

UNCLASSIFIED - FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

10. (U) Sensitive Investigative Matter / Academic Nexus

10.1. (U) Overview

(U) Certain investigative matters should be brought to the attention of FBI management and DOJ officials because of the possibility of public notoriety and sensitivity. Accordingly, assessments and predicated investigations involving "sensitive investigative matters" have special approval and reporting requirements.

10.2. (U) Purpose, Scope and Definitions

(U//FOUO) A sensitive investigative matter is defined as an investigative matter involving the activities of a domestic public official or political candidate (involving corruption or a threat to the national security), 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 DOJ officials. (AGG-Dom, Part VII.N.) As a matter of FBI policy, "judgment" means that the decision of the authorizing official is discretionary. Descriptions for each of the officials and entities contained in the sensitive investigative matter definition are as follows:

- A. (U//FOUO) **Domestic Public Official**—A domestic public official is an individual elected or appointed to a position of trust in a federal, state, local or tribal governmental entity or political subdivision thereof. A matter involving a domestic public official is a "sensitive investigative matter" if the assessment or predicated investigation involves corruption or a threat to the national security.
- B. (U//FOUO) **Political candidate**—A political candidate is an individual who is seeking election to, or nomination for election to, or who has authorized others to explore on his or her behalf the possibility of election to, an office in a federal, state, local or tribal governmental entity or political subdivision thereof. As with domestic public officials, a matter involving a political candidate is a sensitive investigative matter if the assessment or predicated investigation involves corruption or a threat to the national security.
- C. (U//FOUO) **Political organization or individual prominent in such an organization**—

- D. (U//FOUO) **Religious organization or individual prominent in such an organization**—

b2
b7E

UNCLASSIFIED - FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

E. (U//FOUO) Member of the media or a news organization—

[Redacted]

F. (U//FOUO) Academic Nexus—

[Redacted]

b2
b7E

(U//FOUO) The sensitivity related to an academic institution arises from the American tradition of "academic freedom" (e.g., an atmosphere in which students and faculty are free to express unorthodox ideas and views and to challenge conventional thought without fear of repercussion). Academic freedom does not mean, however, that academic institutions are off limits to FBI investigators in pursuit of information or individuals of legitimate investigative interest.

(U//FOUO)

[Redacted] see the classified appendix.

- G. (U//FOUO) Other Matters—**Any matter that in the judgment of the official authorizing an investigation that should be brought to the attention of FBIHQ and other Department of Justice officials. As a matter of FBI policy, "judgment" means that the decision of the authorizing official is discretionary.

10.3. (U//FOUO) Factors to Consider When Initiating or Approving an Investigative Activity Involving a Sensitive Investigative Matter

(U//FOUO) In addition to the standards for approving investigative activity in Sections 5, 6, 7 and 9, the following factors should be considered by the: (i) FBI employee who seeks to initiate an assessment or predicated investigation involving a sensitive investigative matter; (ii) CDC or OGC when reviewing such matters; and (iii) approving official in determining whether the assessment or predicated investigation involving a sensitive investigative matter should be authorized:

- A. (U//FOUO) Seriousness/severity of the violation/threat;
- B. (U//FOUO) Significance of the information sought to the violation/threat;
- C. (U//FOUO) Probability that the proposed course of action will be successful;
- D. (U//FOUO) Risk of public exposure, and if there is such a risk, the adverse impact or the perception of the adverse impact on civil liberties and public confidence; and
- E. (U//FOUO) Risk to the national security or the public welfare if the proposed course of action is not approved (i.e., risk of doing nothing).

(U//FOUO) In the context of a sensitive investigative matter, particular care should be taken when considering whether the planned course of action is the least intrusive method feasible.

UNCLASSIFIED - FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

10.4. (U) Duration, Approval, Notice and Documentation

(U//FOUO) The following are required approval and notification levels for investigative activities involving sensitive investigative matters:

A. (U//FOUO) Initiated by a Field Office:

(U//FOUO) **Assessment:** An FBI employee may initiate assessment type one and two activities, as described in Section 5.6.A.1 and 2 (prompt checking of leads), without prior supervisory approval. However, because assessments involving sensitive investigative matters must be brought to the attention of FBI Field Office management, CDC review and SAC approval to continue the assessment must be acquired as soon as practicable. For assessment types 3, 4 and 6 assessments (see DIOG Section 5.6.A.3, 4 and 6) involving a sensitive investigative matter, prior CDC review and SAC approval is required. For assessment types 3, 4, and 6, as described in Section 5.6.A.3, 4 and 6, if a sensitive investigative matter arises after the initiation of an assessment, investigative activity must cease until CDC review and SAC approval is acquired.

(U//FOUO) Assessments involving a sensitive investigative matter do not require notification to DOJ or the United States Attorney. (AGG-Dom, Part II.B.5.a) All positive foreign intelligence collection assessments, regardless of whether they involve a sensitive investigative matter, require prior FBIHQ CMS approval. If a sensitive investigative matter arises after the initiation of a positive foreign intelligence collection assessment, notice must be provided to FBIHQ CMS.

(U//FOUO) **Predicated Investigation:** For all predicated investigations involving a sensitive investigative matter, prior CDC review and SAC approval is required, and the Field Office must provide written notification to the appropriate FBIHQ Unit Chief and Section Chief. Additionally, the Field Office must provide written notification to the United States Attorney or the appropriate FBIHQ Section must provide written notification to the DOJ Criminal Division or NSD, as soon as practicable, but no later than 30 calendar days after initiation of the predicated investigation. The notice must identify [redacted]

b2
b7E

[redacted] (see classified appendix for [redacted])
[redacted]

(U//FOUO) If a sensitive investigative matter arises after the initiation of a predicated investigation, investigative activity must cease until CDC review and SAC approval is acquired and notice is furnished to the FBIHQ Unit and Section as specified above.

B. (U//FOUO) Initiated by FBIHQ:

(U//FOUO) **Assessment:** For assessment types 3, 4 and 6, as described in Section 5.6.A.3, 4 and 6, involving a sensitive investigative matter, OGC review and Section Chief approval is required. If a sensitive investigative matter arises after the initiation of an assessment, investigative activity must cease until OGC review and Section Chief approval is acquired.

(U//FOUO) Assessments involving a sensitive investigative matter do not require notification to DOJ or the United States Attorney. (AGG-Dom, Part II.B.5.a) All positive foreign intelligence collection assessments, regardless of whether they involve a sensitive investigative matter, require prior FBIHQ CMS approval. If a sensitive investigative matter arises after the initiation of a positive foreign intelligence collection assessment, notice must be provided to FBIHQ CMS.

UNCLASSIFIED - FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

(U//FOUO) **Predicated Investigation:** For predicated investigations involving a sensitive investigative matter, OGC review, Section Chief approval, and written notification to the United States Attorney, DOJ Criminal Division or DOJ NSD is required, as soon as practicable, but no later than 30 calendar days after the initiation of such an investigation.

b2
b7E

The notice must identify [redacted]

(see classified appendix [redacted])

(U//FOUO) If a sensitive investigative matter arises after the initiation of a predicated investigation, investigative activity must cease until OGC review and Section Chief approval is acquired and notice is furnished as specified above.

10.5. (U//FOUO) Distinction Between Sensitive Investigative Matter and Sensitive Circumstance

(U//FOUO) The term "sensitive investigative matter" should not be confused with the term "sensitive circumstance" as that term is used in undercover operations. A "sensitive circumstance" relates to an undercover operation requiring FBIHQ approval. A comprehensive list of sensitive circumstances for criminal activities is contained in the Attorney General's Guidelines on FBI Undercover Operations and in Section 11 of the DIOG for national security matters. The Criminal Undercover Operations Review Committee (CUORC) and [redacted] must review and approve undercover operations that involve sensitive circumstances. The detailed policy for undercover operations is described in DIOG Section 11.8, the Field Guide for Undercover and Sensitive Operations (FGUSO), and the FBIHQ substantive Division program implementation guides.

b2
b7E

10.6. (U//FOUO) Sensitive Operations Review Committee

(U//FOUO) [redacted]

b5

UNCLASSIFIED - FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

11. (U) Investigative Methods

11.1. (U) Overview

(U//FOUO) The conduct of assessments, predicated investigations and other activities authorized by the AGG-Dom may present choices between the use of different investigative methods (formerly investigative "techniques") that are each operationally sound and effective, but that are more or less intrusive, considering such factors as the effect on the privacy and civil liberties of individuals and the potential damage to reputation. The least intrusive method feasible is to be used in such situations. However, the choice of methods is a matter of judgment. The FBI is authorized to use any lawful method consistent with the AGG-Dom, even if intrusive, where the degree of intrusiveness is warranted in light of the seriousness of a criminal or national security threat or the strength of the information indicating its existence, or in light of the importance of foreign intelligence sought to the United States' interests. (AGG-Dom, Part I.C.2.)

(U) The availability of a particular investigative method in a particular case may depend upon the level of investigative activity (assessment, preliminary investigation, full investigation, assistance to other agencies).

11.1.1. (U) Least Intrusive Method

(U) The AGG-Dom requires that the "least intrusive" means or method be considered and—if operationally sound and effective—used to obtain intelligence or evidence in lieu of more intrusive methods. This principle is also reflected in Executive Order 12333, which governs the activities of the United States intelligence community. The concept of least intrusive method applies to the collection of intelligence and evidence.

(U) Selection of the least intrusive means is a balancing test as to which FBI employees must use common sense and sound judgment to effectively execute their duties while mitigating the potential negative impact on the privacy and civil liberties of all people encompassed within the assessment or predicated investigation, including targets, witnesses, and victims. This principle is not intended to discourage investigators from seeking relevant and necessary intelligence, information, or evidence, but rather is intended to encourage investigators to choose the least intrusive—yet still effective—means from the available options to obtain the material. Additionally, FBI employees should operate openly and consensually with United States persons to the extent practicable when collecting foreign intelligence that does not concern criminal activities or threats to the national security.

(U) Section 4.4 describes the least intrusive methods concept and the standards to be applied by FBI employees.

UNCLASSIFIED - FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

11.2. (U) Authorized Investigative Methods in Assessments and Predicated Investigations

(U) The below listed investigative methods may be used in assessments and predicated investigations. The use and/or dissemination of information obtained by the use of all authorized investigative methods must comply with the AGG-Dom and DIOG Section 14.

11.2.1. (U) Authorized Investigative Methods in Assessments

(AGG-Dom, Part II.A.4.)

(U//FOUO) An FBI employee must document on the FD-71, or in Guardian, the use of or the request and approval for the use of authorized investigative methods in type 1 and 2 assessments (see DIOG Section 5.6.A.1 and 2). By exception, certain assessment type 1 and 2 situations may require the use of an EC to document the use and approval of certain investigative methods. All authorized investigative methods in type 3, 4, and 6 assessments (see DIOG Section 5.6.A.3, 4 and 6) must use an EC to document the use of or the request and approval for the use of the applicable investigative method. For a detailed description of these methods see DIOG Section 5.9.

- A. (U) Obtain publicly available information.
- B. (U) Access and examine FBI and other Department of Justice records, and obtain information from any FBI or other Department of Justice personnel.
- C. (U) Access and examine records maintained by, and request information from, other federal, state, local, or tribal, or foreign governmental entities or agencies.
- D. (U) Use online services and resources (whether non-profit or commercial).
- E. (U) Use and recruit human sources in conformity with the Attorney General's Guidelines Regarding the Use of FBI Confidential Human Sources.
- F. (U) Interview or request information from members of the public and private entities.
- G. (U) Accept information voluntarily provided by governmental or private entities.
- H. (U) Engage in observation and conduct physical surveillance not requiring a court order.
- I. (U//FOUO) Grand jury subpoenas for telephone or electronic mail subscriber information during type 1 and 2 assessments.

(U//FOUO) **Note:** In assessments, supervisory approval is required prior to use of the following investigative methods: certain interviews, tasking of a CHS, and physical surveillance not requiring a court order. During predicated investigations the supervisory approval requirements for these investigative methods may not apply.

11.2.2. (U) Authorized Investigative Methods in Preliminary Investigations

(AGG-Dom, Part V.A.1-10)

(U) In preliminary investigations the authorized methods include the following: [AGG-Dom, Part II.B. and Part V.A.]

- A. (U) The investigative methods approved for assessments.
- B. (U) Mail covers.

UNCLASSIFIED - FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

- C. (U) 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).
- D. (U) Consensual monitoring of communications, including consensual computer monitoring, subject to legal review by the CDC or the OGC. When a sensitive monitoring circumstance is involved, the monitoring must be approved by the DOJ Criminal Division or, if the investigation concerns a threat to the national security or foreign intelligence, by the DOJ National Security Division.
- (U//FOUO) **Note:** For additional information, see the classified appendix.
- (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 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.
- E. (U) Use of closed-circuit television, direction finders, and other monitoring devices, subject to legal review by the CDC or the OGC. (The methods described in this paragraph usually do not require court orders or warrants unless they involve an intrusion into an area where there is a reasonable expectation of privacy or non-consensual monitoring of communications, but legal review is necessary to ensure compliance with all applicable legal requirements.)
- F. (U) Polygraph examinations.
- G. (U) 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 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 DOJ National Security Division in the review process.
- H. (U) 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 FISA orders [50 U.S.C. §§ 1861-63]).
- I. (U) 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).
- J. (U) 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 FISA (50 U.S.C. §§ 1841-1846).

11.2.3. (U) Authorized Investigative Methods in Full Investigations

(AGG-Dom, Part V.A.11-13)

(U) In full investigations, to include enterprise investigations, all investigative methods approved for assessments and preliminary investigations may be used. In addition, the three investigative methods listed below may only be used in full investigations:

UNCLASSIFIED - FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

- A. (U) Electronic surveillance in conformity with chapter 119 of title 18, United States Code (18 U.S.C. §§ 2510-2522), or the Foreign Intelligence Surveillance Act, or Executive Order 12333 § 2.5.
- B. (U//FOUO) 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. **Note:** For additional information regarding certain searches, see the classified appendix.
- C. (U) Acquisition of foreign intelligence information in conformity with Title VII of the FISA.
(U//FOUO) **Note:** Not all investigative methods are authorized while collecting foreign intelligence as part of a full investigation. See DIOG Section 9 for more information.

11.2.4. (U) Particular Investigative Methods

(U//FOUO) All lawful investigative methods may be used in activities under the AGG-Dom as authorized by the AGG-Dom. Authorized methods include, but are not limited to, those identified in the rest of this section. In some instances they are subject to special restrictions or review or approval requirements. (AGG-Dom, Part V.A.)

UNCLASSIFIED - FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

11.3. (U) Investigative Method: Mail Covers

11.3.1. (U) Summary

(U) A mail cover may be sought only in a predicated investigation when there exists reasonable grounds to demonstrate that the mail cover is necessary to: (i) protect the national security; (ii) locate a fugitive; (iii) obtain evidence of the commission or attempted commission of a federal crime; or (iv) assist in the identification of property, proceeds or assets forfeitable because of a violation of criminal law. 39 C.F.R. § 233.3(e)(2).

(U//FOUO) [REDACTED]

b2
b7E

(U) [REDACTED]

b2
b7E

As a general rule, a mail cover in the APO/FPO system overseas may only be ordered by a military authority competent to order searches and seizures for law enforcement purposes, usually a commanding officer. See DoD 4525.6-M, the DoD Postal Manual.

(U//FOUO) Application: [REDACTED]

b2
b7E

11.3.2. (U) Legal Authority

- A. (U) Postal Service Regulation 39 C.F.R. § 233.3 is the sole authority and procedure for initiating a mail cover and for processing, using and disclosing information obtained from a mail cover;
- B. (U) There is no Fourth Amendment protection for information on the outside of a piece of mail. See, e.g., U.S. v. Choate, 576 F.2d 165, 174 (9th Cir., 1978); and U.S. v. Huie, 593 F.2d 14 (5th Cir., 1979); and
- C. (U) AGG-Dom, Part V.A.2.

11.3.3. (U) Definition of Investigative Method

(U) A mail cover is the non-consensual recording of any data appearing on the outside cover of any sealed or unsealed mail matter to obtain information in order to:

- A. (U) Protect the national security;
- B. (U) Locate a fugitive;
- C. (U) Obtain evidence of commission or attempted commission of a federal crime;
- D. (U) Obtain evidence of a violation or attempted violation of a postal statute; or
- E. (U) Assist in the identification of property, proceeds or assets forfeitable under law. 39 C.F.R. § 233.3(c) (1).

UNCLASSIFIED - FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

(U) In this context, a "recording" means the transcription, photograph, photocopy, or other facsimile of the image of the outside cover, envelope, or wrappers of mailed matter. A warrant or court order is almost always required to obtain the contents of any class of mail, sealed or unsealed.

11.3.4. (U) Standard for Use and Approval Requirements for Investigative Method

(U) The standard to obtain a mail cover is established by the Postal Service regulation. The Chief Postal Inspector may order a mail cover "[w]hen a written request is received from any law enforcement agency in which the requesting authority specifies the reasonable grounds to demonstrate the mail cover is necessary to:

- (U) Protect the national security;
- (U) Locate a fugitive;
- (U) Obtain information regarding the commission or attempted commission of a crime; or
- (U) Assist in the identification of property, proceeds or assets forfeitable because of a violation of criminal law." 29 C.F.R. § 233.3(e)(2).

(U//FOUO) **National Security Mail Cover:** A national security mail cover request must be approved by the Director or designee, currently only the EAD of the National Security Branch. All requests for national security mail covers must be reviewed by the Field Office SSA according to the below-criteria. A national security mail cover sought "to protect the national security" includes protecting the United States from actual or threatened attack or other grave, hostile act; sabotage; international terrorism; or clandestine intelligence activities, including commercial [economic] espionage by foreign powers or their agents.

(U//FOUO) After being approved by the SSA, the Field Office must transmit the mail cover letter request by EC, with the draft letter as an attachment, to the National Security Law Branch (NSLB) for legal review and concurrence. Upon review and concurrence, the NSLB must transmit the letter request for signature approval to the EAD, National Security Branch, or, in his or her absence, to the Director.

(U//FOUO) **Criminal Mail Cover:** A criminal mail cover request may be approved by the Field Office SSA. The SSA may approve a request for a mail cover if there are reasonable grounds to demonstrate that the mail cover is necessary to assist in efforts to: (i) locate a fugitive; (ii) obtain information regarding the commission or attempted commission of a federal crime; or (iii) to assist in the identification of property, proceeds or assets forfeitable because of a violation of criminal law.

(U//FOUO) **SSA review and or approval of a national security or criminal mail cover request:** Approval of any mail cover request or an extension is conditioned on the following criteria being met:

A. (U//FOUO) [REDACTED]

b2
b7E

UNCLASSIFIED - FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

B. (U//FOUO) [REDACTED]
[REDACTED] b2
b7E

C. (U//FOUO) [REDACTED]
[REDACTED] b2
b7E

D. (U//FOUO) [REDACTED]
[REDACTED] b2
b7E

E. (U//FOUO) [REDACTED]
[REDACTED] b2
b7E

F. (U//FOUO) [REDACTED]
[REDACTED] (Note:
Under postal regulations, a mail cover must not include matter mailed between the mail
cover subject and the subject's attorney, unless the attorney is also a subject under the
investigation.) b2
b7E

G. (U//FOUO) [REDACTED]
[REDACTED] b2
b7E

H. (U//FOUO) [REDACTED]
[REDACTED] b2
b7E

I. (U//FOUO) [REDACTED]
[REDACTED] b2
b7E

(U) **Emergency Requests:** When time is of the essence, the Chief Postal Inspector, or
designee, may act upon an oral request to be confirmed by the requesting authority, in
writing, within three calendar days. Information may be released prior to receipt of the

UNCLASSIFIED - FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

written request only when the releasing official is satisfied that an emergency situation exists. 39 C.F.R. § 233.3(e)(3).

(U) An "emergency situation" exists when the immediate release of information is required to prevent the loss of evidence or when there is a potential for immediate physical harm to persons or property. 39 C.F.R. § 233.3(c)(10).

11.3.5. (U) Duration of Approval

- A. (U) **National Security:** A national security mail cover is limited to 120 days from the date the mail cover is initiated. Extensions can only be authorized by the Chief Postal Inspector or his designee at the National Headquarters of the Office of the Chief Postal Inspector. 39 C.F.R. § 233.3(g)(6).
- B. (U) **Criminal mail covers except fugitives:** A mail cover in a criminal case is limited to no more than 30 days, unless adequate justification is provided by the requesting authority. 39 C.F.R. § 233.3(g)(5). Renewals may be granted for additional 30-day periods under the same conditions and procedures applicable to the original request. The requesting authority must provide a statement of the investigative benefit of the mail cover and anticipated benefits to be derived from the extension.
- C. (U) **Fugitives:** No mail cover instituted to locate a fugitive may remain in force for longer than 120 continuous days unless personally approved for further extension by the Chief Postal Inspector or his/her designees at National Headquarters. 39 C.F.R. § 233.3(g)(6).
- D. (U) **Exception for Indictments:** Except for fugitive cases, no mail cover may remain in force when an information has been filed or the subject has been indicted for the matter for which the mail cover has been requested. If the subject is under investigation for further criminal violations, or a mail cover is required to assist in the identification of property, proceeds or assets forfeitable because of a violation of criminal law, a new mail cover order must be requested. 39 C.F.R. § 233.3(g)(7).

11.3.6. (U) Specific Procedures

(U//FOUO) The Postal Regulation requires that physical storage of all reports issued pursuant to a mail cover request to be at the discretion of the Chief Postal Inspector. 39 C.F.R. § 233.3(h)(1). Accordingly, FBI employees must conduct a timely review of mail cover documents received from the USPS. A copy of the signed mail cover request and the signed transmittal letter must be maintained in the investigative case file.

(U//FOUO)

b2
b7E

11.3.7. (U) Compliance and Monitoring

(U//FOUO) FBI employees must conduct a timely review of mail cover information received from the USPS for any potential production of data beyond the scope of the requested mail cover ("overproduction") and either destroy or return the overproduction to the assigned USPS representative noting the reason for the return.

UNCLASSIFIED - FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

11.4. (U) Investigative Method: 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., [redacted])

b2
b7E

11.4.1. (U) Summary

(U//FOUO) Application: In predicated investigations, the FBI may conduct 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 [redacted]

b2
b7E

[redacted] not otherwise prohibited by AGG-Dom, Part

III.B.2-3. [redacted]

11.4.2. (U) Legal Authority

A. (U) AGG-Dom, Part V.A.3,

B. (U) Fourth Amendment to the United States Constitution

11.4.3. (U) Definition of Investigative Method

(U) The Fourth Amendment to the United States Constitution prevents the FBI from conducting unreasonable searches and seizures. It also generally requires a warrant be obtained if the search will intrude on a reasonable expectation of privacy. To qualify as a "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. If an individual has a reasonable expectation of privacy, a warrant or order issued by a court of competent jurisdiction or an exception to the requirement for such a warrant or order is required before a search may be conducted. Physical searches of personal or real property may be conducted without a search warrant or court order if there is no reasonable expectation of privacy in the property or area. As a general matter, there is no reasonable expectation of privacy in areas that are exposed to public view or that are otherwise available to the public. A reasonable expectation of privacy may be terminated by an individual abandoning property, setting trash at the edge of the curtilage or beyond for collection, or when a private party reveals the contents of a package.

(U) Examples of Searches not Requiring a Warrant because there is no Reasonable Expectation of Privacy: (i) Vehicle identification numbers or personal property that is exposed to public view and may be seen when looking through the window of a car that is parked in an area that is open to and accessible by members of the public; (ii) neither the examination of books and magazines in a book store nor the purchase of such items is a search or seizure under the Fourth Amendment. See Maryland v. Macon, 472 U.S. 463 (1985); and (iii) a deliberate overflight in navigable air space to photograph marijuana plants is not a search, despite the landowners subjective expectation of privacy. See California v. Ciraolo, 476 U.S. 207 (1986).

(U) Whether an area is curtilage is determined by reference to four factors: (i) proximity of the area in question to the home; (ii) whether the area is within an enclosure surrounding the home; (iii) nature of the use to which the area is put; and (iv) steps taken to protect the area from observation by passers-by.

UNCLASSIFIED - FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

(U) An area is curtilage if it "is so intimately tied to the home itself that it should be placed under the home's 'umbrella' of Fourth Amendment protection."

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

(U//FOUO) No supervisory approval is required for the use of this method. However, if there is a doubt as to whether a person has a reasonable expectation of privacy in the area to be searched, consult with the CDC or FBI Office of the General Counsel to determine whether a search warrant is required. Use of this method must be documented in the case file.

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)

(2) (U//FOUO)

[REDACTED]

b2
b7E

UNCLASSIFIED - FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

- (3) (U//FOUO) [redacted]
[redacted]
- (4) (U//FOUO) [redacted]
[redacted]
- (5) (U//FOUO) [redacted]
- (6) (U//FOUO) [redacted]
[redacted]
- (7) (U//FOUO) [redacted]
- (8) (U//FOUO) [redacted]
[redacted]
- (9) (U//FOUO) [redacted]
[redacted]
- (10) (U//FOUO) [redacted]
[redacted]
- (11) (U//FOUO) [redacted]
- (12) (U//FOUO) [redacted]
- (13) (U//FOUO) [redacted]
[redacted]
- (14) (U//FOUO) [redacted]
[redacted]
- (15) (U//FOUO) [redacted]
- (16) (U//FOUO) [redacted]
[redacted]
- (17) (U//FOUO) [redacted]
[redacted]
- (U//FOUO) [redacted]
[redacted]
- (1) (U//FOUO) [redacted]
[redacted]
- (2) (U//FOUO) [redacted]
[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

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

11.6. (U) Investigative Method: Use of closed-circuit television, direction finders, and other monitoring devices (Not needing a Court Order)

(U) Note: Use of this method is subject to legal review by the CDC or OGC.

11.6.1. (U) Summary

(U//FOUO) [REDACTED]

b2
b7E

(U//FOUO) Application: [REDACTED]
[REDACTED] not otherwise prohibited by AGG-Dom, Part III.B.2-3.
[REDACTED]

b2
b7E

11.6.2. (U) Legal Authority

- A. (U) AGG-Dom, Part V
- B. (U) Tracking devices use (18 U.S.C. § 2510[12] [C])
- C. (U) Rule 41 Federal Rules of Criminal Procedure
- D. (U) Fourth Amendment to the United States Constitution

11.6.3. (U//FOUO) Definition of Investigative Method

A. (U//FOUO) 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.

B. (U//FOUO) Electronic Tracking Devices: [REDACTED]

b2
b7E

[REDACTED] Electronic tracking devices are specifically excluded from Title III requirements (18 U.S.C. § 2510[12] [C]). In circumstances where a court order is required (pursuant to FRCP Rule 41[e][2][B]), a judge or magistrate may authorize the use of an electronic tracking device within the jurisdiction of the court and outside that jurisdiction, if the device is installed in that jurisdiction. (FRCP Rule 41 b[4]; 18 U.S.C. § 3117.)

C. (U//FOUO) [REDACTED]

b2
b7E

UNCLASSIFIED - FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

(U//FOUO)

b2
b7E

An example would be using thermal-imaging to detect heat emanating from within a home to make inferences about the use of high-powered marijuana-growing lamps inside the home (Kyllo v. United States, 533 U.S. 27 (2001)).

(U) Whether an area is curtilage is determined by reference to four factors: (i) proximity of the area in question to the home; (ii) whether the area is within an enclosure surrounding the home; (iii) nature of the use to which the area is put; and (iv) steps taken to protect the area from observation by passers-by.

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

(U//FOUO) When a video camera is physically operated as a hand-held video and is being used in an area in which no one has a reasonable expectation of privacy, its use is equivalent to using a still camera and does not require supervisory approval.

(U//FOUO) For those situations that require SSA approval for the use of CCTV, tracking devices, and other monitoring devices, SSA approval, which should be documented using the FD-759, may be granted if the following criteria have been met:

- A. (U//FOUO) Legal review and concurrence from the CDC or OGC that a court order is not required for installation or use of the device because there has been lawful consent, no reasonable expectation of privacy exists, or no physical trespass necessary to install the device. **Note:** Whenever circumstances change in either installation or monitoring, a new legal review should be obtained to determine whether a separate authorization is necessary.
- B. (U//FOUO) Use of the method is reasonably likely to achieve investigative objectives:

C. (U//FOUO)

b2
b7E

D. (U//FOUO)

b2
b7E

1. (U//FOUO)

b2
b7E

2. (U//FOUO)

b2
b7E

UNCLASSIFIED - FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

3. (U//FOUO) [REDACTED] b2
[REDACTED] b7E
[REDACTED]
4. (U//FOUO) [REDACTED] b2
[REDACTED] b7E
[REDACTED]

11.6.5. (U) Duration of Approval

(U//FOUO) [REDACTED] b2
[REDACTED] b7E
[REDACTED]
[REDACTED]

11.6.6. (U//FOUO) Specific Procedures

(U//FOUO) To use the method, the case agent must:

- A. (U//FOUO) [REDACTED] b2
[REDACTED] b7E
- B. (U//FOUO) [REDACTED] b2
[REDACTED] b7E
- C. (U//FOUO) [REDACTED] b2
[REDACTED] b7E
- D. (U//FOUO) [REDACTED] b2
[REDACTED] b7E
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
- E. (U//FOUO) [REDACTED] b2
[REDACTED] b7E
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
1. (U//FOUO) [REDACTED] b2
[REDACTED] b7E
[REDACTED]
2. (U//FOUO) [REDACTED] b2
[REDACTED] b7E
[REDACTED]
3. (U//FOUO) [REDACTED] b2
[REDACTED] b7E
[REDACTED]
[REDACTED]

UNCLASSIFIED - FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

(U//FOUO) [REDACTED]

b2
b7E

11.6.7. (U//FOUO) Compliance and Monitoring

(U//FOUO) Authorization documents regarding the use of the CCTV, electronic tracking devices [REDACTED] must be documented in the substantive investigative ELSUR file and will be available for compliance and monitoring review.

b2
b7E

UNCLASSIFIED - FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

11.7. (U) Investigative Method: Polygraph

11.7.1. (U) Summary

(U//FOUO) Application:

[REDACTED]
[REDACTED] not otherwise prohibited by AGG-Dom, Part III.B.2-3.
[REDACTED]

b2
b7E

11.7.2. (U) Legal Authority

(U) AGG-Dom, Part V.A.6.

11.7.3. (U//FOUO) Definition of Investigative Method

(U//FOUO) The polygraph is used to: (i) aid in determining whether a person has pertinent knowledge of a particular matter under investigation or inquiry; (ii) aid in determining the truthfulness of statements made or information furnished by a subject, victim, witness, CHS, or an individual making allegations; (iii) obtain information leading to the location of evidence, individuals or sites of offense; and (iv) assist in verifying the accuracy and thoroughness of information furnished by applicants and employees.

(U//FOUO)

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

b2
b7E

(U//FOUO) Note: This policy does not limit other authorized activities of the FBI, such as the FBI's responsibilities to conduct background checks and inquiries concerning applicants and employees under federal personnel security programs.

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

(U//FOUO) An SSA may approve the use of a polygraph if:

A. (U//FOUO)

B. (U//FOUO)

C. (U//FOUO)

11.7.5. (U) Duration of Approval

(U//FOUO)

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

b2
b7E

b2
b7E

UNCLASSIFIED - FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

11.7.6. (U//FOUO) Specific Procedures

(U//FOUO) An EC must be prepared requesting SSA approval for the polygraph. If an AUSA is assigned to the case, an FBI employee must confer with the USAO to discuss any prosecutorial issues prior to the administration of a polygraph.

11.7.7. (U//FOUO) Compliance and Monitoring

(U//FOUO) Except for polygraphs administered as part of a background check or as part of a federal personnel security program, all polygraphs must be conducted under and documented to a substantive case file.

UNCLASSIFIED - FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

11.8. (U) Investigative Method: Undercover Operations

11.8.1. (U) Summary

(U//FOUO)

[REDACTED]

b2
b7E

(U//FOUO) Undercover operations must be conducted in conformity with The Attorney General's Guidelines on Federal Bureau of Investigation Undercover Operations (AGG-UCO) in investigations relating to activities in violation of federal criminal law that do not concern threats to the national security or foreign intelligence. In investigations that 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 NSD in the review process. (AGG-Dom, Part V.A.7) Other undercover operations involving threats to the national security or foreign intelligence are reviewed and approved pursuant to FBI policy as described herein.

(U//FOUO) Application:

[REDACTED]

b2
b7E

11.8.2. (U) Legal Authority

- A. (U) AGG-Dom, Part V.A.7
- B. (U) AGG-UCO

11.8.3. (U//FOUO) Definition of Investigative Method

- A. (U//FOUO) An "undercover activity" is any investigative activity involving the use of an assumed identity by an undercover employee for an official purpose, investigative activity, or function. An "undercover employee" is 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.
- B. (U//FOUO) An "undercover operation" is an operation that involves a series of related "undercover activities" over a period of time by an "undercover employee." A series of related undercover activities consists of more than five separate substantive contacts by an undercover employee with the individuals under investigation. In investigations relating to activities in violation of federal criminal law that do not concern threats to the national security or foreign intelligence, undercover activity involving sensitive circumstances, which are listed in the AGG-UCO and the FGUSO, constitutes an undercover operation regardless of the number of contacts involved. A substantive contact is a communication, whether by

UNCLASSIFIED - FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

oral, written, wire, or electronic means, that includes information of investigative interest. Mere incidental contact (e.g., a conversation that establishes an agreed time and location for another meeting) is not a substantive contact within the meaning of this policy.

(U//FOUO) Distinction Between Sensitive Circumstance and Sensitive Investigative Matter:

(U//FOUO) The term "sensitive investigative matter" as used in the AGG-Dom should not be confused with the term "sensitive circumstance" as that term is used in undercover operations or ELSUR matters. The term sensitive circumstance relates to a circumstance that arises in an undercover operation that requires the UCO to obtain FBIHQ approval. A comprehensive list of sensitive circumstances for criminal activities is contained in the AGG-UCO and for national security matters in Section 28 of the NFIPM. The Criminal Undercover Operations Review Committee (CUORC) and the national security Undercover Review Committee (UCRC) must review and approve undercover operations that involve sensitive circumstances. The detailed policy for undercover operations is described in this section of the DIOG, the Field Guide for Undercover and Sensitive Operations (FGUSO), and the FBIHQ substantive Division program implementation guides.

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

- A. (U//FOUO) An official considering approval or authorization of a proposed undercover application must weigh the risks and benefits of the operation, giving careful consideration to the following:
1. (U//FOUO) The risks of personal injury to individuals, property damage, financial loss to persons or business, damage to reputation, or other harm to persons;
 2. (U//FOUO) The risk of civil liability or other loss to the government;
 3. (U//FOUO) The risk of invasion of privacy or interference with privileged or confidential relationships and any potential constitutional concerns or other legal concerns;
 4. (U//FOUO) The risk that individuals engaged in undercover operations may become involved in illegal conduct;
 5. (U//FOUO) The suitability of government participation in the type of activity that is expected to occur during the operation. (AGG-UCO, Part IV.A.)
- B. (U//FOUO) The following approval and authorization requirements apply to undercover operations relating to activities in violation of federal criminal law that do not concern threats to the national security or foreign intelligence:
1. (U//FOUO) An "undercover activity" in which an undercover employee plans to meet with a subject requires the approval of the SSA.
 2. (U//FOUO) An "undercover operation" must be approved by the SAC (or an ASAC with delegated approval authority). The CDC must review all undercover operations before approval and provide advice to the SAC regarding predication of subjects, entrapment issues, and whether the proposal meets the requirements of the AGG-UCO or other DOJ and FBI policy guidance.

UNCLASSIFIED - FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

3. (U//FOUO) In addition to SAC approval, authorization from the responsible FBIHQ Assistant Director or Executive Assistant Director must be obtained if the undercover operation involves a sensitive circumstance or certain fiscal circumstances, as those terms are defined in the AGG-UCO or other FBI guidance.
 4. (U//FOUO) Undercover operations that involve a sensitive circumstance (Group I undercover operations) require review by the CUORC as part of the authorization process. This requirement applies to both new and renewal proposals.
 5. (U//FOUO) Undercover operations that do not involve a sensitive circumstance (Group II undercover operations) require notice to the appropriate FBIHQ substantive Unit and to the Undercover and Sensitive Operations Unit following SAC approval. A renewal that would extend the operation beyond one year requires authorization from the responsible Assistant Director.
 6. (U//FOUO) All Innocent Images National Initiative (IINI) undercover operations deemed Group I and Group II operations require initiation and renewal approvals from FBIHQ, Cyber Division. Group I IINI undercover operations will also be reviewed by the CUORC.
 7. (U//FOUO) Requirements for interim approval and emergency approval for undercover operations are contained in the FGUSO.
- C. (U//FOUO) The following approval requirements apply to undercover operations that concern threats to the national security or foreign intelligence:
1. (U//FOUO) An "undercover operation" must be approved by the SAC (or an ASAC with delegated approval authority). The CDC must review all undercover operations before approval and provide advice to the SAC regarding predication of subjects, entrapment issues, and whether the proposal meets the requirements of Section 28 of the NFIPM, or its successor, or other DOJ and FBI policy guidance.
 2. (U//FOUO) In addition to SAC approval, authorization from the responsible FBIHQ Assistant Director or Executive Assistant Director must be obtained if the undercover operation involves a sensitive circumstance, as defined in Section 28 of the NFIPM, or its successor.
 3. (U//FOUO) Undercover operations that involve a sensitive circumstance must be reviewed and authorized by the responsible Assistant Director (Group I operations). Review by the UCRC must precede such authorization. If the matter involves religious or political organizations, the review must include participation by a representative of the DOJ NSD. (AGG-Dom, Section V; Section 28 of the NFIPM, or its successor)
 4. (U//FOUO) Undercover operations that do not involve a sensitive circumstance (Group II undercover operations) must be forwarded to the appropriate substantive Unit at FBIHQ for review on a UACB basis prior to initiation of the operation. A renewal that would extend the operation beyond 12 months requires authorization from the responsible Deputy Assistant Director or Assistant Director.
 5. (U//FOUO) Requirements for interim approval and emergency approval for undercover operations are contained in Section 28 of the NFIPM, or its successor.

UNCLASSIFIED - FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

11.8.5. (U) Duration of Approval

(U//FOUO)

[Redacted]

b2
b7E

11.8.6. (U) Additional Guidance

A. (U//FOUO)

[Redacted]

b2
b7E

B. (U//FOUO)

[Redacted]

b2
b7E

C. (U//FOUO)

[Redacted]

b2
b7E

11.8.7. (U//FOUO) Compliance and Monitoring, and Reporting Requirements

(U//FOUO) All UCOs must provide an

[Redacted] to appropriate

[Redacted]

summary using the

[Redacted]

b2
b7E

UNCLASSIFIED - FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

11.9. (U) Investigative Method: 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 FISA orders (50 U.S.C. §§ 1861-63).

(U) Summary

(U//FOUO)

b2
b7E

(U//FOUO) Application:

b2
b7E

When collecting positive foreign intelligence, if the subject is a non-United States person, a request for business records pursuant to 50 U.S.C. §§ 1861-63 is lawful.

11.9.1. (U) Federal Grand Jury Subpoena

A. (U) Legal Authorities

(U) A Federal Grand Jury is an independent panel charged with determining whether there is probable cause to believe one or more persons committed a particular federal offense within the venue of the district court. If the FGJ believes probable cause exists, it will vote a "true bill" and the person will be indicted. An FGJ indictment is the most typical way persons are charged with felonies in federal court. A FGJ can collect evidence through the use of an FGJ subpoena, which is governed by Rule 6 of the FRCP. FRCP 6(e) controls the release of information obtained by the prosecutor as part of the FGJ proceeding. FRCP 6(e) allows federal prosecutors to share valuable foreign intelligence, counterintelligence, and terrorism-related threat information, and it is the DOJ's policy that such information should be shared to the fullest extent permissible by law and in a manner consistent with the rule. The Attorney General has issued revised Guidelines for the Disclosure and Use of Grand Jury Information under Rule 6(e)(3)(D) (hereinafter "FGJ-Guidelines"). A memorandum issued by the Deputy Attorney General on May 15, 2008, provides amplifying guidance.

UNCLASSIFIED - FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

B. (U//FOUO) Definition of Method

(U//FOUO) FGJ subpoenas are demands for documents, records, testimony of witnesses, or any other evidence deemed relevant by a sitting grand jury. The FBI can request the issuance of an FGJ subpoena in coordination with the responsible United States Attorney's Office in all criminal investigative matters



b2
b7E

FGJ subpoenas are limited to use prior to the indictment of the individual to whom the subpoena relates.

C. (U) Approval Requirements

(U) There are no FBI supervisory approval requirements, but all FGJ subpoenas must be issued by the United States Attorney's Office that is handling the assessment or investigation to which the subpoenaed materials or witnesses are relevant.

D. (U) Duration of Approval

(U) FGJ subpoenas include a "return date," which is the date on which the subpoenaed materials or testimony is due to the grand jury.

E. (U) Specific Procedures

(U) FGJ subpoenas are governed by Rule 6(e) of the Federal Rules for Criminal Procedure and can only be obtained in coordination with the responsible United States Attorney's Office or the appropriate DOJ Division.

(U) Note: 28 C.F.R. § 50.10 requires the approval of the Attorney General before a trial or FGJ subpoena may be issued to a third party to obtain the telephone toll records of a member of the news media. Specific justification is required. Coordination with the Assistant United States Attorney handling the grand jury presentation or trial is necessary. Before proposing such a subpoena, an agent should review 28 C.F.R. § 50.10.

F. (U) Notice and Reporting Requirements

(U) There are no FBI notice or reporting requirements for FGJ subpoenas.

G. (U) Grand Jury Proceedings—Generally

1. (U) Procedural Issues and Handling of FGJ Materials

UNCLASSIFIED - FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

(U) The FGJ makes its determination whether to return a "true bill of indictment" based on evidence presented by the prosecuting attorney in an ex parte proceeding. The grand jury operates under the direction and guidance of the United States District Court. Generally, only witnesses for the prosecution testify before the grand jury.

(U) Only the United States Attorney or an assistant, other DOJ attorneys prosecuting the matter, the witness under examination, an interpreter (as needed), and the stenographer or operator of a recording device may be present while the grand jury is in session. No judge is present during the presentation of evidence although the court will sometime rule on evidentiary issues and will provide initial instructions to the FGJ. No person other than the grand jurors may be present while the grand jury is deliberating or voting.

2. (U) Restrictions on Disclosure

(U) As a general rule, no one other than a grand jury witness may disclose matters occurring before the grand jury. Government agents, even if called as witnesses, may not disclose matters occurring before the grand jury.

3. (U) Exceptions Permitting Disclosure

a. (U) **Disclosures by the government without the court's permission.** The government, through its attorney, may disclose grand jury matters under the following conditions:

i. (U) Under Rule 6(e)(3)(A), the government may disclose a grand jury matter to the following persons and in the following situations provided the government does not disclose the grand jury's deliberations or any grand juror's vote and the government provides the court that impaneled the grand jury with the names of all persons to whom disclosure was made and certifies that the government has advised the receiving party of the obligation of secrecy under this rule.

(U) Persons eligible to receive material under this subsection are: 1) an attorney for the government for use in performing that attorney's duty; 2) any government personnel, including state, local, Indian tribe, or foreign government personnel that an attorney for the government considers necessary to assist in performing that attorney's duty to enforce federal law; and 3) a person authorized under 18 U.S.C. § 3322.

(U) **Note:** FBI OGC attorneys and CDCs are not "attorneys for the government." Under this Rule, FRCP 1 defines "attorney for the government" as "the Attorney General, an authorized assistant of the Attorney General, a United States Attorney, [and] an authorized assistant of the United States Attorney."

ii. (U) An attorney for the government may disclose any grand jury matter to another Federal Grand Jury.

UNCLASSIFIED - FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

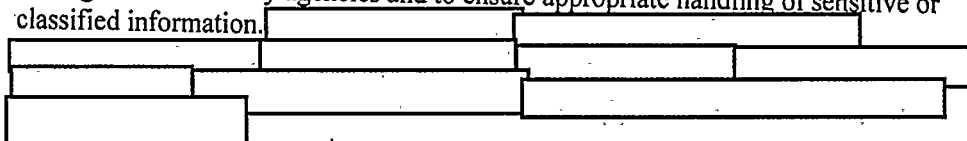
- iii. (U) An attorney for the government may disclose any grand jury matter involving foreign intelligence, counterintelligence, or foreign intelligence information to any federal law enforcement, intelligence, protective, immigration, national defense, or national security official to assist the official receiving the information in the performance of that official's duties. The government attorney must file, under seal, with the court that impaneled the grand jury, a notice that such information was disclosed and the agencies or departments that received the information. As used in Rule 6(e), foreign intelligence information is information that relates to the ability of the United States to protect against actual or potential attack or grave hostile acts by a foreign power or its agents; sabotage or international terrorism by a foreign power or its agents or clandestine intelligence activities by an intelligence service or network of a foreign power or its agents, or information with respect to a foreign power or foreign territory that relates to the national defense or security of the United States or the United States conduct of foreign affairs.
- iv. (U) An attorney for the government may disclose any grand jury matter involving, either in the United States or elsewhere, a threat of attack or other grave hostile acts of a foreign power or its agent, a threat of domestic or international sabotage, or clandestine intelligence gathering activities by an intelligence service or network of a foreign power or by its agent to any appropriate federal, state, local, Indian tribal, or foreign government official for the purpose of preventing or responding to such threat or activities. The government attorney must file, under seal, with the court that impaneled the grand jury, a notice that such information was disclosed and the agencies or departments that received the information.
- b. (U) **Disclosures by the government requiring the Court's permission.** The government, through its attorney, may disclose grand jury matters under the following conditions only with permission of the court. Petitions to make these disclosures are generally, but not always, filed with the court that impaneled the grand jury. Unless the hearing on the government's petition is to be ex parte, the petition must be served on all parties to the proceedings and the parties must be afforded a reasonable period of time to respond.
 - i. (U) An attorney for the government may petition for disclosure to a foreign court or prosecutor for use in an official criminal investigation.
 - ii. (U) An attorney for the government may petition for disclosure to a state, local, Indian tribal, or foreign government official, if the government attorney can show that the matter may disclose a violation of state, Indian tribal, or foreign criminal law, and the purpose of the disclosure is to enforce that law.
 - iii. (U) An attorney for the government may petition for disclosure to an appropriate military official if the government attorney can show the matter

UNCLASSIFIED - FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

may disclose a violation of military criminal law under the Uniform Code of Military Justice, and the purpose of the disclosure is to enforce that law.

c. (U//FOUO) FBI's Conduit Rule

(U//FOUO) Only the federal prosecutor is authorized to make an initial disclosure of Rule 6(e)(3)(D) foreign intelligence information. As a practical matter, such disclosures are ordinarily accomplished through the FBI, which may have existing information-sharing mechanisms with authorized receiving officials. If the prosecutor intends to share information directly with another official, consultation with the FBI is required to ensure that disclosures will be consistent with the existing policy of intelligence community agencies and to ensure appropriate handling of sensitive or classified information.



b2
b7E

(U//FOUO) If, in cases of emergency, the prosecutor must disclose information before consulting with the FBI, the prosecutor must notify the FBI as soon as practicable.

d. (U) Other Limitations

(U) Rule 6(e)(3)(D) does not eliminate certain other information protection requirements, such as restrictions on disclosures of tax returns, on certain financial information under the Right to Financial Privacy Act, and on classified information, to name only a few examples. Specific statutes may impose additional burdens of disclosures.

e. (U) Disclosure

- i. (U) An FBI employee may become a "Receiving Official," the person to whom grand jury information has been disclosed, if the FBI receives grand jury information developed during investigations conducted by other agencies. A Receiving Official is any federal, state, local, Indian tribal, or foreign government official receiving grand jury information, disclosed by an attorney for the government, under any provision of Rule 6(e)(3)(D). A Receiving Official may only use the disclosed material as necessary in the conduct of his/her official duties. The Receiving Official ordinarily must consult with the federal prosecutor before disseminating the information publicly, including in open court proceedings.
- ii. (U//FOUO) Receiving Officials may only use grand jury information in a manner consistent with the FGJ-Guidelines and any additional conditions placed on the use or handling of grand jury information by the attorney for the government.

UNCLASSIFIED - FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

- iii. (U//FOUO) If dissemination is necessary to the performance of his or her official duties, a Receiving Official may disseminate Rule 6(e)(3)(D) information outside of that official's agency to other government officials.
 - iv. (U) A Receiving Official, other than a foreign government official, must consult with the attorney for the government before disseminating Rule 6(e)(3)(D) information publicly (including through its use in a court proceeding that is open to or accessible to the public), unless prior dissemination is necessary to prevent harm to life or property. In such instances, the Receiving Official shall notify the attorney for the government of the dissemination as soon as practicable.
 - v. (U) A foreign government Receiving Official must obtain the prior consent from the disclosing official where possible, or if the disclosing is unavailable, from the agency that disseminated the information to that foreign official before dissemination of the information to a third government or publicly. Public dissemination includes using the information in a court proceeding that is open to or accessible by the public.
 - vi. (U) A Receiving Official shall handle Rule 6(e)(3)(D) information in a manner consistent with its sensitivity and shall take appropriate measures to restrict access to this information to individuals who require access for the performance of official duties.
 - vii. (U) A Receiving Official shall immediately report to the disclosing attorney for the government: any unauthorized dissemination of Rule 6(e)(3)(D) information; or any loss, compromise, or suspected compromise of Rule 6(e)(3)(D) information.
- f. (U) Violations
- i. (U) A Receiving Official who knowingly violates Rule 6(e)(3)(D) by using the disclosed information outside the conduct of his or her official duties, or by failing to adhere to any limitations on the dissemination of such information, may be subject to contempt of court proceedings and to restriction on future receipt of Rule 6(e)(3)(D) information.
 - ii. (U) A state, local, Indian tribal, or foreign government official who receives Rule 6(e)(3)(D) information, and who knowingly violates these guidelines, may be subject to contempt of court proceedings.
 - iii. (U) An attorney for the government who knowingly violates Rule 6(e)(3)(D) may be subject to contempt of court proceedings.

UNCLASSIFIED - FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

g. (U) Limitation on Unauthorized Disclosures.

(U) Rule 6(e)(3)(D)(i) provides that Receiving Officials may use disclosed information only to conduct their "official duties subject to any limitation on the unauthorized disclosure of such information." This "limitation on unauthorized disclosures" is understood to encompass applicable statutory, regulatory, and guideline restrictions regarding classification, privacy, or other information protection, as well as any additional restrictions imposed by the federal prosecutor.

(U//FOUO) **Note:** The FGJ-Guidelines do not require that the Receiving Official notify the federal prosecutor of subsequent disclosures, except for consultation for public disclosures and consent for certain disclosures by foreign officials. The Receiving Official is bound by whatever restrictions govern his or her use and disclosure of the information as part of his official duties. (Memo dated 5/15/08, Guidelines for the Disclosure and Use of FGJ Information under Rule 6[e][3][D]).

h. (U//FOUO) Limitation of Use.

- i. (U//FOUO) Because of the restrictions involved in handling information that is obtained by the use of a grand jury subpoena, whenever possible, alternatives to the grand jury subpoena, such as [REDACTED] should be considered as an alternative method of obtaining evidence.
- ii. (U) A grand jury subpoena may only be used for purposes of gathering information that is relevant to the grand jury's investigation. Grand jury secrecy continues indefinitely, regardless of whether there is an indictment, unless the material becomes a matter of public record, such as by being introduced at trial.
- iii. (U) Rule 6(e)(3)(D) does not require notice to the court of subsequent dissemination of the information by Receiving Officials.
- iv. (U//FOUO) Disclosure of grand jury material cannot be made within the FBI for unrelated investigations unless a government attorney has determined that such disclosure to a particular investigator is needed to assist that attorney in a specific criminal investigation. The ability of government attorneys to freely share grand jury material with other government attorneys for related or unrelated criminal investigations does not extend to investigators without case specific authorization from the government attorney and notice to the court. Therefore, grand jury material must be restricted when placed into a general system of records that is freely accessible to FBI employees and others with access (e.g., ACS).
- v. (U//FOUO) If a government attorney authorizes the disclosure of grand jury material in the possession of the FBI for use in an unrelated federal criminal

b2
b7E

UNCLASSIFIED - FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

matter, such approval should be documented in the grand jury subfile of both the initiated case file and the subsequent case file. That documentation will be in addition to any necessary supplementation to the government attorney's FRCP Rule 6(e) disclosure letter and/or to the internal disclosure list.

- vi. (U//FOUO) The USAO should be consulted immediately for precautionary instructions if grand jury material will have application to civil law enforcement functions (e.g., civil RICO or civil forfeiture). There are very limited exceptions that allow government attorneys to use grand jury material or information in civil matters (e.g., civil penalty proceedings concerning banking law violations). These exceptions do not automatically apply to investigative personnel. Therefore, any similar use of grand jury information by the FBI must be approved in advance by the government attorney.
- vii. (U//FOUO) Disclosure cannot be made without a court order for use in non-criminal investigations, such as background investigations or name checks.
- viii. (U//FOUO) Government personnel who are preparing a response to a Freedom of Information Act or Privacy Act request may properly access grand jury material under the Rule because they are considered to be assisting the grand jury attorney by ensuring against any improper disclosure.
- i. (U) **Matters Occurring Before the Grand Jury**
 - i. (U) **Core Grand Jury Material:** There can be no dissemination of matters occurring before the grand jury unless such dissemination comes within one of the exceptions discussed above. There is no uniform legal definition of what constitutes matters occurring before the grand jury except for what is generally referred to as "core" grand jury material. "Core grand jury material" includes the following: (i) names of targets and witnesses; (ii) grand jury testimony; (iii) grand jury subpoenas; (iv) documents with references to grand jury testimony (including summaries and analyses); (v) documents that clearly reveal the intentions or direction of the grand jury investigation; and (vi) other material that reveals the strategy, direction, testimony, or other proceedings of a grand jury.
 - ii. (U) **Documents Created Independent of Grand Jury but Obtained by Grand Jury Subpoena:** Rule 6(e) generally prohibits disclosing "matters occurring before the grand jury." The rule, however, does not define that phrase. The issue of whether pre-existing documents fall within that prohibition has never been settled conclusively by the Supreme Court, although many lower courts have discussed it at length. Courts generally agree that this prohibition does not cover all information developed in the course of a grand jury investigation; rather, the secrecy rule applies only to information that would reveal the existence, strategy or direction of the grand jury investigation, the nature of the evidence produced before the grand jury, the views expressed by

UNCLASSIFIED - FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

members of the grand jury, or anything else that actually occurred before the grand jury. In addition, courts have frequently held that Rule 6(e) does not protect documents subpoenaed from the government that are sought by third parties only for the information contained within the document rather than to determine the direction or strategy of the grand jury investigation. Due to developing law on this issue, FBI personnel should consult with the AUSA responsible to determine how to best handle these documents.

- iii. **(U//FOUO) Data Extracted from Records Obtained by Grand Jury Subpoena:** Information extracted from business records that was obtained by grand jury subpoena is often used to facilitate investigations. Some of that type of data is, by statute or case law, subject to "the Rule." In other cases, determination of whether data must be considered subject to "the Rule" depends on the case law and local practice in the federal district. Information extracted from grand jury subpoenaed financial records subject to the Right to Financial Privacy Act of 1978 (12 U.S.C. § 3420) must be treated as grand jury material "unless such record has been used in the prosecution of a crime for which the grand jury issued an indictment or presentment...." With the approval of the USAO, information from subpoenaed telephone records may be disclosed for use in unrelated federal criminal investigations in those districts where such material is not considered a "matter occurring before a grand jury." If the USAO approves generally of this procedure, such information may be used in unrelated criminal investigations without authorization from a government attorney in each instance.

j. **(U) Federal Grand Jury Physical Evidence and Statements of Witnesses**

- i. (U) Physical evidence provided to the government in response to a grand jury subpoena is subject to the secrecy rule regardless of whether such evidence is presented to the grand jury. Physical evidence provided voluntarily or obtained by means other than grand jury process (such as by a search warrant) is not a grand jury matter regardless of whether such evidence was previously or is thereafter presented to the grand jury.
- ii. (U) Statements of witnesses obtained as a result of grand jury process, including grand jury subpoena, such as a statement given in lieu of grand jury testimony, are matters occurring before the grand jury irrespective of whether such witnesses testified before the grand jury or are not required to testify. Voluntary statements of witnesses made outside of the grand jury context (not pursuant to any grand jury process including a grand jury subpoena), including statements made outside the grand jury by a witness who is being prepared for grand jury testimony, are not grand jury matters irrespective of whether the witness previously testified or will thereafter testify before the grand jury.
- iii. (U) Rule 6(e)(3)(B) requires a federal prosecutor who discloses grand jury material to government investigators and other persons supporting the grand

UNCLASSIFIED - FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

jury investigation to promptly provide the court that impaneled the grand jury the names of the persons to whom such disclosure has been made and to certify that he/she has advised such persons of their obligation of secrecy under the Rule. In order to document the certification required by the Rule, government attorneys often execute and deliver to the court a form, normally referred to as a "Certification" or "Rule 6(e) letter." A copy of this document should be maintained with the grand jury material held in the FBI's custody.

iv. **(U//FOUO) Documentation of Internal Disclosures of Grand Jury Material:**

Grand jury material should be kept in such a fashion as to maintain the integrity of the evidence. Upon taking custody of grand jury material, the FBI employee should categorize it in a manner to identify its production source and how it was obtained, to include the identity of a custodian of record for documentary evidence. Practical considerations often require agents assisting government attorneys to seek assistance in the same investigation from others within the FBI. In many districts, support personnel and supervisors of case agents need not be routinely included in the list provided to the court. In lieu of a Rule 6(e) letter from the USAO containing an exhaustive list of names of FBI personnel, an FBI record of additional internal disclosures must be maintained by the case agent in order to establish accountability. Use of this "internal certification" procedure should be authorized by the appropriate USAO. The internal form should record the date of disclosure as well as the identity and position of the recipient. Such internal disclosures may be made only in support of the same investigation in which a federal prosecutor has previously issued a Rule 6(e) letter. In addition, the internal record should reflect that all recipients of grand jury materials were advised of the secrecy requirements of Rule 6(e). Whenever practicable, recipients should be listed on this internal certification prior to disclosure. Local Rule 6(e) customs should govern the internal certification process used.

v. **(U//FOUO) Storage of Grand Jury Material:** The FBI cannot make or allow unauthorized disclosure of grand jury material. Material and records obtained pursuant to the grand jury process are frequently stored in FBI space. FBI personnel should report any unauthorized disclosure to the appropriate government attorney who, in turn, must notify the court. In order to protect against unauthorized disclosure, grand jury material must be secured in the following manner:

1. **(U//FOUO)** The cover, envelope, or container containing grand jury materials must be marked with the warning: "GRAND JURY MATERIAL - DISSEMINATE ONLY PURSUANT TO RULE 6(e)." No Grand Jury stamp or mark should be affixed to the original material. Agents, analysts and other authorized parties should work from copies of grand jury material whenever possible to ensure the original material retains its integrity.

UNCLASSIFIED - FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

2. (U//FOUO) Access to grand jury material must be limited to authorized persons (e.g., those assisting an attorney for the government in a specific criminal investigation). All necessary precautions should be taken to protect grand jury material, to include maintaining the material in a secure location when not in use. The material must be appropriately segregated, secured, and safeguarded. Absent chain-of-custody considerations, grand jury material may be maintained in the 1A section of the file. Grand jury material need not be kept in an evidence or bulky exhibit room and may be entrusted to a support services technician (SST) or evidence control technician (ECT). Should grand jury material be entered into a computer database, the data must be marked with the 6(e) warning and maintained within the system in a restricted manner.
3. (U//FOUO) Registered mail or other traceable courier (such as Federal Express) approved by the Chief Security Officer (CSO) must be used to mail or transmit to other Field Offices any documents containing grand jury material. Couriers and other personnel employed in these services will not be aware of the contents of the material transmitted because of the wrapping procedures specified below, and therefore, then do not require a background investigation for this purpose. The names of persons who transport the material need not be placed on a disclosure list, but the receiving office must provide the case agent in the originating office with the names of personnel in the receiving office to whom disclosure is made.
4. (U//FOUO) Grand jury material that is to be mailed or transmitted by traceable courier outside a facility must be enclosed in opaque inner and outer covers. The inner cover must be a sealed wrapper or envelope that contains the addresses of the sender and the addressee, who must be authorized to have access to the grand jury material. The inner cover must be conspicuously marked "Grand Jury Information To Be Opened By Addressee Only." The outer cover must be sealed, addressed, return addressed, and bear no indication that the envelope contains grand jury material. When the size, weight, or nature of the grand jury material precludes the use of envelopes or standard packaging, the material used for packaging or covering must be of sufficient strength and durability to protect the information from unauthorized disclosure or accidental exposure.
5. (U//FOUO) If the government attorney determines that the sensitivity of, or threats to, grand jury material necessitates a more secure transmission method, the material may be transmitted by an express mail service approved for the transmission of national security information or be hand carried by the assigned government attorney or his or her designated representative.
6. (U//FOUO) Grand jury material containing classified national security information must be handled, processed, and stored according to 28 C.F.R.

UNCLASSIFIED - FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

Part 17. Grand jury material containing other types of sensitive information, such as federal tax return information, witness security information, and other types of highly sensitive information that have more stringent security requirements than that usually required for grand jury material must be stored and protected pursuant to the security regulations governing such information and any special security instructions provided by the organization that originated the information.

7. (U//FOUO) Original documents that are obtained through the grand jury process should be returned to the attorney for the government or, with the government attorney's permission, to the owner if there is no indictment or the prosecution has concluded.

k. (U) Requests for Subpoenas in Fugitive Investigations

(U//FOUO) It is generally a misuse of the grand jury to use the grand jury as an investigative aid in the search for a fugitive. Therefore, with the exceptions discussed below, grand jury subpoenas for testimony or records related to the fugitive's whereabouts may not be requested in FBI fugitive investigations.

- i. (U//FOUO) Grand jury process may be used to locate a fugitive if the grand jury is interested in hearing the fugitive's testimony. Thus, if the grand jury seeks the testimony of the fugitive in an investigation that the grand jury is indicting, the grand jury may subpoena other witnesses and records in an effort to locate the fugitive witness. However, interest in the fugitive's testimony must not be a pretext. The sole motive for inquiring into the fugitive's location must be the potential value of fugitive's testimony to the grand jury's investigation. A subpoena for the fugitive witness must be approved by the grand jury before seeking to subpoena witnesses or records to locate the fugitive. Further, it is not proper to seek to obtain grand jury testimony from any witness, including a fugitive, concerning an already-returned indictment. Thus, it would not be proper to seek to locate a fugitive for the purpose of having the fugitive testify about matters for which an indictment has already been returned, unless there are additional unindicted defendants to be discovered or additional criminal acts to be investigated through the testimony of the fugitive. Current policy on "target" witnesses must be observed. Grand jury subpoenas for witnesses and records aimed at locating a fugitive witness who is a target of the grand jury investigation should be sought only where a target subpoena for the fugitive has already been approved by the responsible Assistant Attorney General.
- ii. (U//FOUO) Use of the grand jury to learn the present location of a fugitive is also proper when the present location is an element of the offense under investigation. On adequate facts, the present location of a fugitive might tend to establish that another person is harboring the fugitive, or has committed misprision, or is an accessory after the fact in the present concealment of the fugitive. However, this justification would likely be viewed as a subterfuge if the suspected harbinger or

UNCLASSIFIED - FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

the person potentially guilty of misprision or as an accessory were given immunity in the grand jury in order to compel his/her testimony about the location of the fugitive. With regard to escaped federal prisoner and bond default matters, the present location of a fugitive is not relevant evidence in a grand jury investigation because these offenses address the circumstances of a prior departure from a known location. The fugitive's present location is not a relevant factor as it is in harboring or as it may be in a misprision investigation. Inasmuch as unlawful flight to avoid prosecution cases are, as a rule, not prosecuted and cannot be prosecuted without written authorization from the Attorney General or an Assistant Attorney General, any effort to use the grand jury in the investigation of such cases must be preceded by consultation with the DOJ and by written authorization to prosecute from the Assistant Attorney General in charge of the Criminal Division.

11.9.2. (U) Administrative Subpoena

A. (U) Summary

(U) The Attorney General of the United States is vested with the authority to issue administrative subpoenas under two provisions of the United States Code that have relevance to FBI criminal investigations, 21 U.S.C. § 876 and 18 U.S.C. § 3486. The FBI has no inherent authority to issue administrative subpoenas but relies on delegated authority from the Attorney General. The use of administrative subpoenas is limited to three categories of investigations—drug program investigations, child sexual exploitation and abuse investigations, and health care fraud investigations—and may not be used for any other purpose. The delegated authority varies depending on the federal violation being investigated. The type of information that can be obtained using an administrative subpoena is also limited by law or by policy of the Attorney General.

(U//FOUO) Note: Within the FBI, the authority to issue administrative subpoenas is limited to those positions holding the delegated authority from the Attorney General; that authority may not be redelegated.



b2
b7E

B. (U) Legal Authority and Delegation

1. (U) Investigations involving the sale, transfer, manufacture or importation of unlawful drugs

(U) Authority: 21 U.S.C. § 876 and DOJ Regulation at 28 C.F.R. App to Pt. 0, Subpt. R § 4.

(U) May be issued to: Any individual or business holding records relevant to the drug investigation.

(U) Records to be obtained: Any records relevant to the investigation.

(U//FOUO) Delegated authority to issue: By DOJ regulation, the Attorney General's delegation includes SACs, ASACs, SSRAs and "those FBI Special Agent Squad

UNCLASSIFIED - FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

Supervisors who have management responsibilities over Organized Crime/Drug Program investigations."

(U//FOUO) [REDACTED]

b2
b7E

(U//FOUO) **Limitations:** [REDACTED]

b2
b7E

[REDACTED] The Right to Financial Privacy Act limitations described in paragraph D of this section apply. If addressed to a provider of "electronic communication service" or a "remote computing service," provisions in the Electronic Communication Privacy Act (ECPA) govern, as discussed in paragraph D of this section.

2. (U) **Investigations involving the sexual exploitation or abuse of children**

(U) **Authority:** 18 U.S.C. § 3486(a) and Attorney General Order 2718-2004.

(U) **May be issued to:** A "provider of an electronic communication service" or a "remote computer service" (both terms defined in Section 11.9.2.D.2.b, below) and only for the production of basic subscriber or customer information. The subpoena may require production as soon as possible but in no event less than 24 hours after service of the subpoena.

(U) **Records to be obtained:** [REDACTED]

b2
b7E

(U//FOUO) **Delegated authority to issue:** [REDACTED]

b2
b7E

(U//FOUO) **Limitations:** By law, these administrative subpoenas may only be issued in cases that involve a violation of 18 U.S.C. §§ 1201, 2241(c), 2242, 2243, 2251, 2251A, 2252, 2252A, 2260, 2421, 2422, or 2423 in which the victim has not attained the age of 18 years. Under the Attorney General's delegation, an administrative subpoena in these investigations may be issued only to "providers of electronic communication services" or to "remote computing services" to obtain the information listed above. These

UNCLASSIFIED - FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

administrative subpoenas may not be issued to any other person or entity or to obtain any other information, including the content of communications. [REDACTED]

b2
b7E

3. (U) Investigations involving Federal Health Care Fraud Offenses

(U) Authority: 18 U.S.C. § 3486(a)

(U) Records to be obtained: Records relevant to an investigation relating to a "federal health care offense." Federal health care offense is defined in 18 U.S.C. § 24

(U) May be issued to: Any public or private entity or individual with records relevant to the federal health care offense. (Note: These are referred to in guidance issued by the Attorney General as "investigative demands.")

(U//FOUO) Delegated authority to issue: There is no delegation to the FBI. Delegated to personnel within DOJ's Criminal Division and to United States Attorneys, who may redelegate the authority to Assistant United States Attorneys.

(U) Limitations: The Right to Financial Privacy Act (RFPA) limitations described in paragraph D of this section apply. The provisions in ECPA govern, as discussed in paragraph D of this section, if the request for records is addressed to a "provider of electronic communication service" or a "remote computing service." The subpoena may not require the production of records at a place more than 500 miles from the place the subpoena is served. [REDACTED]

b2
b7E

(U) Restriction on individual health care information: Pursuant to 18 U.S.C. § 3486, health information about an individual acquired through an authorized investigative demand may not be used in, or disclosed to any person for use in, any administrative, civil, or criminal action against that individual unless the action or investigation arises from and is directly related to receipt of health care, payment for health care, or action involving a fraudulent claim related to health care.

(U//FOUO) [REDACTED]

b2
b7E

C. (U) Approval Requirements

(U//FOUO) Use of an administrative subpoena requires SSA approval. The SSA may issue the administrative subpoena if the authority has been so delegated. Further review and approval may be required depending on the delegation. Review by the CDC is appropriate if legal questions arise in preparing and issuing the subpoena.

(U//FOUO) Note: An individual designated by proper authority to serve in an "acting" status in one of the positions with delegated authority may sign and issue an administrative subpoena. The "acting" status should be documented in an appropriate Field Office administrative file and noted in the case file. For example, if the ASAC with authority to sign is away on leave or temporary duty and another individual has been designated by the SAC to serve as "acting" ASAC, that individual has authority to issue the administrative subpoena.

UNCLASSIFIED - FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

A relief supervisor is not considered to be in an "acting" status for purposes of issuing an administrative subpoena.

D. (U) Limitations on Use of Administrative Subpoenas

1. (U) Financial Privacy Limitations

- a. (U) **Obtaining records from a financial institution.** "Financial records" are those records that pertain to a customer's relationship with a financial institution. The term "financial institution" is broadly defined as a bank, savings bank, card issuer, industrial loan company, trust company, savings association, building and loan or homestead association, credit union, or consumer finance institution, located in any state, territory, or the District of Columbia. See 12 U.S.C. § 3401. [Note: The scope of the RFPA's definition of financial institution for this purpose, which limits the restrictions the RFPA places on federal law enforcement in using an administrative subpoena, is narrower than the definition of financial institution that is used in connection with NSLs. For that purpose, the RFPA refers to the broader definition found in the Bank Secrecy Act (BSA). Among the entities included in the BSA definition are money transmitting businesses, car dealers, travel agencies, and persons involved in real estate closings. See 12 U.S.C. § 3414(d) and 31 U.S.C. § 5312. (a)(2) and (c)(1).] When seeking financial records from a financial institution, the FBI must send a certificate of compliance required by 12 U.S.C. § 3403 to the financial institution. The certificate must indicate, among other things, that notice has been provided by the FBI to the individual customer whose financial records are to be obtained. The content of the notice is set out in 12 U.S.C. § 3405. A court order may be obtained that allows for delayed notice pursuant to 12 U.S.C. § 3409. Notice is not required if the administrative subpoena is issued to obtain the financial records of a corporation or for records not pertaining to a customer. Notice is also not required if the administrative subpoena seeks only basic account information, defined as name, address, type of account, and account number. See 12 U.S.C. § 3413(g).
- b. (U) **Obtaining records from a Credit Bureau.** A credit bureau or consumer reporting agency may only provide name, address, former addresses, place of employment and former place of employment in response to an administrative subpoena. 15 U.S.C. § 1681f. A credit bureau or consumer reporting agency may not release financial information in a credit report or consumer report, or the names and locations of financial institutions at which the consumer has accounts pursuant to an administrative subpoena. A court order, a grand jury subpoena, or, in an appropriate case, a national security letter may be used to obtain this information. 15 U.S.C. § 1681b. Notice of disclosure will be provided by the credit bureau or consumer reporting agency to the consumer if the consumer requests this information.

2. (U) Electronic Communication Privacy Act

- a. (U) **Use of an Administrative Subpoena.** The ability to gather subscriber information and the content of electronic communications using an administrative subpoena is governed by ECPA. In cases involving the sexual exploitation or abuse of children, only basic subscriber or customer information may be obtained with an

UNCLASSIFIED - FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

administrative subpoena under the terms of the Attorney General's delegation, as described above. No content information may be obtained. In drug and health care fraud investigations, an administrative subpoena may be used to obtain basic subscriber or customer information and certain stored communications, under limited circumstances, from entities that provide electronic communication services to the public.

- b. (U) **Definitions.** ECPA applies to two types of entities that provide electronic communications to the public. The term "provider of electronic communication services" is defined in 18 U.S.C. § 2510(15) as "any service that provides the user thereof the ability to send or receive wire or electronic communications." The term "remote computing services" is defined in 18 U.S.C. § 2711(12) as the "provision to the public of computer storage or processing services by means of an electronic communication system."

- c. (U) **Subscriber information.** [REDACTED]

b2
b7E

- d. (U) **Records or other information pertaining to a subscriber.** [REDACTED]

b2
b7E

- e. (U) **Content.** Content is the actual substance of files stored in an account, including the subject line of an e-mail.

- (1) (U) Unopened e-mail held in storage for 180 days or less may not be obtained using an administrative subpoena. A search warrant is required.
- (2) (U) Unopened e-mail that has been held in electronic storage for more than 180 days may be obtained with an administrative subpoena. (In the Ninth Circuit, the opened e-mail and un-opened e-mail must have been in storage for 180 days before it can be obtained with an administrative subpoena. See Theofel v. Farey-Jones, 359 F.3d 1066.) The government must provide notice to the subscriber or customer prior to obtaining such content. A limited exception to the notice requirement is provided in 18 U.S.C. § 2705.
- (3) (U) E-mail that has been opened and the content of other electronically stored files held in storage by an entity that provides storage services to the public (i.e., a remote computing service, as defined in 18 U.S.C. § 2711), may be obtained using an administrative subpoena with notice to the customer or subscriber, unless notice is delayed in accordance with 18 U.S.C. § 2705.

UNCLASSIFIED - FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

- (4) (U) E-mail that has been opened and the content of other electronically stored files held in storage by an entity that does not provide electronic communication services to the public, such as that on the internal network of a business, may be obtained using an administrative subpoena. Notice to the individual is not required because this demand is not restricted by ECPA.

3. (U//FOUO) Members of the Media

(U//FOUO) An administrative subpoena directed to a provider of electronic communication services or any other entity seeking to obtain local and long distance connection records, or records of session times of calls, made by a member of the news media may only be issued with the specific approval of the Attorney General. Requests for this approval should be reviewed by the CDC and coordinated with an Assistant United States Attorney (AUSA). The request must provide justification for issuance of the subpoena consistent with the Department of Justice policies set forth in 28 C.F.R. § 50.10. Guidance on this policy may be obtained from the Investigative Law Unit and/or the Privacy and Civil Liberties Unit, OGC.

E. (U//FOUO) Compliance/Monitoring

1. (U) Limits on use.

b2
b7E

2. (U//FOUO) Overproduction.

b2
b7E

3. (U//FOUO) Factors for compliance. The following factors should be considered to ensure compliance with applicable laws and regulations that govern the FBI's use of administrative subpoenas:

- a. (U//FOUO) The administrative subpoena must relate to a type of investigation for which the subpoena is authorized;
- b. (U//FOUO) The administrative subpoena must be directed to a recipient to whom an administrative subpoena is authorized;
- c. (U//FOUO) The administrative subpoena may request only records that are authorized under the pertinent law;

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]
[Redacted]

b2
b7E

1. (U//FOUO) Cover EC

(U//FOUO) [Redacted]

[Redacted]

b2
b7E

a. (U//FOUO) [Redacted]

[Redacted]

b. (U//FOUO) [Redacted]

[Redacted]

c. (U//FOUO) [Redacted]

[Redacted]

d. (U//FOUO) [Redacted]

b2
b7E

[Redacted]

e. (U//FOUO) [Redacted]

[Redacted]

f. (U//FOUO) [Redacted]

[Redacted]

g. (U//FOUO) [Redacted]

[Redacted]

h. (U//FOUO) [Redacted]

[Redacted]

i. (U//FOUO) [Redacted]

[Redacted]

j. (U//FOUO) [Redacted]

[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]

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

b2
b7E

(U//FOUO)

b2
b7E

(U//FOUO)

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)

b2
b7E

UNCLASSIFIED - FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

[Redacted]

b2
b7E

(U//FOUO)

[Redacted]

b2
b7E

(U//FOUO)

[Redacted]

b2
b7E

(U//FOUO)

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

[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 RFPA, 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

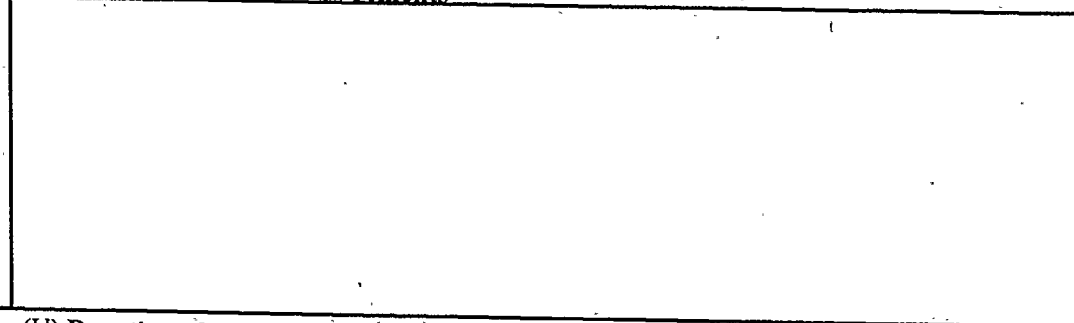
A. (U) Legal Authority

(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

F. (U) Compliance Requirements

(U) The case agent who receives production of documents pursuant to a FISA business records order must do the following:

1. (U//FOUO) Handle the production as required by the Standard Minimization Procedures Adopted for Business Record Orders

b2
b7E

2. (U) Whether or not required by paragraph 1, prior to uploading the documents or data received into FBI databases, review the documents produced to determine whether they are responsive to the order.

- a. (U//FOUO) If the producing party has mistakenly provided material that is entirely non-responsive (e.g., the producing party inverted numbers on an account and produced entirely irrelevant and non-responsive material), the case agent must sequester the material and discuss with the CDC or NSLB the appropriate way to return the unresponsive material to the producing party and obtain the responsive material.

- b. (U//FOUO) If the producing party has produced responsive material and material that is beyond the parameters of the order issued by the FISC (e.g., the FISC ordered production of one month's records and the party produced records for 6 weeks), the case agent must determine whether the material produced that is outside the parameters of the FISC order is subject to statutory protection (e.g., records that are subject to the Right to Financial Privacy Act, the Buckley Amendments, the Electronic Communications Privacy Act, Fair Credit Reporting Act).

- i. (U//FOUO) If the overproduced material is subject to statutory protection, then the overproduced material must be treated like overproduction is treated in the context of a national security letter.

- ii. (U//FOUO) If the overproduced material is not subject to statutory protection, then it may be uploaded. In determining whether to upload the overproduced material, the case agent should consider the extent to which the overproduction includes non-public information regarding United States persons who are not the subject of a national security investigation; the sensitivity of the information contained within the overproduction; and the burdensomeness of separating the overproduced material from the responsive material.

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).

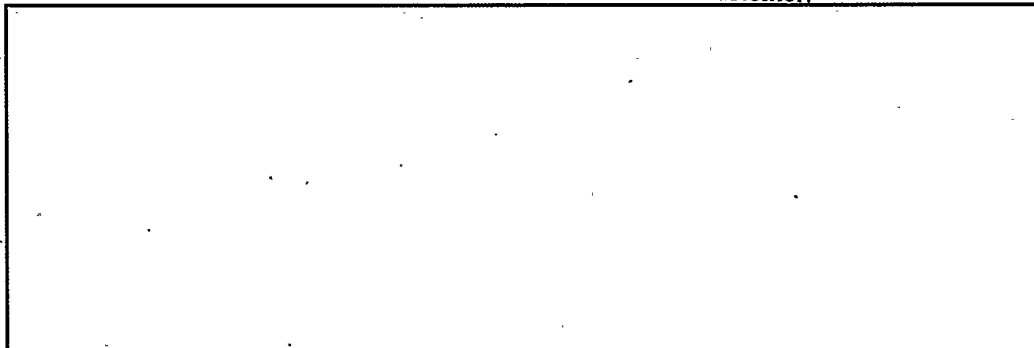
(U) **Electronic Communication Service (ECS):** is "any service that provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15). For example, telephone companies and electronic mail companies generally act as providers of electronic communication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

I. (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

-
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.

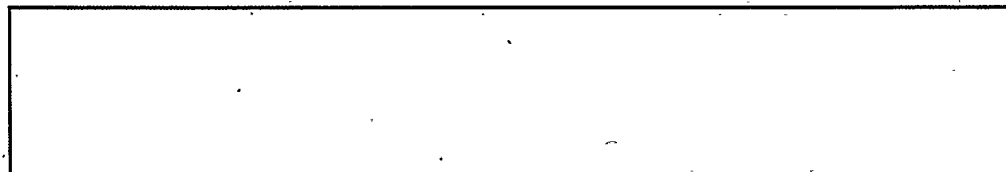
(U) **Nationwide Scope:** Search warrants under 18 U.S.C. § 2703(a) may be issued by a federal "court with jurisdiction over the offense under investigation," and may be executed outside the district of the issuing court for material responsive to the warrant. State courts may also issue warrants under 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

b2
b7E

[REDACTED]

(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]

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. [REDACTED]

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) [REDACTED]

b2
b7E

(U) **Notice:** [REDACTED]

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)

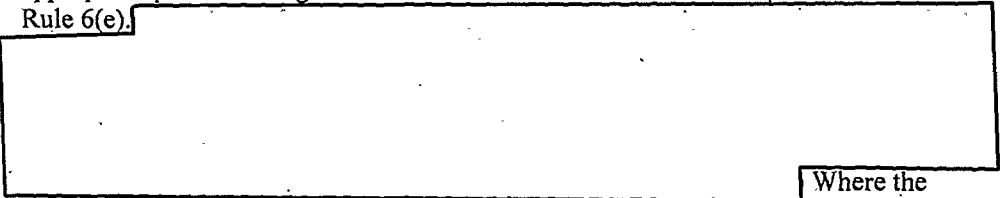


b2
b7E

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)

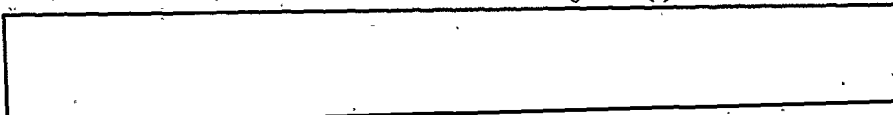
UNCLASSIFIED - FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

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:

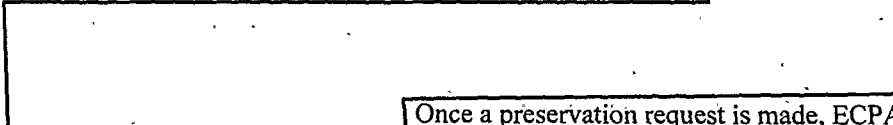
- (a) (U) The disclosure is with the consent (express or implied) of the customer or subscriber or 18 U.S.C. § 2702(c)(2);
- (b) (U) The disclosure "may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service," 18 U.S.C. § 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):**



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).



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

(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;

(b)

b2
b7E

(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.

b2
b7E

(U//FOUO)

b2
b7E

(U//FOUO)

b2
b7E

(U//FOUO)

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:

b2
b7E

UNCLASSIFIED - FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

[Redacted]

B. (U//FOUO) Contact with Providers: [Redacted]

[Redacted]

b2
b7E

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

[REDACTED] FISAMS will route the request to appropriate parties for their review and approval of the request [REDACTED]
[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.

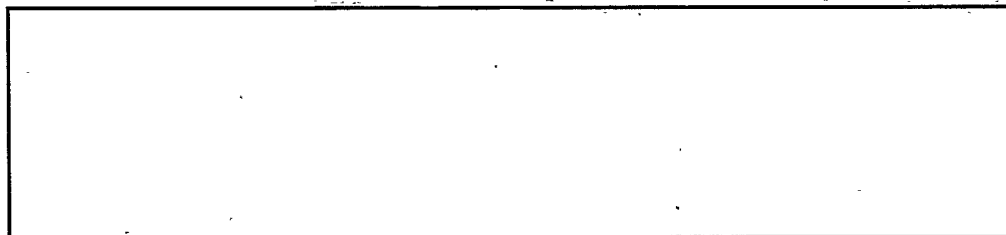
11.11.6. (U//FOUO) Specific Procedures

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]

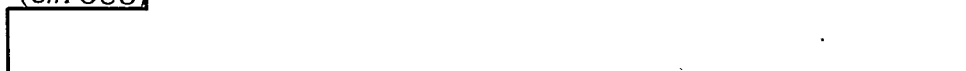
b2
b7E

UNCLASSIFIED - FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide



b2
b7E

2. (U//FOUO)



b2
b7E

3. (U//FOUO)



b2
b7E

4. (U//FOUO)



b2
b7E

5. (U//FOUO)



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

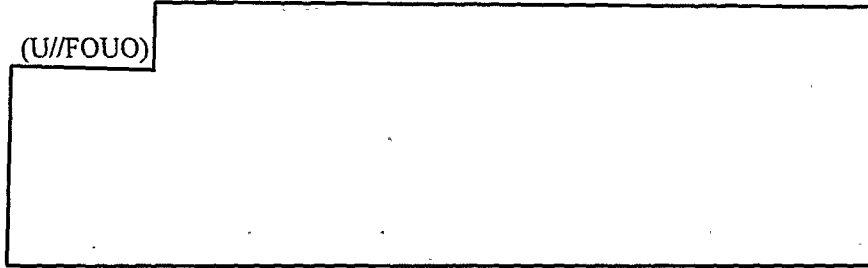
iii. (U//FOUO)

[Redacted]

b2
b7E

UNCLASSIFIED - FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

iv. (U//FOUO)



b2
b7E

b. (U//FOUO)



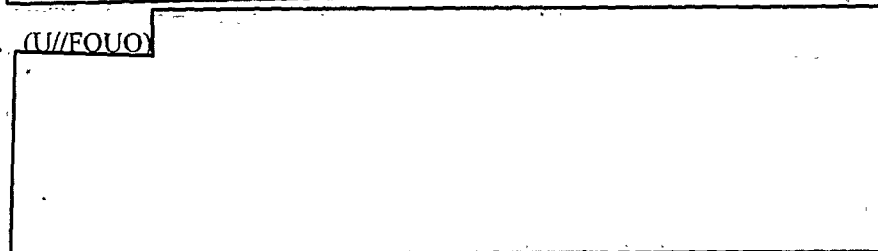
b2
b7E

i. (U//FOUO)



b2
b7E

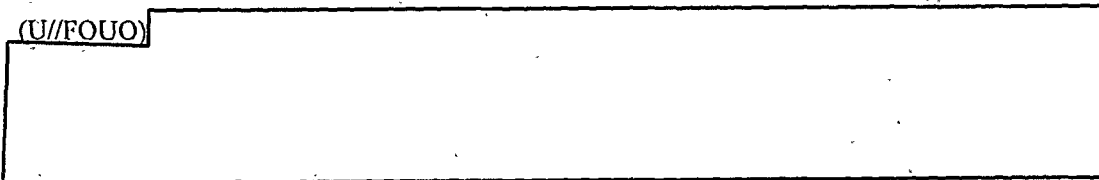
ii. (U//FOUO)



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)



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)

b2
b7E

c. (U//FOUO)

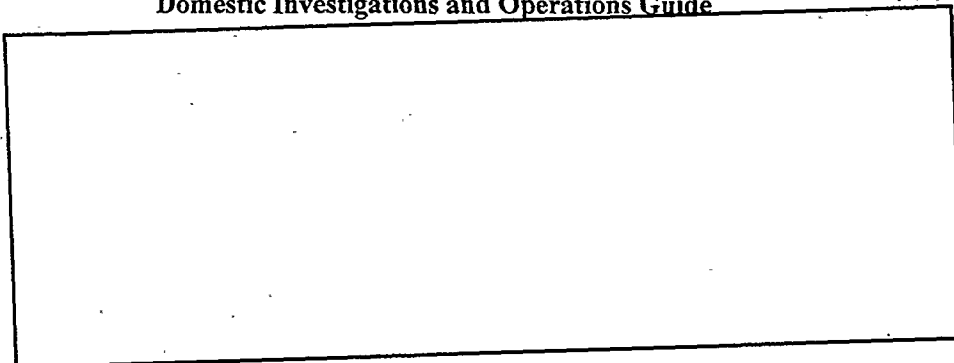
b2
b7E

☐ 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. ☐

(U//FOUO)

b2
b7E

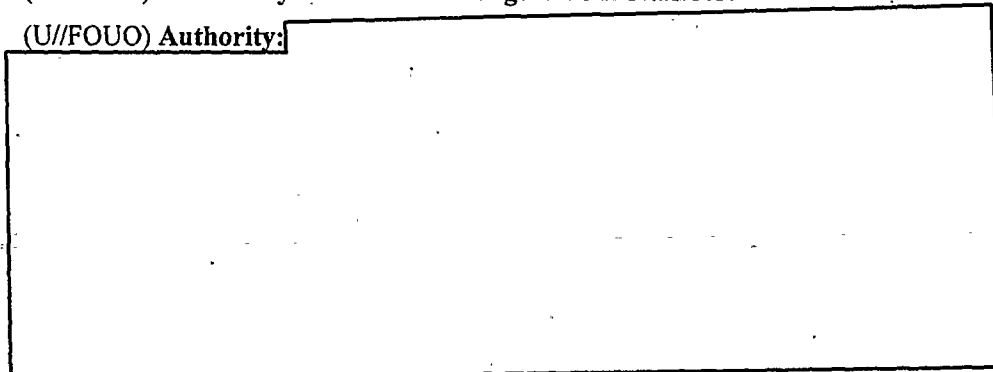
UNCLASSIFIED - FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide



b2
b7E

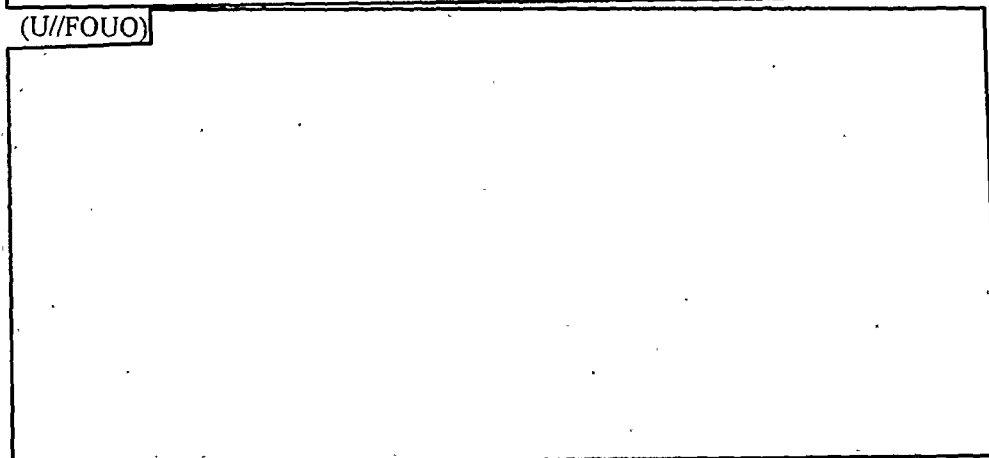
2. (U//FOUO) To Identify an Unknown Target Phone Number:

(U//FOUO) Authority:



b2
b7E

(U//FOUO)



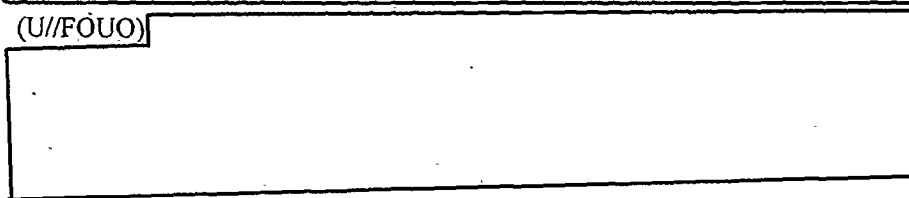
b2
b7E

a. (U//FOUO)



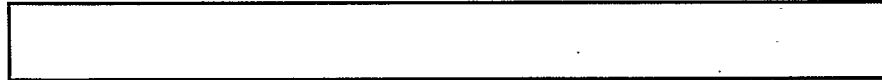
b2
b7E

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."