 18 U.S.C. §§ 2703(b)(1)(B)(ii), 2703 (b)(2); and
- c. (U) everything that can be obtained using a 18 U.S.C. § 2703(d) court order without notice.



b2
b7E



b2
b7E

UNCLASSIFIED - FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

[REDACTED]

b2
b7E

(U) **Legal Standard:** To order delayed notice, the court must find that "there is reason to believe that notification of the existence of the court order may . . . endanger[] the life or physical safety of an individual; [lead to] flight from prosecution; [lead to] destruction of or tampering with evidence; [lead to] intimidation of potential witnesses; or . . . otherwise seriously jeopardiz[e] an investigation or unduly delay[] a trial." 18 U.S.C. §§ 2705(a)(1)(A) and 2705(a)(2). The applicant must satisfy this standard anew each time an extension of the delayed notice is sought.

(U) **Nationwide Scope:** Federal court orders under 18 U.S.C. § 2703(d) have effect outside the district of the issuing court. Title 18 United States Code Section 2703(d) orders may compel providers to disclose information even if the information is stored outside the district of the issuing court. See 18 U.S.C. § 2703(d) ("any court that is a court of competent jurisdiction" may issue a 18 U.S.C. § 2703[d] order); 18 U.S.C. § 2711(3) (court of competent jurisdiction includes any federal court having jurisdiction over the offense being investigated without geographic limitation).

(U) Title 18 United States Code Section 2703(d) orders may also be issued by state courts. See 18 U.S.C. §§ 2711(3), 3127(2)(B). Title 18 United States Code Section 2703(d) orders issued by state courts, however, do not have effect outside the jurisdiction of the issuing state. See 18 U.S.C. §§ 2711(3).

6. (U) **Court Order without Prior Notice to the Subscriber or Customer:** FBI employees need an 18 U.S.C. § 2703(d) court order to obtain most account logs and most transactional records.

(U) A court order under 18 U.S.C. § 2703(d) may compel disclosure of:

- a. (U) All "record(s) or other information pertaining to a subscriber to or customer of such service (not including the contents of communications [held by providers of electronic communications service and remote computing service])," and
- b. (U) Basic subscriber information that can be obtained using a subpoena without notice. 18 U.S.C. § 2703(c)(1);

(U) **Types of Transactional Records:** The broad category of transactional records includes all records held by a service provider that pertain to the subscriber beyond the specific records listed in 2703(c)(1) [REDACTED]

b2
b7E

(U//FOUO) [REDACTED]

[REDACTED]

b2
b7E

- c. (U) **Cell site and Sector information:** Cell site and sector information is considered "a record or other information pertaining to a subscriber" and therefore, production of historical and prospective cell site and sector information may be compelled by a court order under 18 U.S.C. § 2703(d). Requests made pursuant to 18 U.S.C. § 2703(d) for disclosure of prospective cell site and sector

UNCLASSIFIED - FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

information—which is delivered to law enforcement under Communications Assistance for Law Enforcement Act (CALEA) at the beginning and end of calls— must be combined with an application for pen register/trap and trace device. Some judicial districts will require a showing of probable cause before authorizing the disclosure of prospective cell site and sector information.

d. [Redacted]

b2
b7E

(U//FOUO) [Redacted]

b2
b7E

(U) [Redacted]

b2
b7E

(U) [Redacted]

b2
b7E

UNCLASSIFIED - FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

(U) **Legal Standard:** A court order under 18 U.S.C. § 2703(d) is known as an "articulable facts" court order or simply a "d" order. "This section imposes an intermediate standard to protect on-line transactional records. It is a standard higher than a subpoena, but not a probable cause warrant. The intent of raising the standard for access to transactional data is to guard against "fishing expeditions" by law enforcement." (See H.R. Rep. No. 102-827, at 31 (1994), reprinted in 1994 U.S.C.C.A.N. 3489.)

(U) The FBI must state sufficient specific and articulable facts for the court to find that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation.

b2
b7E

7. (U) **Subpoena with Prior Notice to the Subscriber or Customer:** Investigators can subpoena opened e-mail from a provider if they either give prior notice to the subscriber or comply with the delayed notice provisions of 18 U.S.C. § 2705(a)—which requires a written certification by the SAC or ASAC that there is reason to believe that notification of the existence of the subpoena may have an adverse result.

(U) FBI employees who obtain a subpoena and either give prior notice to the subscriber or comply with the delayed notice provisions of 18 U.S.C. § 2705(a), may obtain:

- a. (U) "The contents of any wire or electronic communication" held by a provider of remote computing service "on behalf of . . . a subscriber or customer of such remote computing service." 18 U.S.C. § 2703(b)(1)(B)(i), § 2703(b)(2);
- b. (U) "The contents of a wire or electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days." 18 U.S.C. § 2703(a); and
- c. (U) Basic subscriber information listed in 18 U.S.C. § 2703(c)(2).

(U)

b2
b7E

(U) **Notice:**

b2
b7E

(U) **Legal standards for delaying notice.** The supervisory official must certify in writing that "there is reason to believe that notification of the existence of the court order may . . . endanger[] the life or physical safety of an individual; [lead to] flight

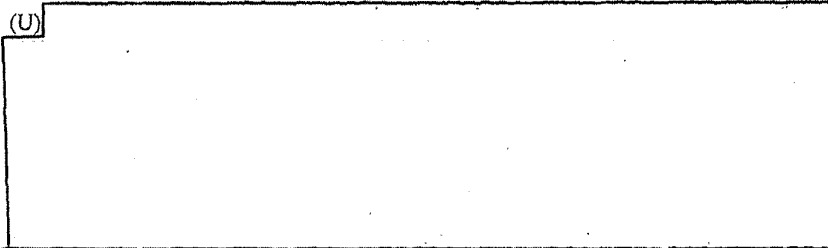
UNCLASSIFIED - FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

from prosecution; [lead to] destruction of or tampering with evidence; [lead to] intimidation of potential witnesses; or . . . otherwise seriously jeopardiz[e] an investigation or unduly delay[] a trial." 18 U.S.C. §§ 2705(a)(1)(A), 2705(a)(2). Importantly, this standard must be satisfied anew every time an extension of the delayed notice is sought.

8. (U) **Subpoena without Prior Notice to the Subscriber or Customer:** Investigators can subpoena basic subscriber information listed in 18 U.S.C. § 2703(c)(2).

(U) The government may use an administrative subpoena authorized by a federal or state statute or a federal or state grand jury or trial subpoena to compel a provider to disclose basic subscriber information listed in 18 U.S.C. § 2703(c)(2): "name; address; local and long distance telephone connection records, or records of session times and durations; length of service (including start date) and types of service used; telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and means and source of payment for such service (including any credit card or bank account number)[.]"

(U)



b2
b7E

See PATRIOT Act § 210, 115 Stat. 272, 283 (2001).

(U) **Legal Standard:** The legal threshold for issuing a subpoena is low. In United States v. Morton Salt Co., 338 U.S. 632, 642-43 (1950), the Court articulated the deferential standard for judicial review of administrative enforcement actions is a four-factor evaluation of "good faith" issuance requiring that: (i) the investigation is conducted pursuant to a legitimate purpose; (ii) the information requested under the subpoena is relevant to that purpose; (iii) the agency does not already have the information it is seeking with the subpoena; and (iv) the agency has followed the necessary administrative steps in issuing the subpoena.

(U//FOUO) In the event that a federal grand jury subpoena is used, however, appropriate protections against disclosure must be followed in compliance with FRCP Rule 6(e).

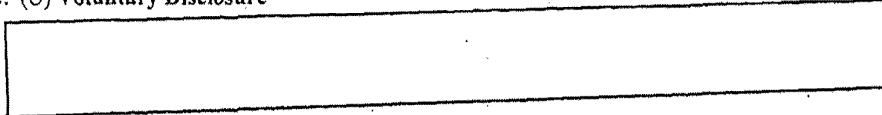


b2
b7E

Where the telephone billing records being sought are those of a member of the news media, approval of the Attorney General is required. (See DIOG Section 11.9.1.E)

UNCLASSIFIED - FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

C. (U) Voluntary Disclosure



b2
b7E

1. (U) **Service NOT Available to the Public:** Providers of services not available "to the public" are not prohibited from disclosure under ECPA, and so the provider may freely disclose both contents and other records relating to stored communications. Andersen Consulting v. UOP, 991 F. Supp. 1041 (N.D. Ill. 1998) (giving hired consulting firm employees access to UOP's e-mail system is not equivalent to providing e-mail to the public). Only providers of services to the public are prohibited from disclosing stored contents and records, unless statutorily authorized.

2. (U) **Services That ARE Available to the Public:** If the services offered by the provider are available to the public, then ECPA precludes both the disclosure of contents to any third party, including the government, and the disclosure of other records to any governmental entity unless a statutory exception applies. The statutory exceptions permit disclosure by a provider to the public, in essence when the needs of public safety and service providers outweigh privacy interests.

(U) If the provider is authorized to disclose the information to the government under 18 U.S.C. § 2702 and is willing to do so voluntarily, law enforcement does not need to obtain a legal order to compel the disclosure.

(U) If a provider voluntarily discloses under the statute, there is no follow-up legal process required or available. If the provider, on the other hand, either may not or will not disclose the information, FBI employees must rely on compelled disclosure provisions and obtain the appropriate legal orders.

i. (U) **Voluntary disclosure of Stored Contents**

(U) ECPA authorizes the voluntary disclosure of stored contents when:

- (a) (U) The disclosure is with the consent (express or implied) of the originator, addressee, intended recipient, or the subscriber in the case of opened e-mail, 18 U.S.C. § 2702(b)(3);
- (b) (U) The disclosure "may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service," 18 U.S.C. § 2702(b)(5);
- (c) (U) The provider "in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of information relating to the emergency," 18 U.S.C. § 2702(b)(8);
- (d) (U) To the National Center for Missing and Exploited Children, in connection with a report submitted thereto under Section 227 of the Victims of Child Abuse Act of 1990. (42 U.S.C. § 13032 and 18 U.S.C. § 2702[b][6]); or
- (e) (U) The contents are inadvertently obtained by the service provider and appear to pertain to the commission of a crime. Such disclosures can only be made to a law enforcement agency. 18 U.S.C. § 2702(b)(7)

UNCLASSIFIED - FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

ii. (U) **Voluntary disclosure of Non-content Customer Records**

(U) ECPA provides for the voluntary disclosure of non-content customer records by a provider to a governmental entity when:

- (a) (U) The disclosure is with the consent (express or implied) of the customer or subscriber or 18 U.S.C. § 2702(c)(2);
- (b) (U) The disclosure "may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service," 18 U.S.C. § 2702(c)(3);
- (c) (U) The provider "in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of information relating to the emergency," 18 U.S.C. § 2702(c)(4); or
(U//FOUO) Note: an emergency disclosure under this statutory exception is justified when the circumstances demand immediate action on the part of the government to prevent death or serious bodily injury, and does not depend on the immediacy of the risk of danger itself. For example, an e-mail that discusses a planned terrorist attack but not the timing for the attack would constitute an emergency that threatens life or limb, even though the timing of the attack is unknown. It is the need for immediate action to prevent the serious harm threatened by these circumstances rather than the immediacy of the threat itself that is the reason Congress authorized voluntary disclosures under this exception. H.Rpt. No. 107-497 p 13-14 (June 11, 2002) accompanying H.R. 3482, The Cyber Security Enhancement Act of 2002, which passed as part of the comprehensive Homeland Security Act, See P.L. 107-296 § 225.
- (d) (U) To the National Center for Missing and Exploited Children, in connection with a report submitted thereto under Section 227 of the Victims of Child Abuse Act of 1990. (42 U.S.C. § 13032 and 18 U.S.C. § 2702(c)[5])

iii. (U) **Preservation of Evidence under 18 U.S.C. § 2703(f):**

[Redacted]

b2
b7E

(U) A governmental entity is authorized to direct providers to preserve stored records and communications pursuant to 18 U.S.C. § 2703(f).

[Redacted]

b2
b7E

Once a preservation request is made, ECPA requires that the provider must retain the records for 90 days, renewable for another 90-day period upon a government request. See 18 U.S.C. § 2703 (f)(2).

(U) Specifically, 18 U.S.C. § 2703(f)(1) states:

- (a) (U) A provider of wire or electronic communication service or a remote computing service, upon the request of a governmental entity, must take all

UNCLASSIFIED - FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process.

- (b) (U) There is no legally prescribed format for 18 U.S.C. § 2703(f) requests.

b2
b7E

[REDACTED]

(U) FBI employees who send 18 U.S.C. § 2703(f) letters to network service providers should be aware of two limitations. First, the authority to direct providers to preserve records and other evidence is not prospective. That is, 18 U.S.C. § 2703(f) letters can order a provider to preserve records that have already been created but cannot order providers to preserve records not yet made. If FBI employees want providers to record information about future electronic communications, they must comply with the electronic surveillance statutes. A second limitation of 18 U.S.C. § 2703(f) is that some providers may be unable to comply effectively with 18 U.S.C. § 2703(f) requests

b2
b7E

iv. (U) **Video Tape Rental or Sales Records**

(U) Title 18 United States Code Section 2710 makes the unauthorized disclosure of records by any person engaged in the rental, sale, or delivery of prerecorded video cassette tapes or similar audiovisual materials unlawful and provides an exclusionary rule to prohibit personally identifiable information otherwise obtained from being admissible as evidence in any court proceeding. Personally identifiable information is defined as "information that identifies a person as having requested or obtained specific video material or services"

- (a) (U) The disclosure to law enforcement of "personally identifiable information" is permitted only when the law enforcement agency:
- (1) (U) Has the written consent of the customer;
 - (2) (U) Obtains a warrant issued under the FRCP or equivalent state warrant; or
 - (3) (U) A grand jury subpoena;

b2
b7E

(b)

[REDACTED]

(U) This type of information was specifically not included in the definition of "personally identifiable information" to allow law enforcement to obtain information about individuals during routine investigations such as neighborhood investigations.

UNCLASSIFIED - FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

(U//FOUO) The disclosure of "personally identifiable information" in a national security case may be compelled through use of the above legal processes or pursuant to a business records order issued under 50 U.S.C. § 1861.

11.10.4. (U) Approval Requirements for Investigative Method

A. (U) Voluntary Emergency Disclosure

(U//FOUO) ECPA protects subscriber and transactional information regarding communications from disclosure by providers of telephone or other electronic communication services. Generally, an NSL, grand jury subpoena, or other form of legal process must be used to compel the communication service provider to disclose such information.

[Redacted]

b2
b7E

(U//FOUO) [Redacted]

b2
b7E

(U//FOUO) [Redacted]

b2
b7E

(U//FOUO) [Redacted]

b2
b7E

11.10.5. (U) Duration of Approval

(U) As authorized by statute (e.g., for as long as the emergency necessitating usage exists and only in those circumstances when it is impracticable to obtain legal process) and applicable court order or warrant.

11.10.6. (U//FOUO) Specific Procedures

A. (U//FOUO) Filing requirements:

[Redacted]

b2
b7E

UNCLASSIFIED - FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

[Redacted]

b2
b7E

B. (U//FOUO) Contact with Providers:

[Redacted]

b2
b7E

C. (U) Cost Reimbursement:

(U) Policy and procedures regarding cost reimbursement are described in the following:

(U) Consistent payment procedures

[Redacted]

b2
b7E

(U) 5/25/2005 Cost Reimbursement Guidance (18 U.S.C. § 2706 - ECPA)

11.10.7. (U) Notice and Reporting Requirements

A. (U) **Voluntary disclosures:** Title 18 United States Code Section 2702(d) requires the Attorney General to report annually to Congress information pertaining to the receipt of voluntary disclosures of the contents of stored wire or electronic communications in an emergency under 18 U.S.C. § 2702(b)(8), specifically:

1. (U) The number of accounts from which DOJ received voluntary disclosures under subsection (b)(8); and
2. (U) Summary of the basis for disclosure in those instances where the investigation pertaining to those disclosures was closed without the filing of criminal charges.

B. (U) **Roles/Responsibilities:** OGC/ILB is assigned the administrative responsibility to, by December 31 of each year:

1. (U) Tabulate the number of voluntary disclosures of stored contents received under the authority of 18 U.S.C. § 2702(b)(8) for the calendar year;
2. (U) Prepare the report summarizing the basis for disclosure in those instances where the investigation pertaining to those disclosures was closed without the filing of criminal charges; and
3. (U) Submit the report to OGC for review and submission to DOJ according to the statutory requirement for annual report by the Attorney General.

11.10.8. (U) Other Applicable Policies

[Redacted]

b2
b7E

UNCLASSIFIED - FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

11.11. (U) Investigative Method: Pen Registers and Trap and Trace devices in conformity with chapter 206 of Title 18, United States Code, and the Foreign Intelligence Surveillance Act

11.11.1. (U) Summary

(U) Pen register and trap and trace (PR/TT) devices enable the prospective collection of non-content traffic information associated with wire and electronic communications, such as: the phone numbers dialed from or to a particular telephone, including electronic communications; messages sent from or to a particular telephone; or the Internet provider (IP) address of communications on the Internet and other computer networks.

(U//FOUO) **Application:** The PR/TT may be used in preliminary and full national security and criminal investigations. This method may not be used for: (i) targeting a United States person when providing assistance to other agencies, unless there is already an open FBI preliminary or full investigation related to the request for assistance or the predicate exists to open a preliminary or full investigation; (ii) targeting a United States person when collecting against a foreign intelligence requirement; or (iii) during an assessment.

11.11.2. (U) Legal Authority

(U) 18 U.S.C. §§ 3121 et seq. and 50 U.S.C. §§ 1842 et seq. regulate the use of PR/TT devices. PR/TT orders can collect IP addresses, port numbers and the "To" and "From" information from e-mail; they cannot intercept the content of a communication, such as words in the "subject line" or the body of an e-mail.

11.11.3. (U) Definition of Investigative Method

(U) A pen register device records or decodes dialing, routing addressing or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided that such information must not include the contents of any communication. 18 U.S.C. § 3127(3).

(U) A trap and trace device captures the incoming electronic or other impulses that identify the originating number or other dialing, routing, addressing or signaling information reasonably likely to identify the source of a wire or electronic communication, provided that such information does not include the contents of any communication. 18 U.S.C. § 3127(4).

11.11.4. (U) Standards for Use and Approval Requirements for Investigative Method

A. (U) Pen Register/Trap and Trace under FISA: Applications for authority to use a PR/TT device can be made to the FISC in national security investigations.

1. (U) **Legal Standard:** Applications to the FISC are to be under oath and must include:
 - a. (U) The identity of the federal officer making the application; and
 - b. (U) A certification by the applicant that the information likely to be obtained is foreign intelligence information not concerning a United States person or, if concerning a United States person, is information that is relevant to an ongoing investigation to protect the United States against international terrorism or clandestine intelligence activities; and that such investigation, if of a United States

UNCLASSIFIED - FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

person, is not conducted solely upon the basis of activities protected by the First Amendment to the Constitution.

2. (U//FOUO) Procedures: Requests for initiation or renewal of FISA PR/TT must be made using

[REDACTED]

b2
b7E

FISAMS will route the request to appropriate parties for their review and approval of the request [REDACTED] Routing a paper copy for signatures is not required.

3. (U) Emergency Authority—FISA: 50 U.S.C. § 1843

(U//FOUO) Under the provisions of FISA, the Attorney General may grant Emergency Authority (EA) for PR/TT. Requests for Emergency Authority must be referred to the appropriate FBIHQ Division.

(U//FOUO)

[REDACTED]

b2
b7E

- a. (U) The Attorney General may authorize the installation and use of a PR/TT upon a determination that an emergency exists and that the factual basis exists for a court order. The FISC must be informed at the time of the authorization and an application for a court order must be made to the court no more than seven (7) days after the authorization. Emergency-authorized PR/TT use must terminate when the information sought is obtained, when the FISC denies the application, or seven (7) days after the Attorney General authorization is given.
- b. (U) If the FISC denies the application after an emergency PR/TT device has been installed, no information collected as a result may be used in any manner, except with the approval of the Attorney General upon a showing that the information indicates a threat of death or serious bodily harm to any person.

(U) Notwithstanding the foregoing, the President, acting through the Attorney General, may authorize the use of a PR/TT, without a court order, for a period not to exceed 15 calendar days, following a declaration of war by Congress.

(U//FOUO) If an emergency situation arises after regular business hours, [REDACTED]

[REDACTED] at any time during an emergency.

b2
b7E

- B. (U) Criminal Pen Register/Trap and Trace under 18 U.S.C. §§ 3121 et seq.: Applications for the installation and use of a PR/TT device may be made to a "court of competent

UNCLASSIFIED - FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

jurisdiction"—i.e., "any district court of the United States (including a magistrate judge of such a court) or any United States court of appeals having jurisdiction over the offense being investigated, or any court of general criminal jurisdiction of a State authorized by the law of that State to enter orders authorizing the use of a pen register or trap and trace device." 18 U.S.C. § 3127(2).

1. (U) **Legal Standard:** Applications for authorization to install and use a PR/TT device must include:
 - a. (U) The identity of the attorney for the government or the state law enforcement or investigative officer making the application and the identity of the law enforcement agency conducting the investigation; and
 - b. (U) A certification by the applicant that the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by that agency.
2. (U//FOUO) **Procedures:** An SSA must approve a request for initiation or renewal of PR/TT use prior to submission of the request to an attorney for the government. Before approving such a request, the SSA should consider of the following:
 - a. (U//FOUO) The use of resources based on the investigative purpose set forth;
 - b. (U//FOUO) Whether there is sufficient factual basis for the certification to be made in the application (i.e., is the information likely to be obtained relevant to an ongoing criminal investigation);
 - c. (U//FOUO) Whether the customer or subscriber has consented to the use of a PR/TT, see 18 U.S.C. § 3121(b)(3); or
 - d. (U//FOUO) Whether the use of a PR/TT is the least intrusive method feasible under the circumstances.

(U//FOUO) A copy of the approving EC must be maintained in the investigative case file and/or sub file and in the ELSUR Administrative Subfile to the corresponding case file.

(U//FOUO) A PR/TT order is executable anywhere within the United States and, upon service, the order applies to any person or entity providing wire or electronic communication service in the United States whose assistance may facilitate the execution of the order. Whenever such an order is served on any person or entity not specifically named in the order, upon request of such person or entity, the attorney for the government or law enforcement or investigative officer that is serving the order must provide written or electronic certification that the order applies to the person or entity being served.

3. (U) **Emergency Authority—Criminal:**

(U) The Attorney General, the Deputy Attorney General, the Associate Attorney General, any Assistant Attorney General, any acting Assistant Attorney General, or any Deputy Assistant Attorney General may specially designate any investigative or law enforcement officer to determine whether an emergency situation that requires the installation and use of a PR/TT device before an order authorizing such installation and use can, with due diligence, be obtained.

(U) An emergency situation as defined in this section involves:

UNCLASSIFIED - FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

- a. (U) Immediate danger of death or serious bodily injury to any person;
- b. (U) Conspiratorial activities characteristic of organized crime;
- c. (U) An immediate threat to a national security interest; or
- d. (U) An ongoing attack on a protected computer (as defined in 18 U.S.C. § 1030) that constitutes a crime punishable by a term of imprisonment greater than one year.

(U) If the DOJ authorizes the emergency installation of a PR/TT, the government has 48 hours after the installation to apply for a court order according to 18 U.S.C. § 3123. It is a violation of law to fail to apply for a court order within this 48 hour period. Use of the PR/TT shall immediately terminate when the information sought is obtained, when the application for a court order is denied, or if no court order has been obtained 48 hours after the installation of the PR/TT device.

(U//FOUO) As with requesting authorization for an emergency Title III, [redacted]

b2
b7E

[redacted] Once that approval has been obtained, the DOJ attorney will advise the AUSA that the emergency use has been approved and that the law enforcement agency may proceed with the installation and use of the PR/TT. The DOJ attorney will send a verification memorandum, signed by the authorizing official, to the AUSA. The AUSA will include an authorization memorandum with the application for the court order approving the emergency use.

(U//FOUO) If an emergency situation arises after regular business hours, [redacted]

b2
b7E

[redacted] During regular business hours, [redacted]

11.11.5. (U) Duration of Approval

(U) **National Security:** The use of a PR/TT device may be authorized by the FISC for a period of time not to exceed 90 days in cases targeting a United States person. Extensions may be granted for periods not to exceed 90 days upon re-application to the court. In cases targeting a non-United States person, an order or extension may be for a period of time not to exceed one year.

(U) **Criminal:** The installation and use of a PR/TT device may be authorized by court order under 18 U.S.C. § 3123 for a period not to exceed sixty days, which may be extended for additional sixty-day periods.

11.11.6. (U//FOUO) Specific Procedures

A. (U//FOUO) Prior to installing and using a PR/TT device (whether issued in a criminal or national security matter), the case agent should:

1. (U//FOUO) [redacted]

b2
b7E

UNCLASSIFIED - FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

[Redacted]

b2
b7E

2. (U//FOUO)

[Redacted]

b2
b7E

3. (U//FOUO)

[Redacted]

b2
b7E

4. (U//FOUO)

[Redacted]

b2
b7E

5. (U//FOUO)

[Redacted]

b2
b7E

11.11.7. (U) Use and Dissemination of Information Derived from Pen Register/Trap and Trace Authorized Pursuant to FISA

(U) 50 U.S.C. § 1845

- A. (U) No information acquired from a PR/TT device installed and used pursuant to FISA may be used or disclosed by federal officers or employees except for lawful purposes.
- B. (U) No information acquired pursuant to a FISA authorized PR/TT may be disclosed for law enforcement purposes unless such disclosure is accompanied by a statement that such information, or any information derived therefrom, may only be used in a criminal proceeding with the advance authorization of the Attorney General.
- C. (U) Whenever the United States intends to enter into evidence or otherwise use or disclose in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States against an aggrieved person any information obtained or derived from the use of a PR/TT device acquired pursuant to FISA, the United States must, before the trial, hearing, or other proceeding or at a reasonable time before an effort to so disclose or so use that information or submit it into evidence, notify the aggrieved person, and the court or other authority in which the information is to be disclosed or used, that the United States intends to so disclose or so use such information.

(U) Note: 50 U.S.C. § 1801(k) defines aggrieved person as: "a person who is the target of an electronic surveillance or any other person whose communications or activities were subject to electronic surveillance."

UNCLASSIFIED - FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

11.11.8. (U) Notice and Reporting Requirements

A. (U) **Annual Report for Criminal Pen Register/Trap and Trace:** The Attorney General is required to make an annual report to Congress on the number of criminal PR/TT orders applied for by DOJ law enforcement agencies. 18 U.S.C. § 3126. The report is to include the following information:

1. (U) The period of interceptions authorized by the order, and the number and duration of any extensions;
2. (U) The offense specified in the order or application, or extension;
3. (U) The number of investigations involved;
4. (U) The number and nature of the facilities affected; and
5. (U) The identity, including the district, of the applying agency making the application and the person authorizing the order.

(U//FOUO) DOJ, Criminal Division, Office of Enforcement Operations requires that the FBI provide quarterly reports on pen register usage. To satisfy DOJ data requirements and standardize and simplify field reporting, Court-ordered pen register usage must be reported to FBIHQ [redacted] within five workdays of the expiration date of an original order or extensions, or denial of an application for an order. For all criminal PR/TT orders or extensions issued on or after January 1, 2009 [redacted] [redacted] These reporting requirements do not apply to PR/TT authorized pursuant to consent or under the provisions of FISA.

b2
b7E

B. (U) **Semi-Annual Report for National Security Pen Registers and Trap and Trace:** The Attorney General must inform the House Permanent Select Committee on Intelligence, Senate Select Committee on Intelligence, Committee of the Judiciary of the House Representatives, and Committee of the Judiciary of the Senate concerning all uses of PR/TT devices pursuant to 50 U.S.C. § 1846. This report is coordinated through DOJ NSD. A semi-annual report must be submitted that contains the following information:

1. (U) The total number of applications made for orders approving the use of PR/TT devices;
2. (U) The total number of such orders either granted, modified, or denied; and
3. (U) The total number of PR/TT devices whose installation and use was authorized by the Attorney General on an emergency basis and the total number of subsequent orders approving or denying the installation and use of such PR/TT devices.

11.11.9. (U) Special Circumstances

A. (U//FOUO) **Avoiding Collection and Investigative Use of "Content" in the Operation of Pen Registers and Trap and Trace Devices**

1. (U//FOUO) **Overview:** Telecommunication networks provide users the ability to engage in extended dialing and/or signaling, (also known as "post cut-through dialed digits" or PCTDD), which in some circumstances are simply call-routing information and, in others, are call content. For example, PCTDD occur when a party places a calling card, credit card, or collect call by first dialing a long-distance carrier access number and then, after the initial call is "cut through," dials the telephone number of the destination party. In

UNCLASSIFIED - FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

other instances, PCTDD may represent call content, such as when a party calls an automated banking service and enters an account number, calls a pharmacy's automated prescription refill service and enters prescription information, or enters a call-back number when prompted by a voice mail service. See United States Telecom Assn v. Federal Communications Commission, 227 F.3d 450, 462 (D.C. Cir. 2000)

[Redacted]

b2
b7E

(U//FOUO) The definition of both a pen register device and a trap and trace device provides that the information collected by these devices "shall not include the contents of any communication." 18 U.S.C. § 3127. In addition, 18 U.S.C. § 3121(c) makes explicit the requirement to "use technology reasonably available" that restricts the collection of information "so as not to include the contents of any wire or electronic communications." "Content" includes any information concerning the substance, purpose, or meaning of a communication. 18 U.S.C. § 2510(8). When the pen register definition is read in conjunction with the limitation provision, however, it suggests that although a PR/TT device may not be used for the express purpose of collecting content, the incidental collection of content may occur despite the use of "reasonably available" technology to minimize, to the extent feasible, any possible over collection of content while still allowing the device to collect all of the dialing and signaling information authorized.

DOJ Policy: In addition to this statutory obligation, DOJ has issued a directive to all DOJ agencies requiring that no affirmative investigative use may be made of PCTDD incidentally collected that constitutes content, except in cases of emergency—to prevent an immediate danger of death, serious physical injury, or harm to the national security.

(U//FOUO) [Redacted]

b2
b7E

2. (U//FOUO) Collection: [Redacted]

b2
b7E

a. (U//FOUO) [Redacted]

b2
b7E

UNCLASSIFIED - FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

[Redacted]

b2
b7E

b. (U//FOUO) [Redacted]

b2
b7E

3. (U//FOUO) Use of PCTDD: [Redacted]

b2
b7E

a. (U//FOUO) [Redacted]

b2
b7E

i. (U//FOUO) [Redacted]

b2
b7E

ii. (U//FOUO) [Redacted]

b2
b7E

(U//FOUO) [Redacted]

b2
b7E

iii. (U//FOUO) [Redacted]

b2
b7E

UNCLASSIFIED - FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

iv. (U//FOUO)

[Redacted]

b2
b7E

b. (U//FOUO)

[Redacted]

b2
b7E

i. (U//FOUO)

[Redacted]

b2
b7E

ii. (U//FOUO)

[Redacted]

b2
b7E

4. (U//FOUO) **What constitutes PCTDD content:** In applying the above, the term "content" is interpreted to mean "any information concerning the substance, purpose, or meaning of a communication" as defined in 18 U.S.C. § 2510. Questions concerning whether specific PCTDD are content as opposed to dialing, routing or signaling information should be addressed to the CDC or OGC for coordination with DOJ as necessary.

(U//FOUO)

[Redacted]

b2
b7E

- B. (U//FOUO) **Use of cell site simulators/digital analyzers/wireless intercept tracking technology.** A PR/TT order or consent is required for the FBI to use equipment to capture any "signaling information"—including the Mobile Station Identification Number (MSIN) and Electronic Serial Number (ESN) or other registration-type data—emitted from a wireless phone into the public airspace—even though this can be accomplished without the assistance of the service provider. Because 18 U.S.C. § 3127 defines PR/TT devices in terms of recording, decoding or capturing dialing, routing, addressing, or signaling

UNCLASSIFIED - FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

information, the government's use of its own device to capture such signaling data—whether passively monitoring or actively interrogating—constitutes the use of a "pen register" device and requires an order or statutory exception to avoid violating the statute. The following discusses how wireless intercept tracking technology (WITT) is used:

1. (U//FOUO) To Locate a Known Phone:

- a. (U//FOUO) **Authority:** A standard PR/TT order is adequate to authorize the use of this technology to determine the location of a known targeted phone, provided that the language authorizes FBI employees to install or cause to be installed and use a pen register device, without geographical limitation, at any time of day or night within (X) days from the date the order is signed, to record or decode dialing, routing, addressing, or signaling information transmitted by the "Subject Telephone." The application and order should generally also request authority to compel disclosure of cell site location data on an ongoing basis under 18 U.S.C. § 2703(d)—or probable cause, if such is required by the particular district court—as such information may assist in determining the general location of the targeted phone.

b. (U//FOUO)

[Redacted]

b2
b7E

c. (U//FOUO)

[Redacted]

b2
b7E

[Redacted] Under Kyllo v. United States, 533 U.S. 27 (2001), the use of equipment not in general public use to acquire data that is not otherwise detectable that emanates from a private premise implicates the Fourth Amendment. [Redacted]

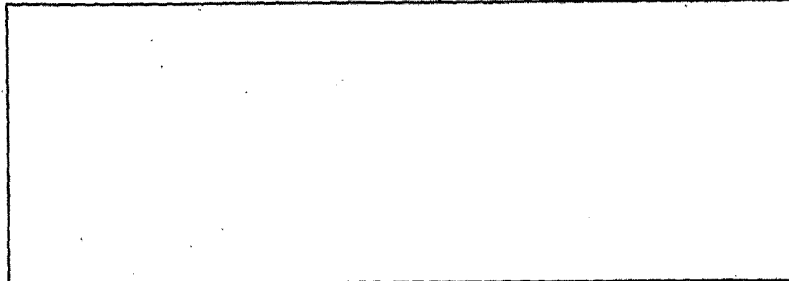
[Redacted]

(U//FOUO)

[Redacted]

b2
b7E

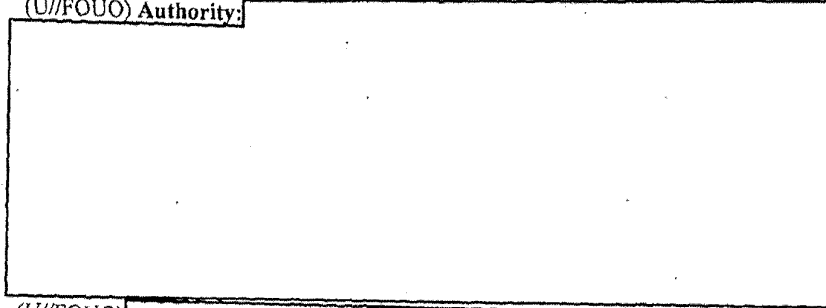
UNCLASSIFIED - FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide



b2
b7E

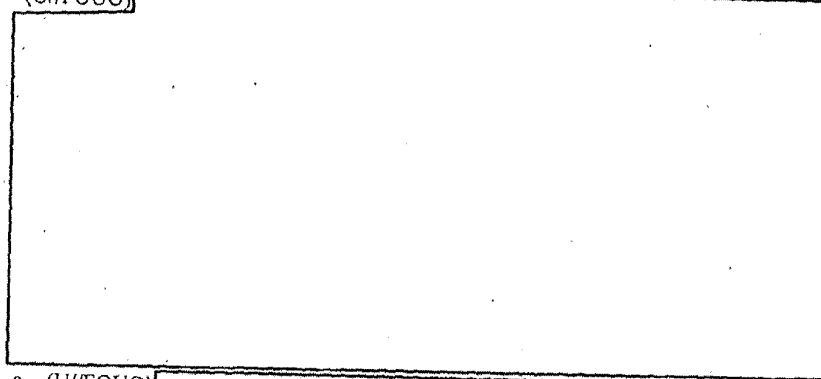
2. (U//FOUO) To Identify an Unknown Target Phone Number:

(U//FOUO) Authority:



b2
b7E

(U//FOUO)



b2
b7E

a. (U//FOUO)



b2
b7E

b. (U//FOUO)



b2
b7E

UNCLASSIFIED - FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide



b2
b7E

- C. (U) **PR/TT Order Language:** The language in the order should state that "the pen register will be implemented unobtrusively and with minimum interference with the services accorded to customers of such service."

UNCLASSIFIED - FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

11.12. (U) Investigative Method: Electronic Surveillance under Title III and under FISA

11.12.1. (U) Summary

(U//FOUO) Electronic Surveillance (ELSUR) is a valuable investigative method. It is, also, a very intrusive means of acquiring information relevant to the effective execution of the FBI's law enforcement, national security and intelligence missions. To ensure that due consideration is given to the competing interests between law enforcement and the effect on privacy and civil liberties, this section contains various administrative and management controls beyond those imposed by statute and DOJ guidelines. Unless otherwise noted, it is the responsibility of the case agent and his/her supervisor to ensure compliance with these instructions. ELSUR is only authorized as an investigative method in the conduct of full investigations. ELSUR requires: (i) administrative or judicial authorization prior to its use; (ii) contact with the Field Office ELSUR Technician to coordinate all necessary recordkeeping; and (iii) consultation with the Technical Advisor (TA) or a designated TTA to determine feasibility, applicability, and use of the appropriate equipment.

(U//FOUO) Application:

b2
b7E

11.12.2. (U) Legal Authority

(U) ELSUR is authorized by chapter 119, 18 U.S.C. §§ 2510-2522 (Title III of the Omnibus and Safe Streets Act of 1968); 50 U.S.C. §§ 1801-1811 (FISA); and E.O. 12333 § 2.5.

11.12.3. (U) Definition of Investigative Method

(U) ELSUR is the non-consensual electronic collection of information (usually communications) under circumstances in which the parties have a reasonable expectation of privacy and court orders or warrants are required.

11.12.4. (U) Standards for Use and Approval Requirements for Investigative Method

A. (U//FOUO) FISA

1. (U//FOUO) FBIHQ and Field Office requests for FISC ELSUR orders must use the FISA Request Form. Field Office requests for FISA orders are submitted and tracked through FISAMS. The FISA request forms, in a question and answer format, have been designed to ensure that all information needed for the preparation of a FISC application is provided to FBIHQ and to the DOJ.
2. (U) A Certification by the Director of the FBI or one of nine other individuals authorized by Congress or the President to provide such certifications that the information being sought is foreign intelligence information; that a significant purpose of the electronic surveillance is to obtain foreign intelligence information; that such

UNCLASSIFIED - FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

information cannot reasonably be obtained by normal investigative techniques; that the information sought is "foreign intelligence information" as defined by FISA; and includes a statement explaining the certifier's basis for the certification.

(U) **Note:** Title 50 of the United States Code Section 1804 specifies the Assistant to the President for National Security Affairs; E.O. 12139 as amended by E.O. 13383 specifies the Director of the FBI, Deputy Director of the FBI, the Director of National Intelligence, the Principal Deputy Director of National Intelligence, the Director of the Central Intelligence Agency, the Secretary of State, the Deputy Secretary of State, the Secretary of Defense, and the Deputy Secretary of Defense as appropriate officials to make certifications required by FISA.

3. (U) Emergency FISA Authority (50 U.S.C. § 1805(f))

(U) The Attorney General, on request from the Director of the FBI or his/her designee, may authorize an emergency FISA for electronic surveillance when it is reasonably determined that an emergency situation exists that precludes advance FISC review and approval and that a factual predication for the issuance of a FISA Order exists. A FISC judge must be informed by DOJ at the time of the emergency authorization and an application must be submitted to that judge as soon as is practicable but not more than seven (7) days after the emergency authority has been approved by the Attorney General. If a court order is denied after an emergency surveillance has been initiated, no information gathered as a result of the surveillance may be used as evidence or disclosed in any trial or other proceeding, and no information concerning any United States person acquired from such surveillance may be used or disclosed 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.

(U//FOUO) For an emergency FISA for electronic surveillance [redacted]

[redacted] at any time.

b2
b7E

B. (U) Title III

(U//FOUO) An SAC (or designee) has the authority to approve requests for "non-sensitive" Title III orders. An Acting SAC may approve such requests in the absence of the SAC. The authority to approve Title III applications may not be delegated lower than the ASAC level. The SAC, with the recommendation of the CDC, must determine whether the request involves sensitive circumstances.

(U//FOUO) If a Title III involves one of the seven "sensitive circumstances," it must be approved by FBIHQ.

(U//FOUO) The following five sensitive circumstances require the approval of a Deputy Assistant Director (DAD) or higher from the Criminal Investigative Division (CID), Counterintelligence Division (CD), or Counterterrorism Division (CTD), as appropriate:

1. (U//FOUO) Significant privilege issues or First Amendment concerns (e.g., attorney-client privilege or other privileged conversations or interception of news media representatives);

UNCLASSIFIED - FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

2. (U//FOUO) Significant privacy concerns (e.g., interceptions of conversations in a bedroom or bathroom);
3. (U//FOUO) Applications based on "relaxed specificity" (i.e., "roving" interception) under 18 U.S.C. § 2518(11)(a) and (b);
4. (U//FOUO) Applications concerning Domestic Terrorism, International Terrorism, or Espionage investigations; or
5. (U//FOUO) Any situation deemed appropriate by the AD of CID or OGC.

(U//FOUO) The following two sensitive circumstances require the approval of the Director, the Acting Director, Deputy Director, or the EAD for the Criminal Cyber Response and Services Branch, or the EAD for the National Security Branch, or the respective Assistant Director for Counterterrorism or Counterintelligence:

6. (U//FOUO) "Emergency" Title III interceptions (i.e., interceptions conducted prior to judicial approval under 18 U.S.C. § 2518(7)); or
7. (U//FOUO) The interception of communications of members of Congress, federal judges, high-level federal officials, high-level state executives, or members of a state judiciary or legislature is anticipated.

(U//FOUO) All requests for electronic surveillance that involve one of the above "sensitive circumstances" must be reviewed by the OGC prior to approval.

(U//FOUO) With the prior approval of the Attorney General, or Attorney General's designee, the United States Attorney or the Strike Force Attorney must apply to a federal judge for a court order authorizing the interception of communications relating to one or more of the offenses listed in Title III (18 U.S.C. § 2516). Judicial oversight continues into the operational phase of the electronic surveillance—installation, monitoring, transcribing and handling of recording media.

(U//FOUO) An extension order may be sought to continue monitoring beyond the initial 30-day period without a lapse in time. When a break in coverage has occurred, a renewal order may be sought to continue monitoring the same interceptees or facilities identified in the original authorization. The affidavit and application in support of an extension or renewal must comply with all of the Title III requirements, including approval of the Attorney General or designee. Except as explained below, extensions that occur within 30 days of the original Title III order do not require review by the SAC or designee. After a lapse of more than 30 days, the SAC or designee must review and request renewed electronic surveillance.

(U//FOUO) There may be situations or unusual circumstances that require the FBI to adopt an already existing Title III from another federal law enforcement agency. This will be approved on a case-by-case basis, only in exceptional circumstances.

(U//FOUO) Before the FBI begins or adopts the administration of a Title III, the Field Office must obtain SAC or designee approval. Thereafter, extensions and renewals within 30 days do not require SAC or designee approval.

(U//FOUO) Emergency Title III interceptions (e.g., interceptions conducted prior to judicial approval under 18 U.S.C. § 2518(7)) – [\[Hyperlink to Memo dated May 22, 2008 Standard and Process Authorization\]](#)

UNCLASSIFIED - FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

(U//FOUO) If an emergency situation arises after regular business hours [redacted]

b2
b7E

[redacted] During regular business hours [redacted] may be reached

(U//FOUO) **Dispute Resolution for both FISA and Title III Applications**

(U//FOUO) [redacted]

b2
b7E

11.12.5. (U) Duration of Approval

A. (U) FISA

(U//FOUO) FISC orders for ELSUR surveillance are provided for the period of time specified in the order that will not exceed: 90 days for United States persons; 120 days for non-United States persons; and one year for a foreign power, as defined in 50 U.S.C. § 1801(a) (1)(2) or (3). For United States persons, renewals of FISA Orders may be requested for the same period of time originally authorized based upon a continued showing of probable cause. For non-United States persons, renewals can be for a period not to exceed one year. All renewal requests should be submitted to DOJ NSD by the requesting Field Office at least 45 days prior to the expiration of the existing order. These requests are to be submitted using the FISA Request Form process in FISAMS.

B. (U) Title III

(U) Title III ELSUR orders are for a period not to exceed 30 days, with subsequent 30 day extensions as authorized by the court.

11.12.6. (U) Specific Procedures

A. (U) FISA

(U//FOUO) [redacted]

b2
b7E

1. (U//FOUO) FISA Verification of Accuracy Procedures

(U//FOUO) [redacted]

b2
b7E

a. (U//FOUO) [redacted]

b2
b7E

i. (U//FOUO) [redacted]

b2
b7E

UNCLASSIFIED - FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

ii. (U//FOUO) [Redacted] b2
b7E

iii. (U//FOUO) [Redacted] b2
b7E

b. (U//FOUO) [Redacted] b2
b7E

2. (U//FOUO) FISA Electronic Surveillance Administrative Sub-file

(U//FOUO) [Redacted] b2
b7E

a. (U//FOUO) [Redacted] b2
b7E

b. (U//FOUO) [Redacted] b2
b7E

3. (U//FOUO) FISA Review Board for FISA Renewals

(U//FOUO) [Redacted] b2
b7E

a. (U//FOUO) [Redacted] b2
b7E

b. (U//FOUO) [Redacted] b2
b7E

UNCLASSIFIED - FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

[Redacted]

b2
b7E

c. (U//FOUO)

[Redacted]

b2
b7E

d. (U//FOUO)

[Redacted]

b2
b7E

(U//FOUO)

[Redacted]

b2
b7E

B. (U) Title III

1. (U//FOUO) The requirements in 18 U.S.C. § 2518 must be followed meticulously in the preparation of a Title III application. In addition, the following points must be covered;

- a. (U//FOUO) Probable cause must be current;
- b. (U//FOUO) There must be a factual basis for concluding that normal investigative procedures have been tried and failed or a demonstration why these procedures appear to be unlikely to succeed or would be too dangerous if tried ("boilerplate" statements in this respect are unacceptable);
- c. (U//FOUO) If the subscriber of the telephone on which coverage is sought is not one of the principals, attempts to identify the subscriber must be made;
- d. (U//FOUO) Minimization will be occur, as statutorily required, if the coverage involves a public telephone booth, a restaurant table, or the like;
- e. (U//FOUO) The facility or premises to be covered is described fully, [Redacted]

b2
b7E

and

f. (U//FOUO) At least 10 days prior to submitting the Title III request to DOJ OEO, the Field Office must forward an electronic communication to FBIHQ [Redacted]

b2
b7E

UNCLASSIFIED - FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

[Redacted]

b2
b7E

2. (U//FOUO)

[Redacted]

b2
b7E

3. (U//FOUO) For details on when, how, and where to conduct pre-Title III ELSUR searches, refer to CID PG.

4. (U//FOUO) Case agents must use the

[Redacted]

b2
b7E

5. (U//FOUO) For additional guidance, see ELSUR Manual.

11.12.7. (U) Notice and Reporting Requirements

A. (U) FISA

(U//FOUO)

[Redacted]

b2
b7E

B. (U) Title III

1. (U//FOUO) The anticipated interception of conversations related to a "Sensitive Investigative Matter" as defined in the AGG-Dom, Part VII.N, requires notice to the appropriate FBIHQ Unit Chief and Section Chief, and DOJ Criminal Division.

2. (U//FOUO)

[Redacted]

b2
b7E

a. (U//FOUO)

[Redacted]

b2
b7E

b. (U//FOUO)

[Redacted]

b2
b7E

c. (U//FOUO)

[Redacted]

b2
b7E

UNCLASSIFIED - FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

3. (U//FOUO) [REDACTED] b2
[REDACTED] b7E
4. (U//FOUO) [REDACTED] b2
[REDACTED] b7E
5. (U//FOUO) Upon completion of a Title III ELSUR activity, the Form 2 report is required to be submitted per 18 U.S.C. § 2519. For details on the completion and submission of the Form 2 report, see the CID PG.

11.12.8. (U) Compliance and Monitoring

A. (U) FISA

(U//FOUO) [REDACTED] b2
b7E

B. (U) Title III

(U//FOUO) Upon completion of Title III ELSUR activity, the Form 2 report is required to be submitted per 18 U.S.C. § 2519. For details on the completion and submission of the Form 2 report, see the CID PG.

11.12.9. (U) Special Circumstances

(U) FISA

(U) Under 50 U.S.C. § 1802, the President, through the Attorney General, may authorize electronic surveillance under FISA without a court order for periods of up to one year, if the Attorney General certifies in writing under oath that the surveillance will be solely directed at acquiring communications that are transmitted by means that are exclusively between or among foreign powers and there is no substantial likelihood of the surveillance acquiring the contents of communications to which United States Persons are parties.

11.12.10. (U) Other Applicable Policies

A. (U) FISA

1. (U//FOUO) CD Policy Guide
2. (U//FOUO) CTD Policy Guide
3. (U//FOUO) Investigative Law Unit Library
4. (U//FOUO) Foreign Intelligence Surveillance Act (FISA) Unit

B. (U//FOUO) OTD PG

1. (U//FOUO) Title III
2. (U//FOUO) Memo dated May 22, 2008 Standard and Process Authorization
3. (U//FOUO) ELSUR Manual
4. (U//FOUO) CID PG
5. (U//FOUO) OTD PG

UNCLASSIFIED - FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

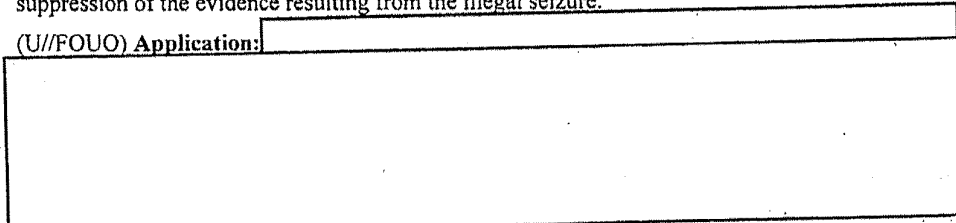
11.13. (U) Investigative Method: Physical searches, including mail openings, requiring judicial order or warrant

(U) AGG-Dom, Part V.A.12.

11.13.1. (U) Summary

(U) The Fourth Amendment to the United States Constitution governs all searches and seizures by government agents. The Fourth Amendment contains two clauses. The first establishes the prohibition against unreasonable searches and seizures. The second provides that no warrant (authorizing a search or seizure) will be issued unless based on probable cause. An unlawful search does not preclude a prosecution. The remedy to the defendant for an unlawful search is suppression of the evidence resulting from the illegal seizure.

(U//FOUO) Application:



b2
b7E

(U) A search is a government invasion of a person's privacy. To qualify as reasonable expectation of privacy, the individual must have an actual subjective expectation of privacy and society must be prepared to recognize that expectation as objectively reasonable. See Katz v. United States, 389 U.S. at 361. The ability to conduct a physical search in an area or situation where an individual has a reasonable expectation of privacy requires a warrant or order issued by a court of competent jurisdiction or an exception to the requirement for such a warrant or order. The warrant or order must be based on probable cause. The United States Supreme Court defines probable cause to search as a "fair probability that contraband or evidence of a crime will be found in a particular place." Illinois v. Gates, 462 U.S. 213, 238 (1983). A government agent may conduct a search without a warrant based on an individual's voluntary consent. A search based on exigent circumstances may also be conducted without a warrant, but the requirement for probable cause remains.

11.13.2. (U) Legal Authority

(U) Searches conducted by the FBI must be in conformity with FRCP Rule 41; FISA, 50 U.S.C. §§ 1821-1829; or E.O. 12333 § 2.5.

11.13.3. (U) Definition of Investigative Method

(U) A physical search constitutes any physical intrusion within the United States into premises or property (including examination of the interior of property by technical means) that is intended to result in the seizure, reproduction, inspection, or alteration of information, material, or property, under circumstances in which a person has a reasonable expectation of privacy.

(U) A physical search requiring a warrant does not include: (i) electronic surveillance as defined in FISA or Title III; or (ii) the acquisition by the United States Government of foreign intelligence information from international foreign communications, or foreign intelligence

UNCLASSIFIED - FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

activities conducted according to otherwise applicable federal law involving a foreign electronic communications system, using a means other than electronic surveillance as defined in FISA.

- A. (U) **Requirement for Reasonableness.** By the terms of the Fourth Amendment, a search must be reasonable at its inception and reasonable in its execution.

b2
b7E

- B. (U) **Reasonable Expectation of Privacy.** The right of privacy is a personal right, not a property concept. It safeguards whatever an individual reasonably expects to be private. The protection normally includes persons, residences, vehicles, other personal property, private conversations, private papers and records. The Supreme Court has determined that there is no reasonable expectation of privacy in certain areas or information. As a result, government intrusions into those areas do not constitute a search and, thus, do not have to meet the requirements of the Fourth Amendment. These areas include: (i) open fields; (ii) prison cells; (iii) public access areas; and (iv) vehicle identification numbers. The Supreme Court has also determined that certain governmental practices do not involve an intrusion into a reasonable expectation of privacy and, therefore, do not amount to a search. These practices include: (i) aerial surveillance conducted from navigable airspace; (ii) field test of suspected controlled substance; and (iii) odor detection. A reasonable expectation of privacy may be terminated by an individual taking steps to voluntarily relinquish the expectation of privacy, such as abandoning property or setting trash at the edge of the curtilage or beyond for collection.

C. (U) **Issuance of search warrant**

1. (U) Under FRCP Rule 41, upon the request of a federal law enforcement officer or an attorney for the government, a search warrant may be issued by:
 - a. (U) a federal magistrate judge, or if none is reasonably available, a judge of a state court of record within the federal district, for a search of property or for a person within the district;
 - b. (U) a federal magistrate judge for a search of property or for a person either within or outside the district if the property or person is within the district when the warrant is sought but might move outside the district before the warrant is executed;
 - c. (U) a federal magistrate judge in any district in which activities related to the terrorism may have occurred, for a search of property or for a person within or outside the district, in an investigation of domestic terrorism or international terrorism (as defined in 18 U.S.C. § 2331); and
 - d. (U) a magistrate with authority in the district to issue a warrant to install a tracking device. The warrant may authorize use of the device to track the movement of a person or property located within the district, outside, or both.
2. (U) Physical searches related to a national security purpose may be authorized by the FISC. (50 U.S.C. §§ 1821-1829)

UNCLASSIFIED - FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

D. (U) Property or Persons That May be Seized with a Warrant.

(U) A warrant may be issued to search for and seize any: (i) property that constitutes evidence of the commission of a criminal offense; (ii) contraband, the fruits of crime, or things otherwise criminally possessed; or (iii) property designed or intended for use or that is or has been used as the means of committing a criminal offense. In addition to a conventional search conducted following issuance of a warrant, examples of search warrants include:

1. (U) Anticipatory Warrants

(U) As the name suggests, an anticipatory warrant differs from other search warrants in that it is not supported by probable cause to believe that contraband exists at the premises to be searched at the time the warrant is issued. Instead, an anticipatory search warrant is validly issued where there is probable cause to believe that a crime has been or is being committed, and that evidence of such crime will be found at the described location at the time of the search, but only after certain specified events transpire. These conditions precedent to the execution of an anticipatory warrant, sometimes referred to as "triggering events," are integral to its validity. Because probable cause for an anticipatory warrant is contingent on the occurrence of certain expected or "triggering" events, typically the future delivery, sale, or purchase of contraband, the judge making the probable cause determination must take into account the likelihood that the triggering event will occur on schedule and as predicted. Should these triggering events fail to materialize, the anticipatory warrant is void.

2. (U) Sneak and peek search warrants

(U) A sneak and peek search warrant allows law enforcement agents to surreptitiously enter a location such as a building, an apartment, garage, storage shed, etc., for the purpose of looking for and documenting evidence of criminal activity. The purpose of this type of warrant is to search for and seize property (either tangible or intangible) without immediately providing notice of the search and a return on the warrant to the owner of the property searched or seized. See FRCP 41(f)(3). A sneak and peek warrant is used to gather additional evidence of criminal activity without prematurely exposing an on-going investigation. The evidence discovered during a sneak and peek search may be used to support a request for a conventional search warrant.

3. (U) Mail Openings

(U) Mail in United States postal channels may be searched only pursuant to court order, or presidential authorization. United States Postal Service regulations governing such activities must be followed. A search of items that are being handled by individual couriers, or commercial courier companies, under circumstances in which there is a reasonable expectation of privacy, or have been sealed for deposit into postal channels, and that are discovered within properties or premises being searched, must be carried out according to unconsented FISA or FRCP Rule 41 physical search procedures.

4. (U) Compelled Disclosure of the Contents of Stored Wire or Electronic Communications

(U) Contents in "electronic storage" (e.g., unopened e-mail/voice mail) require a search warrant. See 18 U.S.C. § 2703(a). A distinction is made between the contents of communications that are in electronic storage (e.g., unopened e-mail) for less than 180

UNCLASSIFIED - FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

days and those in "electronic storage" for longer than 180 days, or those that are no longer in "electronic storage" (e.g., opened e-mail). In enacting the ECPA, Congress concluded that customers may not retain a "reasonable expectation of privacy" in information sent to network providers. However, the contents of an e-mail message that is unopened should nonetheless be protected by Fourth Amendment standards, similar to the contents of a regularly mailed letter. On the other hand, if the contents of an unopened message are kept beyond six months or stored on behalf of the customer after the e-mail has been received or opened, it should be treated the same as a business record in the hands of a third party, such as an accountant or attorney. In that case, the government may subpoena the records from the third party without running afoul of either the Fourth or Fifth Amendment. If a search warrant is used, it may be served on the provider without notice to the customer or subscriber.

11.13.4. (U) Approval Requirements for Investigative Method

- A. (U//FOUO) **Search warrants issued under authority of FRCP Rule 41:** A warrant to search is issued by a federal magistrate (or a state court judge if a federal magistrate is not reasonably available). Coordination with the USAO or DOJ is required to obtain the warrant.
- B. (U//FOUO) **FISA:** In national security investigations, Field Office requests for FISA authorized physical searches must be submitted to FBIHQ using the FBI FISA Request Form. Field Office requests for FISA approval are tracked through FISAMS. This form should be completed by the case agent.
- C. (U//FOUO) **Sensitive Investigative Matter:** Notice to the appropriate FBIHQ substantive Unit Chief and Section Chief is required if the matter under investigation is a sensitive investigative matter. Notice to DOJ is also required, as described in DIOG Section 10.

11.13.5. (U) Duration of Approval

(U) The duration for the execution of a warrant is established by the court order or warrant.

11.13.6. (U) Specific Procedures

A. (U) Obtaining a Warrant under FRCP Rule 41

(U) **Probable Cause.** After receiving an affidavit or other information, a magistrate judge or a judge of a state court of record must issue the warrant if there is probable cause to search for and seize a person or property under FRCP Rule 41(c). Probable cause exists where "the facts and circumstances within the FBI employee's knowledge, and of which they had reasonably trustworthy information are sufficient in themselves to warrant a person of reasonable caution in the belief that..." a crime has been or is being committed, and that seizable property can be found at the place or on the person to be searched. Probable cause is a reasonable belief grounded on facts. In judging whether a reasonable belief exists, the test is whether such a belief would be engendered in a prudent person with the officer's training and experience. To establish probable cause, the affiant must demonstrate a basis for knowledge and belief that the facts are true and that there is probable cause to believe the items listed in the affidavit will be found at the place to be searched.

1. (U) Requesting a Warrant in the Presence of a Judge.

- a. (U) **Warrant on an Affidavit:** When a federal law enforcement officer or an attorney for the government presents an affidavit in support of a warrant, the

UNCLASSIFIED - FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

judge may require the affiant to appear personally and may examine under oath the affiant and any witness the affiant produces.

- b. (U) **Warrant on Sworn Testimony:** The judge may wholly or partially dispense with a written affidavit and base a warrant on sworn testimony if doing so is reasonable under the circumstances.
- c. (U) **Recording Testimony:** Testimony taken in support of a warrant must be recorded by a court reporter or by a suitable recording device, and the judge must file the transcript or recording with the clerk, along with any affidavit.

2. (U) **Requesting a Warrant by Telephonic or Other Means**

- a. (U) **In General:** A magistrate judge may issue a warrant based on information communicated by telephone or other appropriate means, including facsimile transmission.
- b. (U) **Recording Testimony:** Upon learning that an applicant is requesting a warrant, a magistrate judge must: (i) place under oath the applicant and any person on whose testimony the application is based; and (ii) make a verbatim record of the conversation with a suitable recording device, if available, or by a court reporter, or in writing.
- c. (U) **Certifying Testimony:** The magistrate judge must have any recording or court reporter's notes transcribed, certify the transcription's accuracy, and file a copy of the record and the transcription with the clerk. Any written verbatim record must be signed by the magistrate judge and filed with the clerk.
- d. (U) **Suppression Limited:** Absent a finding of bad faith, evidence obtained from a warrant issued under FRCP Rule 41(d)(3)(A) is not subject to suppression on the ground that issuing the warrant in that manner was unreasonable under the circumstances.

3. (U) **Issuing the Warrant**

(U) In general, the magistrate judge or a judge of a state court of record must issue the warrant to an officer authorized to execute it. The warrant must identify the person or property to be searched, identify any person or property to be seized, and designate the magistrate judge to whom it must be returned. The warrant must command the officer to: (i) execute the warrant within a specified time no longer than 10 days; (ii) execute the warrant during the daytime, unless the judge for good cause expressly authorizes execution at another time; and (iii) return the warrant to the magistrate judge designated in the warrant.

4. (U) **Warrant by Telephonic or Other Means**

(U) If a magistrate judge decides to proceed under FRCP Rule 41(d)(3)(A), the following additional procedures apply:

- a. (U) **Preparing a Proposed Duplicate Original Warrant:** The applicant must prepare a "proposed duplicate original warrant" and must read or otherwise transmit the contents of that document verbatim to the magistrate judge.

UNCLASSIFIED - FOR OFFICIAL USE ONLY

Domestic Investigations and Operations Guide

- b. (U) **Preparing an Original Warrant:** The magistrate judge must enter the contents of the proposed duplicate original warrant into an original warrant.
 - c. (U) **Modifications:** The magistrate judge may direct the applicant to modify the proposed duplicate original warrant. In that case, the judge must also modify the original warrant.
 - d. (U) **Signing the Original Warrant and the Duplicate Original Warrant:** Upon determining to issue the warrant, the magistrate judge must immediately sign the original warrant, enter on its face the exact time it is issued, and direct the applicant to sign the judge's name on the duplicate original warrant.
5. (U) **Executing and Returning the Warrant**
- a. (U) **Noting the Time:** The officer executing the warrant must enter on its face the exact date and time it is executed.
 - b. (U) **Inventory:** An officer present during the execution of the warrant must prepare and verify an inventory of any property seized. The officer must do so in the presence of another officer and the person from whom, or from whose premises, the property was taken. If either one is not present, the officer must prepare and verify the inventory in the presence of at least one other credible person.
 - c. (U) **Receipt:** The officer executing the warrant must: (i) give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken; or (ii) leave a copy of the warrant and receipt at the place where the officer took the property.
 - d. (U) **Return:** The officer executing the warrant must promptly return it — together with a copy of the inventory — to the magistrate judge designated on the warrant. The judge must, on request, give a copy of the inventory to the person from whom, or from whose premises, the property was taken and to the applicant for the warrant.
6. (U) **Forwarding Papers to the Clerk**
- (U) The magistrate judge to whom the warrant is returned must attach to the warrant a copy of the return, the inventory, and all other related papers and must deliver them to the clerk in the district where the property was seized. (FRCP Rule 41)
7. (U) **Warrant for a Tracking Device**
- a. (U) **Noting the time:** The officer executing a tracking device warrant must enter on it the exact date and time the device was installed and the period during which it was used.
 - b. (U) **Return:** Within 10 calendar days after the use of the tracking device has ended, the officer executing the warrant must return it to the judge designated in the warrant.
 - c. (U) **Service:** Within 10 calendar days after use of the tracking device has ended, the officer executing the warrant must serve a copy of the warrant on the person who was tracked. Service may be accomplished by delivering a copy to the person

UNCLASSIFIED - FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

who, or whose property was tracked; or by leaving a copy at the person's residence or usual place of abode with an individual of suitable age and discretion who resides at that location and by mailing a copy to the person's last known address. Upon request of the government, the judge may delay notice as provided in FRCP Rule 41(f)(3).

8. (U) Delayed Notice

(U) Upon the government's request, a magistrate judge—or if authorized by FRCP Rule 41(b), a judge of a state court of record—may delay any notice required by FRCP Rule 41 if the delay is authorized by statute.

B. (U) Obtaining a FISA Warrant

(U) Applications for court-authorized physical search pursuant to FISA must be made by a federal officer in writing upon oath or affirmation and with the specific approval of the Attorney General. (See 50 U.S.C. § 1823) Each application must include:

1. (U) The identity of the federal officer making the application;
2. (U) The authority conferred on the Attorney General by the President and the approval of the Attorney General to make the application;
3. (U) The identity, if known, or description of the target of the physical search and a detailed description of the premises or property to be searched and of the information, material, or property to be seized, reproduced, or altered;
4. (U) A statement of the facts and circumstances relied upon and submitted by the applicant that there is probable cause to believe that:
 - a. (U) The target is a foreign power or an agent of a foreign power, provided that no United States person may be considered a foreign power or an agent of a foreign power solely on the basis of activities protected by the First Amendment to the Constitution of the United States; and
 - b. (U) Each of the facilities or places at which the FISA order is directed is being used by a foreign power or an agent of a foreign power.
5. (U) "In determining whether or not probable cause exists for purposes of an order under 50 U.S.C. § 1823(a)(3), a judge may consider past activities of the target, as well as facts and circumstances relating to current or future activities of the target." 50 U.S.C. § 1805(b). As it relates to United States citizens or aliens lawfully admitted for permanent residence, "agent of a foreign power" means any person who:
 - a. (U) Knowingly engages in clandestine intelligence-gathering activities for or on behalf of a foreign power, whose activities involve or may involve a violation of the criminal statutes of the United States;
 - b. (U) 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, whose activities involve or are about to involve a violation of the criminal statutes of the United States;

UNCLASSIFIED - FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

- c. (U) Knowingly engages in sabotage or international terrorism, or activities that are in preparation therefore, for or on behalf of a foreign power;
- d. (U) 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. (U) Knowingly aids or abets any person in the conduct of activities described in subparagraph 'a,' 'b,' or 'c,' above or knowingly conspires with any person to engage in activities described in subparagraph 'a,' 'b,' or 'c,' above. 50 U.S.C. § 1801(b) (2).

(U) For purposes of the above statute, 50 U.S.C. § 1801(a) (1) defines "foreign power" to include "a group engaged in international terrorism or activities in preparation therefore," 50 U.S.C. § 1801(a) (4), as well as, among other things, "a foreign government or any component thereof, whether or not recognized by the United States." Title 50 of the United States Code Section 1801(c) defines "international terrorism" as activities that:

- (a) (U) Involve violent acts or acts dangerous to human life that are a violation of the criminal laws of the United States or of any State, or that would be a criminal violation if committed within the jurisdiction of the United States or any State;
 - (b) (U) Appear to be intended—
 - (1) (U) To intimidate or coerce a civilian population;
 - (2) (U) To influence the policy of a government by intimidation or coercion; or
 - (3) (U) To affect the conduct of a government by assassination or kidnapping; and
 - (c) (U) Occur totally outside the United States, 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 by the applicant to justify the belief that:
 - (i) the target is a foreign power or agent of a foreign power; (ii) the premises or property to be searched contains foreign intelligence information; and (iii) the premises or property to be searched is owned, used, possessed by, or is in transit to or from a foreign power or an agent of a foreign power.
- 6. (U) A statement of the proposed minimization procedures that have been approved by the Attorney General;
 - 7. (U) A detailed description of the nature of the foreign intelligence information sought and the manner in which the physical search will be conducted;
 - 8. (U) A Certification by the Director of the FBI or one of nine other individuals authorized by Congress or the President to provide such certifications that the information being sought is foreign intelligence information; that a significant purpose of the search is to obtain foreign intelligence information; that such information cannot reasonably be

UNCLASSIFIED - FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

obtained by normal investigative techniques; that the information sought is "foreign intelligence information" as defined by FISA; and includes a statement explaining the certifier's basis for the certification.

(U) **Note:** Title 50 of the United States Code Section 1804 specifies the Assistant to the President for National Security Affairs; E.O. 12949, as amended specifies the Director of the FBI, Deputy Director of the FBI, the Director of National Intelligence, the Principal Deputy Director of National Intelligence, the Director of the Central Intelligence Agency, the Secretary of State, the Deputy Secretary of State, the Secretary of Defense, and the Deputy Secretary of Defense as appropriate officials to make certifications required by FISA.

9. (U) Where the physical search may involve the residence of a United States person, the Attorney General must state what investigative techniques have previously been used to obtain the foreign intelligence information concerned and the degree to which these techniques resulted in acquiring such information;
10. (U) A statement of the facts concerning all previous applications before the FISA court that have been made involving any of the persons, premises, or property specified in the application and the actions taken on each previous application;
11. (U) The Attorney General may require any other affidavit or certification from any other officer in connection with an application; and
12. (U) The Court may require the applicant to furnish such other information as may be necessary to make the determinations required to issue an Order.

C. (U) Length of Period of Authorization for FISC Orders

1. (U) Generally, a FISC Order approving an unconsented physical search will specify the period of time during which physical searches are approved and provide that the government will be permitted the period of time necessary to achieve the purpose, or for 90 days, whichever is less, except that authority may be:
 - a. (U) For no more than one year for "Foreign Power" targets (establishments); or
 - b. (U) For no more than 120 days for an agent of a foreign power, with renewals for up to one year for non-United States persons.
2. (U) An extension of physical search authority may be granted on the same basis as the original order upon a separate application for an extension and upon new findings made in the same manner as the original order.
3. (U) **Emergency FISA Authority**
 - a. (U) The Attorney General may authorize an emergency physical search under FISA when he reasonably makes a determination that an emergency situation exists that precludes advance FISA court review and approval, and there exists a factual predication for the issuance of a FISA Court Order. In such instances, a FISC judge must be informed by the Attorney General or his designee at the time of the authorization and an application according to FISA requirements is submitted to the judge as soon as is practicable but not more than seven (7) days after the emergency authority has been approved by the Attorney General.

UNCLASSIFIED - FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

b. (U) If a court order is denied after an emergency authorization has been initiated, no information gathered as a result of the search may be used in any manner except if with the approval of the Attorney General, the information indicates a threat of death or serious bodily harm to any person.

c. (U//FOUO) For an emergency FISA for physical search, [redacted]
[redacted]

b2
b7E

4. (U) Special Circumstances

(U) The President through the Attorney General may also authorize a physical search under FISA without a court order for periods of up to one year, if the Attorney General certifies that the search will be solely directed at premises, information, material, or property that is used exclusively by or under the open and exclusive control of a foreign power; there is no substantial likelihood that the physical search will involve the premises, information, material, or property of a United States person; and there are minimization procedures that have been reported to the court and Congress. The FBI's involvement in such approvals is usually in furtherance of activities pursued according to E.O. 12333. Copies of such certifications are to be transmitted to the FISA Court (see 50 U.S.C. § 1822[a]).

(U) Information concerning United States persons acquired through unconsented physical searches may only be used according to minimization procedures. See: 50 U.S.C. §§ 1824(d)(4) and 1825(a).

5. (U) Required Notice

(U) If an authorized search involves the premises of a United States person, and the Attorney General determines that there is no national security interest in continuing the secrecy of the search, the Attorney General must provide notice to the United States person that the premises was searched and the identification of any property seized, altered, or reproduced during the search.

6. (U//FOUO) FISA Verification of Accuracy Procedures

(U//FOUO) [redacted]
[redacted]

b2
b7E

a. (U//FOUO) Each case file for which an application is prepared for submission to the FISC will include a sub-file to be labeled [redacted]. This sub-file is to contain copies of the supportive documentation relied upon when making the certifications to the [redacted] file is to include:

b2
b7E

i. (U//FOUO) [redacted]
[redacted]

b2
b7E

ii. (U//FOUO) [redacted]
[redacted]

b2
b7E

UNCLASSIFIED - FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

iii. (U//FOUO)

[Redacted]

b2
b7E

b. (U//FOUO)

[Redacted]

b2
b7E

7. (U//FOUO) FISA Physical Search Administrative Sub-file

(U//FOUO) Each case file for which an application is or has been prepared for submission to the FISC will include a sub-file to be labeled [Redacted]. This sub-file is to contain copies of all applications to and orders issued by the FISC for the conduct of physical searches in the investigative case. The following data must be included in this [Redacted].

b2
b7E

a. (U//FOUO)

[Redacted]

b2
b7E

b. (U//FOUO)

[Redacted]

b2
b7E

8. (U//FOUO) FISA Review Board for FISA Renewals

(U//FOUO)

[Redacted]

b2
b7E

a. (U//FOUO)

[Redacted]

b2
b7E

b. (U//FOUO)

[Redacted]

b2
b7E

c. (U//FOUO)

[Redacted]

b2
b7E

UNCLASSIFIED - FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

[Redacted]

b2
b7E

d. (U//FOUO) Appealing the Decision of the Review Board: [Redacted]

[Redacted]

b2
b7E

(U//FOUO) [Redacted]

[Redacted]

b2
b7E

UNCLASSIFIED - FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

11.14. (U) Investigative Method: Acquisition of foreign intelligence information in conformity with Title VII of the Foreign Intelligence Surveillance Act

11.14.1. (U) Summary

(U) Titles I and III of the FISA (codified as 50 U.S.C. §§ 1801, et seq.) provide the standard, traditional methods of collection against agents of foreign powers (including United States and non-United States persons) and foreign power establishments inside the United States. Title VII of FISA, "Additional Procedures Regarding Certain Persons Outside the United States," provides means for collections of individuals outside the United States.

11.14.2. (U) Legal Authority

(U) FISA Amendments Act of 2008 (122 Stat 2436)

(U) AGG-Dom, Part V.A.13

11.14.3. (U) Definition of Investigative Method

(U) Title VII is to be used for conducting FISAs on certain persons located outside the United States

11.14.4. (U//FOUO) Standards for Use and Approval Requirements for Investigative Method

(U//FOUO) See requirements under DIOG Sections 11.12 and 11.13 and requirements specified above.

11.14.5. (U) Duration of Approval

(U//FOUO) See requirements under DIOG Sections 11.12 and 11.13

11.14.6. (U//FOUO) Specific Collection Procedures for Title VII

(U) The relevant procedures (or collections) under Title VII are:

A. (U) Section 702 - "Procedures for Targeting Certain Persons Outside the United States Other than United States Persons"

(U//FOUO) Under Section 702, the Government has the authority to target non-United States persons who are located outside the United States if the collection is effected with the assistance of a United States provider and if the collection occurs inside the United States. This section does not require a traditional FISA request. Rather, under this section the Attorney General and the Director of National Intelligence are required to file yearly determinations (filed as "Certifications") with the FISC that authorize the targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information. The Certifications are accompanied by, in the case of the FBI, an affidavit signed by the FBI Director. In addition, the FBI is required to file "Targeting Procedures" designed to ensure that the acquisition is limited to persons reasonably believed to be located outside the United States and "to prevent the intentional acquisition of any communications as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States." Finally, the FBI is also required to follow minimization procedures.

UNCLASSIFIED - FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

B. (U) Section 703 - "Certain Acquisitions Inside the United States Targeting United States Persons Outside the United States"

(U//FOUO) Under Section 703, the Government has the authority to target United States persons who are located outside the United States if the collection is effected with the assistance of a United States provider and if the collection occurs inside the United States. This section only authorizes electronic surveillance or the acquisition of stored electronic communications or stored electronic data that requires a court order. Under this section, the FBI will submit a FISA request and obtain a FISC order and secondary orders, as needed. The process is the same as the current FISA process. Refer to the FISA Unit's website for further information. This section allows for emergency authorization and the FBI's Standard Minimization Procedures apply to the collection. Finally, under the statute, the surveillance must cease immediately if the target enters the United States. If the FBI wishes to surveil the United States person while he or she is in the United States, the FBI must obtain a separate court order under Title I (electronic surveillance) and/or Title III (physical search) of FISA in order to surveil that United States person while the person is located in the United States.

C. (U) Section 704 - "Other Acquisitions Targeting United States Persons Outside the United States"

(U//FOUO) Under Section 704, the Government has the authority to target United States persons who are located outside the United States if the collection occurs outside the United States (i.e., without the assistance of a United States' provider). The statute requires that the FISA court issue an order finding probable cause to believe that the United States person target is an agent of a foreign power and reasonably believed to be located outside the United States "under circumstances in which the targeted United States person has a reasonable expectation of privacy and a warrant would be required if the acquisition were conducted in the United States for law enforcement purposes." Under this section, the FBI will submit a FISA request and obtain a FISC order but will not obtain secondary orders. The process for obtaining these orders is the same as the current FISA request process. Refer to the FISA Unit's intranet website for further information. This section allows for emergency authorization and the FBI's Standard Minimization Procedures apply to the collection. Finally, surveillance authorized under this section must cease if the United States person enters the United States but may be re-started if the person is again reasonably believed to be outside the United States during the authorized period of surveillance. However, if there is a need to surveil the target while the target is located inside the United States, a separate court order must be obtained.

(U//FOUO) Generally, the FBI requires the assistance of other USIC agencies to implement this type of surveillance. Specific procedures for requesting that another USIC agency implement the surveillance for the FBI, if necessary, are classified and delineated in FBI Corporate Policy 121N.


D. (U) Section 705 - "Joint Applications and Concurrent Authorizations"

(U//FOUO) Section 705(a), "joint applications," allows for the FISC to, upon request of the FBI, authorize a joint application for targeting a United States person under both Sections 703 and 704 (inside and outside the United States simultaneously).

UNCLASSIFIED - FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

(U//FOUO) Section 705(b), "concurrent authorizations," states that if an order has been obtained under Section 105 (electronic surveillance under Title I of FISA) or 304 (physical search under Title III of FISA), the Attorney General may authorize the targeting of a United States person while such person is reasonably believed to be located outside the United States. The Attorney General has this authority under E.O. 12333 § 2.5. In other words, if a United States person target of a "regular" FISA travels outside the United States during the authorized period of the surveillance, the Attorney General, under Section 705(b) and E.O. 12333 § 2.5, can concurrently authorize surveillance to continue while the person is overseas obviating the need to obtain a separate order under Sections 703 or 704. To effectuate this authority, the Attorney General's "Approval page" on all FBI United States person FISAs contains standard language authorizing surveillance abroad, if needed.

(U//FOUO)



b2
b7E

ALL FBI INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 07-08-2009 BY 60322 UC/LP/STP/JCF

UNCLASSIFIED - FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

**Appendix A: The Attorney General's Guidelines for Domestic FBI
Operations**

**The Attorney General's Guidelines for
Domestic FBI Operations**

A-1

FOR OFFICIAL USE ONLY

ACLU EC-75

PREAMBLE

These Guidelines are issued under the authority of the Attorney General as provided in sections 509, 510, 533, and 534 of title 28, United States Code, and Executive Order 12333. They apply to domestic investigative activities of the Federal Bureau of Investigation (FBI) and other activities as provided herein.

TABLE OF CONTENTS

INTRODUCTION 5

 A. FBI RESPONSIBILITIES - FEDERAL CRIMES, THREATS TO THE
 NATIONAL SECURITY, FOREIGN INTELLIGENCE 6

 B. THE FBI AS AN INTELLIGENCE AGENCY 9

 C. OVERSIGHT 10

I. GENERAL AUTHORITIES AND PRINCIPLES 12

 A. SCOPE 12

 B. GENERAL AUTHORITIES 12

 C. USE OF AUTHORITIES AND METHODS 12

 D. NATURE AND APPLICATION OF THE GUIDELINES 14

II. INVESTIGATIONS AND INTELLIGENCE GATHERING 16

 A. ASSESSMENTS 19

 B. PREDICATED INVESTIGATIONS 20

 C. ENTERPRISE INVESTIGATIONS 23

III. ASSISTANCE TO OTHER AGENCIES 25

 A. THE INTELLIGENCE COMMUNITY 25

 B. FEDERAL AGENCIES GENERALLY 25

 C. STATE, LOCAL, OR TRIBAL AGENCIES 27

 D. FOREIGN AGENCIES 27

 E. APPLICABLE STANDARDS AND PROCEDURES 28

IV. INTELLIGENCE ANALYSIS AND PLANNING 29

 A. STRATEGIC INTELLIGENCE ANALYSIS 29

 B. REPORTS AND ASSESSMENTS GENERALLY 29

 C. INTELLIGENCE SYSTEMS 29

V. AUTHORIZED METHODS 31

 A. PARTICULAR METHODS 31

 B. SPECIAL REQUIREMENTS 32

 C. OTHERWISE ILLEGAL ACTIVITY 33

VI. RETENTION AND SHARING OF INFORMATION 35

 A. RETENTION OF INFORMATION 35

 B. INFORMATION SHARING GENERALLY 35

 C. INFORMATION RELATING TO CRIMINAL MATTERS 36

 D. INFORMATION RELATING TO NATIONAL SECURITY AND
 FOREIGN INTELLIGENCE MATTERS 37

VII. DEFINITIONS 42

II. INVESTIGATIONS AND INTELLIGENCE GATHERING

This Part of the Guidelines authorizes the FBI to conduct investigations to detect, obtain information about, and prevent and protect against federal crimes and threats to the national security and to collect foreign intelligence.

When an authorized purpose exists, the focus of activities authorized by this Part may be whatever the circumstances warrant. The subject of such an activity may be, for example, a particular crime or threatened crime; conduct constituting a threat to the national security; an individual, group, or organization that may be involved in criminal or national security-threatening conduct; or a topical matter of foreign intelligence interest.

Investigations may also be undertaken for protective purposes in relation to individuals, groups, or other entities that may be targeted for criminal victimization or acquisition, or for terrorist attack or other deprivations by the enemies of the United States. For example, the participation of the FBI in special events management, in relation to public events or other activities whose character may make them attractive targets for terrorist attack, is an authorized exercise of the authorities conveyed by these Guidelines. Likewise, FBI counterintelligence activities directed to identifying and securing facilities, personnel, or information that may be targeted for infiltration, recruitment, or acquisition by foreign intelligence services are authorized exercises of the authorities conveyed by these Guidelines.

The identification and recruitment of human sources – who may be able to provide or obtain information relating to criminal activities, information relating to terrorism, espionage, or other threats to the national security, or information relating to matters of foreign intelligence interest – is also critical to the effectiveness of the FBI's law enforcement, national security, and intelligence programs, and activities undertaken for this purpose are authorized and encouraged.

The scope of authorized activities under this Part is not limited to "investigation" in a narrow sense, such as solving particular cases or obtaining evidence for use in particular criminal prosecutions. Rather, these activities also provide critical information needed for broader analytic and intelligence purposes to facilitate the solution and prevention of crime, protect the national security, and further foreign intelligence objectives. These purposes include use of the information in intelligence analysis and planning under Part IV, and dissemination of the information to other law enforcement, Intelligence Community, and White House agencies under Part VI. Information obtained at all stages of investigative activity is accordingly to be retained and disseminated for these purposes as provided in these Guidelines, or in FBI policy consistent with these Guidelines, regardless of whether it furthers investigative objectives in a narrower or more immediate sense.

In the course of activities under these Guidelines, the FBI may incidentally obtain information relating to matters outside of its areas of primary investigative responsibility. For example, information relating to violations of state or local law or foreign law may be

incidentally obtained in the course of investigating federal crimes or threats to the national security or in collecting foreign intelligence. These Guidelines do not bar the acquisition of such information in the course of authorized investigative activities, the retention of such information, or its dissemination as appropriate to the responsible authorities in other agencies or jurisdictions. Part VI of these Guidelines includes specific authorizations and requirements for sharing such information with relevant agencies and officials.

This Part authorizes different levels of information gathering activity, which afford the FBI flexibility, under appropriate standards and procedures, to adapt the methods utilized and the information sought to the nature of the matter under investigation and the character of the information supporting the need for investigation.

Assessments, authorized by Subpart A of this Part, require an authorized purpose but not any particular factual predication. For example, 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. Likewise, in the exercise of its protective functions, the FBI is not constrained to wait until information is received indicating that a particular event, activity, or facility has drawn the attention of those who would threaten the national security. Rather, the FBI must take the initiative to secure and protect activities and entities whose character may make them attractive targets for terrorism or espionage. The proactive investigative authority conveyed in assessments is designed for, and may be utilized by, the FBI in the discharge of these responsibilities. For example, assessments may be conducted as part of the FBI's special events management activities.

More broadly, detecting and interrupting criminal activities at their early stages, and preventing crimes from occurring in the first place, is preferable to allowing criminal plots and activities to come to fruition. Hence, assessments may be undertaken proactively with such objectives as detecting criminal activities; obtaining information on individuals, groups, or organizations of possible investigative interest, either because they may be involved in criminal or national security-threatening activities or because they may be targeted for attack or victimization by such activities; and identifying and assessing individuals who may have value as human sources. For example, assessment activities may involve proactively surfing the Internet to find publicly accessible websites and services through which recruitment by terrorist organizations and promotion of terrorist crimes is openly taking place; through which child pornography is advertised and traded; through which efforts are made by sexual predators to lure children for purposes of sexual abuse; or through which fraudulent schemes are perpetrated against the public.

The methods authorized in assessments are generally those of relatively low intrusiveness, such as obtaining publicly available information, checking government records,

and requesting information from members of the public. These Guidelines do not impose supervisory approval requirements in assessments, given the types of techniques that are authorized at this stage (e.g., perusing the Internet for publicly available information). However, FBI policy will prescribe supervisory approval requirements for certain assessments, considering such matters as the purpose of the assessment and the methods being utilized.

Beyond the proactive information gathering functions described above, assessments may be used when allegations or other information concerning crimes or threats to the national security is received or obtained, and the matter can be checked out or resolved through the relatively non-intrusive methods authorized in assessments. The checking of investigative leads in this manner can avoid the need to proceed to more formal levels of investigative activity, if the results of an assessment indicate that further investigation is not warranted.

Subpart B of this Part authorizes a second level of investigative activity, predicated investigations. The purposes or objectives of predicated investigations are essentially the same as those of assessments, but predication as provided in these Guidelines is needed – generally, allegations, reports, facts or circumstances indicative of possible criminal or national security-threatening activity, or the potential for acquiring information responsive to foreign intelligence requirements – and supervisory approval must be obtained, to initiate predicated investigations. Corresponding to the stronger predication and approval requirements, all lawful methods may be used in predicated investigations. A classified directive provides further specification concerning circumstances supporting certain predicated investigations.

Predicated investigations that concern federal crimes or threats to the national security are subdivided into preliminary investigations and full investigations. Preliminary investigations may be initiated on the basis of any allegation or information indicative of possible criminal or national security-threatening activity, but more substantial factual predication is required for full investigations. While time limits are set for the completion of preliminary investigations, full investigations may be pursued without preset limits on their duration.

The final investigative category under this Part of the Guidelines is enterprise investigations, authorized by Subpart C, which permit a general examination of the structure, scope, and nature of certain groups and organizations. Enterprise investigations are a type of full investigations. Hence, they are subject to the purpose, approval, and predication requirements that apply to full investigations, and all lawful methods may be used in carrying them out. The distinctive characteristic of enterprise investigations is that they concern groups or organizations that may be involved in the most serious criminal or national security threats to the public – generally, patterns of racketeering activity, terrorism or other threats to the national security, or the commission of offenses characteristically involved in terrorism as described in 18 U.S.C. 2332b(g)(5)(B). A broad examination of the characteristics of groups satisfying these criteria is authorized in enterprise investigations, including any relationship of the group to a foreign power, its size and composition, its geographic dimensions and finances, its past acts and goals, and its capacity for harm.

A. ASSESSMENTS

1. Purposes

Assessments may be carried out to detect, obtain information about, or prevent or protect against federal crimes or threats to the national security or to collect foreign intelligence.

2. Approval

The conduct of assessments is subject to any supervisory approval requirements prescribed by FBI policy.

3. Authorized Activities

Activities that may be carried out for the purposes described in paragraph 1. in an assessment include:

- a. seeking information, proactively or in response to investigative leads, relating to:
 - i. activities constituting violations of federal criminal law or threats to the national security,
 - ii. the involvement or role of individuals, groups, or organizations in such activities; or
 - iii. matters of foreign intelligence interest responsive to foreign intelligence requirements;
- b. identifying and obtaining information about potential targets of or vulnerabilities to criminal activities in violation of federal law or threats to the national security;
- c. seeking information to identify potential human sources, assess the suitability, credibility, or value of individuals as human sources, validate human sources, or maintain the cover or credibility of human sources, who may be able to provide or obtain information relating to criminal activities in violation of federal law, threats to the national security, or matters of foreign intelligence interest; and
- d. obtaining information to inform or facilitate intelligence analysis and planning as described in Part IV of these Guidelines.

4. **Authorized Methods**

Only the following methods may be used in assessments:

- a. Obtain publicly available information.
- b. Access and examine FBI and other Department of Justice records, and obtain information from any FBI or other Department of Justice personnel.
- c. Access and examine records maintained by, and request information from, other federal, state, local, or tribal, or foreign governmental entities or agencies.
- d. Use online services and resources (whether nonprofit or commercial).
- e. Use and recruit human sources in conformity with the Attorney General's Guidelines Regarding the Use of FBI Confidential Human Sources.
- f. Interview or request information from members of the public and private entities.
- g. Accept information voluntarily provided by governmental or private entities.
- h. Engage in observation or surveillance not requiring a court order.
- i. Grand jury subpoenas for telephone or electronic mail subscriber information.

B. PREDICATED INVESTIGATIONS

1. **Purposes**

Predicated investigations may be carried out to detect, obtain information about, or prevent or protect against federal crimes or threats to the national security or to collect foreign intelligence.

2. **Approval**

The initiation of a predicated investigation requires supervisory approval at a level or levels specified by FBI policy. A predicated investigation based on paragraph 3.c. (relating to foreign intelligence) must be approved by a Special Agent in Charge or by an FBI Headquarters official as provided in such policy.

3. Circumstances Warranting Investigation

A predicated investigation may be initiated on the basis of any of the following circumstances:

- a. An activity constituting a federal crime or a threat to the national security has or may have occurred, is or may be occurring, or will or may occur and the investigation may obtain information relating to the activity or the involvement or role of an individual, group, or organization in such activity.
- b. An individual, group, organization, entity, information, property, or activity is or may be a target of attack, victimization, acquisition, infiltration, or recruitment in connection with criminal activity in violation of federal law or a threat to the national security and the investigation may obtain information that would help to protect against such activity or threat.
- c. The investigation may obtain foreign intelligence that is responsive to a foreign intelligence requirement.

4. Preliminary and Full Investigations

A predicated investigation relating to a federal crime or threat to the national security may be conducted as a preliminary investigation or a full investigation. A predicated investigation that is based solely on the authority to collect foreign intelligence may be conducted only as a full investigation.

a. Preliminary investigations

i. Predication Required for Preliminary Investigations

A preliminary investigation may be initiated on the basis of information or an allegation indicating the existence of a circumstance described in paragraph 3.a.-b.

ii. Duration of Preliminary Investigations

A preliminary investigation must be concluded within six months of its initiation, which may be extended by up to six months by the Special Agent in Charge. Extensions of preliminary investigations beyond a year must be approved by FBI Headquarters.

iii. Methods Allowed in Preliminary Investigations

All lawful methods may be used in a preliminary investigation except for methods within the scope of Part V.A.11.-.13. of these Guidelines.

b. Full Investigations

i. Predication Required for Full Investigations

A full investigation may be initiated if there is an articulable factual basis for the investigation that reasonably indicates that a circumstance described in paragraph 3.a.-b. exists or if a circumstance described in paragraph 3.c. exists.

ii. Methods Allowed in Full Investigations

All lawful methods may be used in a full investigation.

5. Notice Requirements

- a. An FBI field office shall notify FBI Headquarters and the United States Attorney or other appropriate Department of Justice official of the initiation by the field office of a predicated investigation involving a sensitive investigative matter. If the investigation is initiated by FBI Headquarters, FBI Headquarters shall notify the United States Attorney or other appropriate Department of Justice official of the initiation of such an investigation. If the investigation concerns a threat to the national security, an official of the National Security Division must be notified. The notice shall identify all sensitive investigative matters involved in the investigation.
- b. The FBI shall notify the National Security Division of:
 - i. the initiation of any full investigation of a United States person relating to a threat to the national security; and
 - ii. the initiation of any full investigation that is based on paragraph 3.c. (relating to foreign intelligence).
- c. The notifications under subparagraphs a. and b. shall be made as soon as practicable, but no later than 30 days after the initiation of an investigation.

- d. The FBI shall notify the Deputy Attorney General if FBI Headquarters disapproves a field office's initiation of a predicated investigation relating to a threat to the national security on the ground that the predication for the investigation is insufficient.

C. ENTERPRISE INVESTIGATIONS

1. Definition

A full investigation of a group or organization may be initiated as an enterprise investigation if there is an articulable factual basis for the investigation that reasonably indicates that the group or organization may have engaged or may be engaged in, or may have or may be engaged in planning or preparation or provision of support for:

- a. a pattern of racketeering activity as defined in 18 U.S.C. 1961(5);
- b. international terrorism or other threat to the national security;
- c. domestic terrorism as defined in 18 U.S.C. 2331(5) involving a violation of federal criminal law;
- d. furthering political or social goals wholly or in part through activities that involve force or violence and a violation of federal criminal law; or
- e. an offense described in 18 U.S.C. 2332b(g)(5)(B) or 18 U.S.C. 43.

2. Scope

The information sought in an enterprise investigation may include a general examination of the structure, scope, and nature of the group or organization including: its relationship, if any, to a foreign power; the identity and relationship of its members, employees, or other persons who may be acting in furtherance of its objectives; its finances and resources; its geographical dimensions; and its past and future activities and goals.

3. Notice and Reporting Requirements

- a. The responsible Department of Justice component for the purpose of notification and reports in enterprise investigations is the National Security Division, except that, for the purpose of notifications and reports in an enterprise investigation relating to a pattern of racketeering activity that does not involve an offense or offenses described in 18 U.S.C. 2332b(g)(5)(B), the responsible Department of Justice component is the

V. AUTHORIZED METHODS

A. PARTICULAR METHODS

All lawful investigative methods may be used in activities under these Guidelines as authorized by these Guidelines. Authorized methods include, but are not limited to, those identified in the following list. The methods identified in the list are in some instances subject to special restrictions or review or approval requirements as noted:

1. The methods described in Part II.A.4 of these Guidelines.
2. Mail covers.
3. Physical searches of personal or real property where a warrant or court order is not legally required because there is no reasonable expectation of privacy (e.g., trash covers).
4. Consensual monitoring of communications, including consensual computer monitoring, subject to legal review by the Chief Division Counsel or the FBI Office of the General Counsel. Where a sensitive monitoring circumstance is involved, the monitoring must be approved by the Criminal Division or, if the investigation concerns a threat to the national security or foreign intelligence, by the National Security Division.
5. Use of closed-circuit television, direction finders, and other monitoring devices, subject to legal review by the Chief Division Counsel or the FBI Office of the General Counsel. (The methods described in this paragraph usually do not require court orders or warrants unless they involve physical trespass or non-consensual monitoring of communications, but legal review is necessary to ensure compliance with all applicable legal requirements.)
6. Polygraph examinations.
7. Undercover operations. In investigations relating to activities in violation of federal criminal law that do not concern threats to the national security or foreign intelligence, undercover operations must be carried out in conformity with the Attorney General's Guidelines on Federal Bureau of Investigation Undercover Operations. In investigations that are not subject to the preceding sentence because they concern threats to the national security or foreign intelligence, undercover operations involving religious or political organizations must be reviewed and approved by FBI Headquarters, with participation by the National Security Division in the review process.
8. Compulsory process as authorized by law, including grand jury subpoenas and

other subpoenas, National Security Letters (15 U.S.C. 1681u, 1681v; 18 U.S.C. 2709; 12 U.S.C. 3414(a)(5)(A); 50 U.S.C. 436), and Foreign Intelligence Surveillance Act orders for the production of tangible things (50 U.S.C. 1861-63).

9. Accessing stored wire and electronic communications and transactional records in conformity with chapter 121 of title 18, United States Code (18 U.S.C. 2701-2712).
10. Use of pen registers and trap and trace devices in conformity with chapter 206 of title 18, United States Code (18 U.S.C. 3121-3127), or the Foreign Intelligence Surveillance Act (50 U.S.C. 1841-1846).
11. Electronic surveillance in conformity with chapter 119 of title 18, United States Code (18 U.S.C. 2510-2522), the Foreign Intelligence Surveillance Act, or Executive Order 12333 § 2.5.
12. Physical searches, including mail openings, in conformity with Rule 41 of the Federal Rules of Criminal Procedure, the Foreign Intelligence Surveillance Act, or Executive Order 12333 § 2.5. A classified directive provides additional limitation on certain searches.
13. Acquisition of foreign intelligence information in conformity with title VII of the Foreign Intelligence Surveillance Act.

B. SPECIAL REQUIREMENTS

Beyond the limitations noted in the list above relating to particular investigative methods, the following requirements are to be observed:

1. Contacts with Represented Persons

Contact with represented persons may implicate legal restrictions and affect the admissibility of resulting evidence. Hence, if an individual is known to be represented by counsel in a particular matter, the FBI will follow applicable law and Department procedure concerning contact with represented individuals in the absence of prior notice to counsel. The Special Agent in Charge and the United States Attorney or their designees shall consult periodically on applicable law and Department procedure. Where issues arise concerning the consistency of contacts with represented persons with applicable attorney conduct rules, the United States Attorney's Office should consult with the Professional Responsibility Advisory Office.

2. Use of Classified Investigative Technologies

Inappropriate use of classified investigative technologies may risk the compromise of such technologies. Hence, in an investigation relating to activities in violation of federal criminal law that does not concern a threat to the national security or foreign intelligence, the use of such technologies must be in conformity with the Procedures for the Use of Classified Investigative Technologies in Criminal Cases.

C. OTHERWISE ILLEGAL ACTIVITY

1. Otherwise illegal activity by an FBI agent or employee in an undercover operation relating to activity in violation of federal criminal law that does not concern a threat to the national security or foreign intelligence must be approved in conformity with the Attorney General's Guidelines on Federal Bureau of Investigation Undercover Operations. Approval of otherwise illegal activity in conformity with those guidelines is sufficient and satisfies any approval requirement that would otherwise apply under these Guidelines.
2. Otherwise illegal activity by a human source must be approved in conformity with the Attorney General's Guidelines Regarding the Use of FBI Confidential Human Sources.
3. Otherwise illegal activity by an FBI agent or employee that is not within the scope of paragraph 1. must be approved by a United States Attorney's Office or a Department of Justice Division, except that a Special Agent in Charge may authorize the following:
 - a. otherwise illegal activity that would not be a felony under federal, state, local, or tribal law;
 - b. consensual monitoring of communications, even if a crime under state, local, or tribal law;
 - c. the controlled purchase, receipt, delivery, or sale of drugs, stolen property, or other contraband;
 - d. the payment of bribes;
 - e. the making of false representations in concealment of personal identity or the true ownership of a proprietary; and
 - f. conducting a money laundering transaction or transactions involving an aggregate amount not exceeding \$1 million.

UNCLASSIFIED - FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

Appendix E: Key Words, Definitions, and Links

Academic Nexus: [REDACTED]

[REDACTED]

b2
b7E

Aggrieved Person: [REDACTED]

[REDACTED]

b2
b7E

Assessments: The *Attorney General's Guidelines for Domestic FBI Operations* (AGG-Dom) combine "threat assessments" under the former *Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection* and the "prompt and extremely limited checking out of initial leads" under the former *Attorney General's Guidelines on General Crimes, Racketeering Enterprise and Terrorism Enterprise Investigations* into a new investigative category entitled "assessments." [REDACTED]

[REDACTED]

b2
b7E

[REDACTED] The FBI may also conduct assessments as part of its special events management responsibilities. (AGG-Dom, Part II)

Closed Circuit Television (CCTV): a fixed-location video camera that is typically concealed from view or that is placed on or operated by a consenting party.

Consensual Monitoring: Monitoring of communications for which a court order or warrant is not legally required because of the consent of a party to the communication.

Electronic Communication Service: Any service that provides to users thereof the ability to send or receive wire or electronic communications. For example, telephone companies and electronic mail companies generally act as providers of electronic communication services.

Electronic Communications System: Any wire, radio, electromagnetic, photooptical or photoelectronic facilities for the transmission of wire or electronic communications, and any

UNCLASSIFIED - FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

computer facilities or related electronic equipment for the electronic storage of such communications.

Electronic Storage: Any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof, or any storage of such communication by an electronic communication service for purposes of backup protection of such communication. In short, "electronic storage" refers only to temporary storage, made in the course of transmission, by a provider of an electronic communication service.

Electronic Tracking Device: Direction finder including electronic tracking devices, such as, radio frequency beacons and transmitters, vehicle locator units, and the various devices that use a Global Positioning System or other satellite system for monitoring non-communication activity.

Employee: An FBI employee or an employee of another agency working under the direction and control of the FBI.

Enterprise investigations are a type of full investigation and are subject to the same requirements that apply to full investigations described in Section 7. Enterprise investigations focus on groups or organizations that may be involved in the most serious criminal or national security threats to the public, as described in Section 8.5. Enterprise investigations cannot be conducted as preliminary investigations or assessments, nor may they be conducted for the sole purpose of collected foreign intelligence.

Enterprise Investigation: [REDACTED]

[REDACTED]
[REDACTED]

b2
b7E

FISA: The Foreign Intelligence Surveillance Act of 1978, as amended: The law establishes a process for obtaining judicial approval of electronic surveillance and physical searches for the purposes of collecting foreign intelligence. Orders for ELSUR surveillance are provided for the period of time not to exceed: 90 days for United States persons; 120 days for Non-United States persons; and one year for a foreign power. Renewal of FISA Orders may be requested for the same period of time originally authorized based upon a continued showing of probable cause. For Non-United States persons, renewals can be for a period not to exceed one year. [REDACTED]

b2
b7E

[REDACTED] at least 45 days prior to the expiration of the existing order.

UNCLASSIFIED - FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

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 control or policy direction; financial or material support; or leadership, assignments, or discipline.

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 United States-based computers.

Foreign Intelligence: Information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations or foreign persons, or international terrorists.

Foreign Intelligence Requirements:

5. National intelligence requirements issued pursuant to authorization by the Director of National Intelligence, including the National Intelligence Priorities Framework and the National HUMINT Collection Directives, or any successor directives thereto;
6. Requests to collect foreign intelligence by the President or by Intelligence Community officials designated by the President; and
7. Directions to collect foreign intelligence by the Attorney General, the Deputy Attorney General, or an official designated by the Attorney General.

Foreign Power: A foreign government or any component thereof, whether or not recognized by the United States; a faction of a foreign nation or nations, not substantially composed of United States persons; an entity that is openly acknowledged by a foreign government or governments to be directed and controlled by such foreign government or governments; a group engaged in international terrorism or activities in preparation therefore; a foreign-based political organization, not substantially composed of United States persons; or an entity that is directed or controlled by a foreign government or governments.

Full Investigation: A full investigation may be initiated if there is an articulable factual basis for the investigation that reasonably indicates that a circumstance described in paragraph 3.a.-b. exists or if a circumstance described in paragraph 3.c. exists. All lawful methods may be used in a full investigation.

A full investigation of a group or organization may be initiated as an enterprise investigation if there is an articulable factual basis for the investigation that reasonably indicates that the group or organization may have engaged or may be engaged in, or may have or may be engaged in planning or preparation or provision of support for:

1. a pattern of racketeering activity as defined in 18 U.S.C. § 1961(5);
2. international terrorism or other threat to the national security;
3. domestic terrorism as defined in 18 U.S.C. § 2331(5) involving a violation of federal criminal law;
4. furthering political or social goals wholly or in part through activities that involve force or violence and a violation of federal criminal law; or

UNCLASSIFIED - FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

5. an offense described in 18 U.S.C. §§ 2332b(g)(5)(B) or 18 U.S.C. § 43.

Human Source: A Confidential Human Source as defined in the Attorney General's Guidelines Regarding the Use of FBI Confidential Human Sources.

Intelligence Activities: Any activity conducted for intelligence purposes or to affect political or governmental processes by, for, or on behalf of a foreign power.

International Terrorism: Activities that involve violent acts or acts dangerous to human life that violate federal, state, local, or tribal criminal law or would violate such law if committed within the United States or a state, local, or tribal jurisdiction; 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 occur totally outside the United States, or transcend national boundaries in terms of the means by which they are accomplished, the persons they appear to be intended to coerce or intimidate, or the locale in which their perpetrators operate or seek asylum.

National Security Letters: an administrative demand for documents or records that can be made by the FBI during a predicated investigation relevant to a threat to national security. The standard for issuing an NSL, except under 15 U.S.C. § 1681v, is relevance to an authorized investigation to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a United States person is not predicated solely on activities protected by the First Amendment of the Constitution of the United States.

[Redacted]

b2
b7E

Pen Register Device: Records or decodes dialing, routing addressing or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided that such information must not include the contents of any communication.

Physical Surveillance: The deliberate observation by an FBI employee of persons, places, or events, on either a limited or continuous basis, in a public or a semi-public (e.g., commercial business open to the public) setting.

Preliminary Investigation: Preliminary investigations may be carried out to detect, obtain information about, or prevent or protect against federal crimes or threats to the national security.

[Redacted]

b2
b7E

[Redacted]

UNCLASSIFIED - FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

The investigation of threats to the national security may constitute an exercise of the FBI's criminal investigation authority as well as its authority to investigate threats to the national security. As with criminal investigations, detecting and solving crimes and arresting and prosecuting the perpetrators are likely objectives of investigations relating to threats to the national security. These investigations, however, serve important purposes outside the ambit of normal criminal investigations, by providing the basis for, and informing decisions concerning other measures needed to protect the national security.

Proprietary: A sole proprietorship, partnership, corporation, or other business entity operated on a commercial basis, which is owned, controlled, or operated wholly or in part on behalf of the FBI, and whose relationship with the FBI is concealed from third parties.

Provider of Electronic Communication Services: Any service that provides the user thereof the ability to send or receive wire or electronic communications.

Publicly Available: Information that has been published or broadcast for public consumption, is available on request to the public, is accessible on-line or otherwise to the public, is available to the public by subscription or purchase, could be seen or heard by any casual observer, is made available at a meeting open to the public, or is obtained by visiting any place or attending any event that is open to the public.

Records: Any records, databases, files, indices, information systems, or other retained information.

Remote Computing Services:

b2
b7E

Sensitive Investigative Matter: An investigative matter involving a domestic public official, political candidate, religious or political organization or 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.

Sensitive Circumstance:

Sensitive Monitoring Circumstance:

1. Investigation of a member of Congress, a federal judge, a member of the Executive Branch at Executive Level IV or above, or a person who has served in such capacity within the previous two years; (Note: Executive Levels I through IV are defined in 5 U.S.C. §§ 5312-5315.)
2. Investigation of the Governor, Lieutenant Governor, or Attorney General of any state or territory, or a judge or justice of the highest court of any state or territory, concerning an offense involving bribery, conflict of interest, or extortion related to the performance of official duties;
3. A party to the communication is in the custody of the Bureau of Prisons or the United States Marshals Service or is being or has been afforded protection in the Witness Security Program; or

UNCLASSIFIED - FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

4. The Attorney General, the Deputy Attorney General, or an Assistant Attorney General has requested that the FBI obtain prior approval for the use of consensual monitoring in a specific investigation.

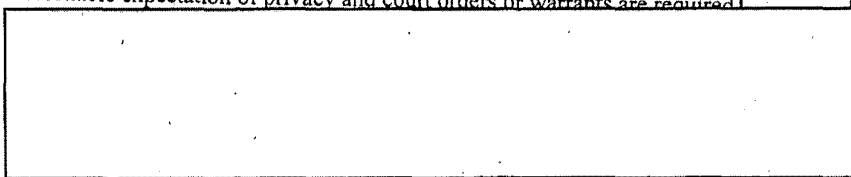
Special Agent in Charge: The Special Agent in Charge of an FBI Field Office (including an Acting Special Agent in Charge), except that the functions authorized for Special Agents in Charge by these Guidelines may also be exercised by the Assistant Director in Charge or by any Special Agent in Charge designated by the Assistant Director in Charge in an FBI Field Office headed by an Assistant Director, and by FBI Headquarters officials designated by the Director of the FBI.

Special Events Management: Planning and conduct of public events or activities whose character may make them attractive targets for terrorist attack.

State, Local, or Tribal: Any state or territory of the United States or political subdivision thereof, the District of Columbia, or Indian tribe.

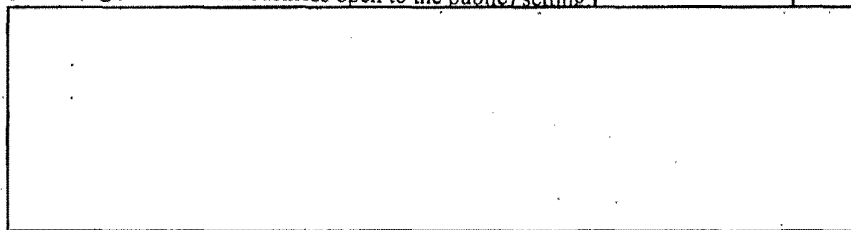
Surveillance:

1. Electronic surveillance (ELSUR) is the non-consensual electronic collection of information (usually communications) under circumstances in which the parties have a reasonable expectation of privacy and court orders or warrants are required. [REDACTED]



b2
b7E

2. Physical surveillance is the deliberate observation by an FBI employee or a CHS of persons, places, or events, on either a limited or continuous basis, in a public or a semi-public (e.g., commercial business open to the public) setting. [REDACTED]



b2
b7E

Threat to the National Security: International terrorism; espionage and other intelligence activities, sabotage, and assassination, conducted by, for, or on behalf of foreign powers, organizations, or persons; foreign computer intrusion; and other matters determined by the Attorney General, consistent with Executive Order 12333 or a successor order.

Trap and Trace Device: Captures the incoming electronic or other impulses that identify the originating number or other dialing, routing, addressing or signaling information reasonably

UNCLASSIFIED - FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

likely to identify the source of a wire or electronic communication, provided that such information does not include the contents of any communication.

Undercover Activity: Any investigative activity involving the use of an assumed identity by an undercover employee for an official purpose, investigative activity, or function.

Undercover Employee: An employee of the FBI, another federal, state, or local law enforcement agency, another entity of the United States Intelligence Community, or another foreign intelligence agency working under the direction and control of the FBI whose relationship with the FBI is concealed from third parties by the maintenance of a cover or alias identity for an official purpose, investigative activity, or function.

Undercover Operation:

b2
b7E

United States: When used in a geographic sense, means all areas under the territorial sovereignty of the United States.

United States Person: Any of the following, but not including any association or corporation that is a foreign power as defined in Subpart G.1.-3.:

1. An individual who is a United States citizen or an alien lawfully admitted for permanent residence;
2. An unincorporated association substantially composed of individuals who are United States persons; or
3. A corporation incorporated in the United States.

In applying paragraph 2., if a group or organization in the United States that is affiliated with a foreign-based international organization operates directly under the control of the international organization and has no independent program or activities in the United States, the membership of the entire international organization shall be considered in determining whether it is substantially composed of United States persons. If, however, the United States-based group or organization has programs or activities separate from, or in addition to, those directed by the international organization, only its membership in the United States shall be considered in determining whether it is substantially composed of United States persons. A classified directive provides further guidance concerning the determination of United States person status.

Use: When used with respect to human sources, means obtaining information from, tasking, or otherwise operating such sources.

UNCLASSIFIED - FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

Appendix F: Acronyms

ACS	Automated Case Support
AD	Assistant Director
ADIC	Assistant Director in Charge
AFID	Alias False Identification
AG	Attorney General
AGG	Attorney General Guidelines
AGG-CHS	The Attorney General's Guidelines Regarding the Use of FBI Confidential Human Sources
AGG-Dom	The Attorney General's Guidelines for Domestic FBI Operations
AGG-Ext	The Attorney General's Guidelines for Extraterritorial FBI Operations
AGG-UCO	The Attorney General's Guidelines on FBI Undercover Operations
AOR	Area of Responsibility
ASAC	Assistant Special Agent in Charge
ATF	Bureau of Alcohol, Tobacco, Firearms and Explosives
AUSA	Assistant United States Attorney
BOP	Bureau of Prisons
BSA	Bank Secrecy Act
CALEA	Communications Assistance for Law Enforcement Act
CAU	Communications Analysis Unit
CCTV	Closed Circuit Television
CD	Counterintelligence Division
CDC	Chief Division Counsel
C.F.R.	Code of Federal Regulations
CHS	Confidential Human Source
CHSPM	Confidential Human Source Policy Manual

UNCLASSIFIED - FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

CHSVSM	Confidential Human Source Validation Source Manual
CIA	Central Intelligence Agency
CID	Criminal Investigative Division
CLEA	Criminal Law Enforcement Application
CMS	Collection Management Section
CPO	Corporate Policy Office
CSO	Chief Security Officer
CTD	Counterterrorism Division
CUORC	Criminal Undercover Operations Review Committee
CW	Cooperative Witness
DAD	Deputy Assistant Director
DAG	Deputy Attorney General
D.C.	District of Columbia
DCO	Division Compliance Officer
D.D.C.	Department Document Committee
DI	Directorate of Intelligence
DIOG	Domestic Investigations Operations Guide
DMS	Domain Management Section
DNI	Director of National Intelligence
DOD	Department of Defense
DOJ	Department of Justice
DOS	Department of State
EA	Emergency Authority
EAD	Executive Assistant Director
EC	Electronic Communication
ECPA	Electronic Communication Privacy Act

UNCLASSIFIED - FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

ECS	Electronic Communication Service
ELSUR	Electronic Surveillance
EO	Executive Order
ERS	ELSUR Records System
ESN	Electronic Serial Number
ESU	Electronic Surveillance Unit
FAA	Federal Aviation Administration
FBI	Federal Bureau of Investigation
FBIHQ	FBI Headquarters
FBINET	FBI Network
FCC	Federal Communications Commission
FCRA	Fair Credit Reporting Act
FGJ	Federal Grand Jury
FGUSO	Field Guide for Undercover and Sensitive Operations
FI	Foreign Intelligence
FI	Full Investigation
FICP	Foreign Intelligence Collection Program
FIG	Field Intelligence Group
FISA	Foreign Intelligence Surveillance Act
FISAMS	FISA Management System
FISC	Foreign Intelligence Surveillance Court
<input type="text"/>	<input type="text"/>
FRCP	Federal Rules of Criminal Procedure
FYI	For Your Information
<input type="text"/>	<input type="text"/>
GPS	Global Positioning System

b2
b7E

b2
b7E

UNCLASSIFIED - FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

GC	General Counsel
HIMU	Human Intelligence Management Unit
HR	House of Representatives
HSC	Homeland Security Council
HSPD	Homeland Security Presidential Directive
HUMINT	Human Intelligence
IA	Intelligence Analyst
ICE	Bureau of Immigration and Customs Enforcement
ICI	Intranet to Counterintelligence
INI	Innocent Images National Initiative
IIR	Intelligence Information Reports
ILB	Investigative Law Branch
ILU	Investigative Law Unit
INTERPOL	International Criminal Police Organization
IOB	Intelligence Oversight Board
IP	Internet Protocol
IT	International Terrorism
Legat	Legal Attaché
LHM	Letterhead Memorandum
MAOP	Manual of Administrative Operations and Procedures
MAR	Monthly Administrative Report
MIOG	Manual of Investigative Operations and Guidelines
MLAT	Mutual Legal Assistance Treaties
MOA	Memorandum of Agreement
MSIN	Mobile Station Identification Number
MOU	Memorandum of Understanding

UNCLASSIFIED - FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

NAFTA	North American Free Trade Association
NARA	National Archives and Records Administration
NATO	North Atlantic Treaty Agreement
NCTAUS	National Commission on Terrorist Attacks upon the United States
NCTC	National Counterterrorism Center
NCMEC	National Center for Missing & Exploited Children
NFIPM	National Foreign Intelligence Program Manual
NFPO	No Foreign Policy Objection
NHCD	National HUMINT Collection Directives
NIPF	National Intelligence Priorities Framework
NISS	National Information Sharing Strategy
NSB	National Security Branch
NSC	National Security Council
NSD	National Security Division, DOJ
NSL	National Security Letter
NSLB	National Security Law Branch
NSPD	National Security Presidential Directive
NSSE	National Special Security Events
OCA	Office of Congressional Affairs
OEO	Office of Enforcement Operations
OGC	Office of the General Counsel
OI	Office of Intelligence, DOJ NSD
OIA	Otherwise Illegal Activity
OIC	Office of Integrity and Compliance
OIO	Office of International Operations
OMB	Office of Management and Budget

UNCLASSIFIED - FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

OO	Office of Origin
OTD	Operational Technology Division
PCLU	Privacy and Civil Liberties Unit
PCTDD	Post Cut-Through Dialed Digits
PD	Presidential Directive
PDD	Presidential Decision Directive
PI	Preliminary Investigation
PIA	Privacy Impact Assessment
PG	Policy-Implementation Guide
PIOB	Potential Intelligence Oversight Board
P.L.	Public Law
PR	Pen Register
PR/TT	Pen Register/Trap and Trace
RCS	Remote Computing Service
RF	Radio Frequency
RFPA	Right to Financial Privacy Act
RICO	Racketeer Influenced and Corrupt Organizations
RMD	Records Management Division
ROCU	Requirements Oversight and Coordination Unit
SA	Special Agent
SAC	Special Agent in Charge
SBP	Subpoena Sub-file
SC	Section Chief
SCI	Sensitive Compartmentalized Information
SCION	Sensitive Compartmentalized Information Operational Network
SIA	Supervisory Intelligence Analyst

UNCLASSIFIED - FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

SMTJ	Special Maritime and Territorial Jurisdiction
SOG	Special Operations Group
SORC	Sensitive Operations Review Committee
SPM	Security Program Manager
SSA	Supervisory Special Agent
SSG	Special Surveillance Group
SSRA	Supervisory Senior Resident Agent
TA	Technical Advisor
TFO	Task Force Officer
TMD	Technical Management Database
TS	Top Secret
TT	Trap and Trace
TTA	Technically Trained Agent
UACB	Unless Advised Contrary by Bureau
UC	Undercover
U.C.	Unit Chief
UCE	Undercover Employee
UCFN	Universal Case File Number
UCO	Undercover Operations
UCRC	Undercover Review Committee
UDP	Undisclosed Participation
USAO	United States Attorney's Office
U.S.C.	United States Code
USIC	United States Intelligence Community
USMS	United States Marshals Service
USP	US Person

F-7

FOR OFFICIAL USE ONLY

ACLU EC-103

UNCLASSIFIED - FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

USPER	US Person
USPS	United States Postal Service
USSS	United States Secret Service
WITT	Wireless Intercept Tracking Technology
WMD	Weapons of Mass Destruction