

**UNCLASSIFIED - FOR OFFICIAL USE ONLY**  
**Domestic Investigations and Operations Guide**

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

**11.12.1. (U) Summary**

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

**(U//FOUO) Application:**

b2  
b7E

**11.12.2. (U) Legal Authority**

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

**11.12.3. (U) Definition of Investigative Method**

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

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

**A. (U//FOUO) FISA**

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

**UNCLASSIFIED - FOR OFFICIAL USE ONLY**  
**Domestic Investigations and Operations Guide**

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

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

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

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

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

[redacted] at any time.

b2  
b7E

B. (U) Title III

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

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

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

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

**UNCLASSIFIED - FOR OFFICIAL USE ONLY**  
**Domestic Investigations and Operations Guide**

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

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

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

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

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

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

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

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

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

UNCLASSIFIED - FOR OFFICIAL USE ONLY  
Domestic Investigations and Operations Guide

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

b2  
b7E

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

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

(U//FOUO) [redacted]

b2  
b7E

**11.12.5. (U) Duration of Approval**

**A. (U) FISA**

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

**B. (U) Title III**

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

**11.12.6. (U) Specific Procedures**

**A. (U) FISA**

(U//FOUO) [redacted]

b2  
b7E

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

(U//FOUO) [redacted]

b2  
b7E

a. (U//FOUO) [redacted]

b2  
b7E

i. (U//FOUO) [redacted]

b2  
b7E

**UNCLASSIFIED - FOR OFFICIAL USE ONLY**  
**Domestic Investigations and Operations Guide**

ii. (U//FOUO)

[Redacted]

b2  
b7E

iii. (U//FOUO)

[Redacted]

b2  
b7E

b. (U//FOUO)

[Redacted]

b2  
b7E

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

(U//FOUO)

[Redacted]

b2  
b7E

a. (U//FOUO)

[Redacted]

b2  
b7E

b. (U//FOUO)

[Redacted]

b2  
b7E

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

(U//FOUO)

[Redacted]

b2  
b7E

a. (U//FOUO)

[Redacted]

b2  
b7E

b. (U//FOUO)

[Redacted]

b2  
b7E

UNCLASSIFIED - FOR OFFICIAL USE ONLY  
Domestic Investigations and Operations Guide

[Redacted]

b2  
b7E

c. (U//FOUO)

[Redacted]

b2  
b7E

d. (U//FOUO)

[Redacted]

b2  
b7E

(U//FOUO)

[Redacted]

b2  
b7E

B. (U) Title III

1. (U//FOUO) The requirements in 18 U.S.C. § 2518 must be followed meticulously in the preparation of a Title III application. In addition, the following points must be covered:
  - a. (U//FOUO) Probable cause must be current;
  - b. (U//FOUO) There must be a factual basis for concluding that normal investigative procedures have been tried and failed or a demonstration why these procedures appear to be unlikely to succeed or would be too dangerous if tried ("boilerplate" statements in this respect are unacceptable);
  - c. (U//FOUO) If the subscriber of the telephone on which coverage is sought is not one of the principals, attempts to identify the subscriber must be made;
  - d. (U//FOUO) Minimization will be occur, as statutorily required, if the coverage involves a public telephone booth, a restaurant table, or the like;
  - e. (U//FOUO) The facility or premises to be covered is described fully, [Redacted] and
  - f. (U//FOUO) At least 10 days prior to submitting the Title III request to DOJ OEO, the Field Office must forward an electronic communication to FBIHQ [Redacted]

b2  
b7E

b2  
b7E

**UNCLASSIFIED - FOR OFFICIAL USE ONLY**  
**Domestic Investigations and Operations Guide**

[Redacted]

b2  
b7E

2. (U//FOUO)

[Redacted]

b2  
b7E

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

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

[Redacted]

b2  
b7E

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

**11.12.7. (U) Notice and Reporting Requirements**

**A. (U) FISA**

(U//FOUO)

[Redacted]

b2  
b7E

**B. (U) Title III**

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

2. (U//FOUO)

[Redacted]

b2  
b7E

a. (U//FOUO)

[Redacted]

b2  
b7E

b. (U//FOUO)

[Redacted]

b2  
b7E

c. (U//FOUO)

[Redacted]

b2  
b7E

**UNCLASSIFIED - FOR OFFICIAL USE ONLY**  
**Domestic Investigations and Operations Guide**

3. (U//FOUO)

b2  
b7E

4. (U//FOUO)

b2  
b7E

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

**11.12.8. (U) Compliance and Monitoring**

**A. (U) FISA**

(U//FOUO)

b2  
b7E

**B. (U) Title III**

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

**11.12.9. (U) Special Circumstances**

**(U) FISA**

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

**11.12.10. (U) Other Applicable Policies**

**A. (U) FISA**

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

**B. (U//FOUO) OTD PG**

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

**UNCLASSIFIED - FOR OFFICIAL USE ONLY**  
**Domestic Investigations and Operations Guide**

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

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

**11.13.1. (U) Summary**

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

(U//FOUO) Application:

b2  
b7E

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

**11.13.2. (U) Legal Authority**

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

**11.13.3. (U) Definition of Investigative Method**

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

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

**UNCLASSIFIED - FOR OFFICIAL USE ONLY**  
**Domestic Investigations and Operations Guide**

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

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



b2  
b7E

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

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

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

**UNCLASSIFIED - FOR OFFICIAL USE ONLY**  
**Domestic Investigations and Operations Guide**

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

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

**1. (U) Anticipatory Warrants**

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

**2. (U) Sneak and peek search warrants**

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

**3. (U) Mail Openings**

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

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

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

**UNCLASSIFIED - FOR OFFICIAL USE ONLY**  
**Domestic Investigations and Operations Guide**

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

**11.13.4. (U) Approval Requirements for Investigative Method**

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

**11.13.5. (U) Duration of Approval**

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

**11.13.6. (U) Specific Procedures**

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

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

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

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

**UNCLASSIFIED - FOR OFFICIAL USE ONLY**  
**Domestic Investigations and Operations Guide**

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

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

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

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

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

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

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

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

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

**UNCLASSIFIED - FOR OFFICIAL USE ONLY**  
**Domestic Investigations and Operations Guide**

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

**UNCLASSIFIED - FOR OFFICIAL USE ONLY**  
**Domestic Investigations and Operations Guide**

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

**8. (U) Delayed Notice**

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

**B. (U) Obtaining a FISA Warrant**

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

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

**UNCLASSIFIED - FOR OFFICIAL USE ONLY**  
**Domestic Investigations and Operations Guide**

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

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

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

**UNCLASSIFIED - FOR OFFICIAL USE ONLY**  
**Domestic Investigations and Operations Guide**

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

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

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

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

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

**UNCLASSIFIED - FOR OFFICIAL USE ONLY**  
**Domestic Investigations and Operations Guide**

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

b2  
b7E

**4. (U) Special Circumstances**

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

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

**5. (U) Required Notice**

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

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

(U//FOUO) [redacted]

b2  
b7E

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

b2  
b7E

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

b2  
b7E

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

b2  
b7E

UNCLASSIFIED - FOR OFFICIAL USE ONLY  
Domestic Investigations and Operations Guide

iii. (U//FOUO)

[Redacted]

b2  
b7E

b. (U//FOUO)

[Redacted]

b2  
b7E

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

(U//FOUO) Each case file for which an application is or has been prepared for submission to the FISC will include a sub-file to be labeled [Redacted]

b2  
b7E

[Redacted] This sub-file is to contain copies of all applications to and orders issued by the FISC for the conduct of physical searches in the investigative case. The following data must be included in this [Redacted] [Redacted] [Redacted]

a. (U//FOUO)

[Redacted]

b2  
b7E

b. (U//FOUO)

[Redacted]

b2  
b7E

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

(U//FOUO)

[Redacted]

b2  
b7E

a. (U//FOUO)

[Redacted]

b2  
b7E

b. (U//FOUO)

[Redacted]

b2  
b7E

c. (U//FOUO)

[Redacted]

b2  
b7E

**UNCLASSIFIED - FOR OFFICIAL USE ONLY**  
**Domestic Investigations and Operations Guide**

[Redacted]

b2  
b7E

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

[Redacted]

b2  
b7E

(U//FOUO)

[Redacted]

b2  
b7E

**UNCLASSIFIED - FOR OFFICIAL USE ONLY**  
**Domestic Investigations and Operations Guide**

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

**11.14.1. (U) Summary**

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

**11.14.2. (U) Legal Authority**

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

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

**11.14.3. (U) Definition of Investigative Method**

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

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

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

**11.14.5. (U) Duration of Approval**

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

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

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

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

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

**UNCLASSIFIED - FOR OFFICIAL USE ONLY**  
**Domestic Investigations and Operations Guide**

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

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

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

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

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

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

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

**UNCLASSIFIED - FOR OFFICIAL USE ONLY**  
**Domestic Investigations and Operations Guide**

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

(U//FOUO)



b2  
b7E

UNCLASSIFIED - FOR OFFICIAL USE ONLY  
Domestic Investigations and Operations Guide

## 12. (U) Assistance to Other Agencies

### 12.1. (U) Overview

(U//FOUO) Part II of the AGG-Dom authorizes the FBI to conduct investigations in order to detect or obtain information about, and prevent and protect against, federal crimes and threats to the national security and to collect foreign intelligence. Part III of the AGG-Dom, Assistance to Other Agencies, authorizes the FBI to provide investigative assistance to other federal, state, local or tribal, or foreign agencies when the investigation has those same objectives or when the investigative assistance is legally authorized for other purposes. Accordingly, FBI employees may provide assistance even if it is not for one of the purposes identified as grounds for an FBI investigation or assessment, if providing the assistance is otherwise authorized by law. For example, investigative assistance is legally authorized in certain contexts to state or local agencies in the investigation of crimes under state or local law, as provided in 28 U.S.C. §§ 540—felonious killing of state and local law enforcement officer; 540A—violent crime against travelers; 540B—serial killings, and to foreign agencies in the investigation of foreign law violations pursuant to international agreements. The FBI may use appropriate lawful methods in any authorized investigative assistance activity.

### 12.2. (U) Purpose and Scope

- (U) The AGG-Dom permits FBI personnel to provide investigative assistance to:
- A. (U) Authorized intelligence activities of other USIC agencies;
  - B. (U) Any federal agency in the investigation of federal crimes, threats to the national security, foreign intelligence collection, or any other purpose that may be lawfully authorized;
  - C. (U) Assist the President in determining whether to use the armed forces pursuant to 10 U.S.C. §§ 331-33, when DOJ-authorized as described in Section 12.5.B.1.c, below;
  - D. (U) Collect information necessary to facilitate public demonstrations in order to protect the exercise of First Amendment rights and ensure public health and safety, when DOJ-authorized and within the restrictions described in Section 12.5.B.1.d, below;
  - E. (U) State or local agencies in the investigation of crimes under state or local law where authorized by federal law (e.g., 28 U.S.C. §§ 540—felonious killing of state and local law enforcement officer; 540A—violent crime against travelers; 540B—serial killings);
  - F. (U) State, local, or tribal agencies in the investigation of matters that may involve federal crimes or threats to national security, or for such other purposes as may be legally authorized; and
  - G. (U) Foreign agencies in the investigations of foreign law violations pursuant to international agreements, and as otherwise set forth below, consistent with the interests of the United States (including national security interests) and with due consideration of the effect on any United States person.
- (U) The FBI is further authorized to provide technical and scientific assistance to all duly constituted law enforcement agencies, other organizational units of the Department of Justice, and other federal agencies. 28 C.F.R. § 0.85(g). The FBI's authority and procedures for providing technical assistance is further set forth in Section 12.6 below.

**UNCLASSIFIED - FOR OFFICIAL USE ONLY**  
**Domestic Investigations and Operations Guide**

(U) Authorized investigative assistance by the FBI to other agencies includes participation in joint operations and activities with such agencies. (AGG-Dom, Part III.E.1) The procedures for providing investigative assistance, together with the approval and notification requirements, are provided below.

**12.3. (U//FOUO) Standards for Providing and Approving Investigative Assistance to Other Agencies**

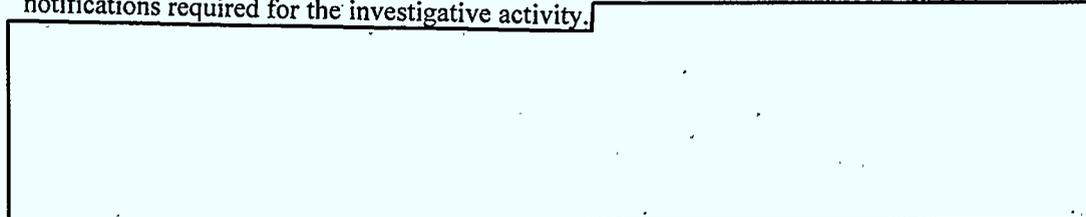
(U//FOUO) The determination of whether to provide FBI assistance to other agencies is both statutory and discretionary and must be based on consideration of the following factors:

- A. (U//FOUO) Assistance is within the scope authorized by the AGG-Dom;
- B. (U//FOUO) Assistance is not based solely on the exercise of First Amendment activities or on the race, ethnicity, national origin or religion of the subject; and
- C. (U//FOUO) Assistance is an appropriate use of personnel and financial resources.

**12.4. (U) Documentation, Record Retention and Dissemination**

**A. (U) Documentation**

(U//FOUO) When providing assistance to a domestic or foreign agency, the required documentation in an appropriate case file includes: (i) the name and type of agency; (ii) the investigative methods used; (iii) the opening and closing dates of the request; and (iv) notifications required for the investigative activity.



b2  
b7E

**B. (U) Records Retention for Assistance Furnished to Another Agency**

(U//FOUO) A database of records created with the [redacted] is maintained to permit the prompt retrieval of the status of the assistance activity (opened or closed), the dates of opening and closing, and the basis for the assistance activity. (AGG-Dom, Part III.E.3)

b2  
b7E

**C. (U) Dissemination of Information**

(U//FOUO) For unclassified information, the [redacted] should be used to document the dissemination of information to: (i) United States Intelligence Community Agencies; (ii) United States Federal Agencies; (iii) State, Local, or Tribal Agencies; and (iv) Foreign Agencies. Dissemination to Foreign Agencies must be in accordance with the FBI Foreign Dissemination Manual, dated May 23, 2008. Classified information must be disseminated pursuant to applicable federal law, Presidential directive, Attorney General policy and FBI policy.

b2  
b7E

**12.5. (U) Duration, Approval and Notice for Investigative Assistance to Other Agencies**

(U//FOUO) Investigative assistance that may be furnished to other agencies is described below by agency type. Dissemination of information to other agencies must be consistent with Director

**UNCLASSIFIED - FOR OFFICIAL USE ONLY**  
**Domestic Investigations and Operations Guide**

of National Intelligence directives, the AGG-Dom, DIOG Section 14, FBI Foreign Dissemination Manual, and any applicable MOU/MOA, law, treaty or other policy.

(U//FOUO) **Sensitive Investigative Matter:** Any assistance to other agencies involving a sensitive investigative matter requires CDC review, SAC approval, and notification to the appropriate FBIHQ substantive Unit Chief and Section Chief. (If assistance is to a foreign agency, notification to the Office of International Operations (OIO) Unit Chief and Section Chief is also required.) Additionally, FBIHQ must provide notice to the DOJ Criminal Division or NSD as soon as practicable, but not later than 30 calendar days after the initiation of any assistance involving a sensitive investigative matter (see classified appendix for additional notice requirements).

**A. (U) United States Intelligence Community Agencies**

**1. (U) Authority**

(U//FOUO) The FBI may provide investigative assistance (including operational support) to authorized intelligence activities of other USIC agencies. (AGG-Dom, Part III.A.) Investigative assistance must be in compliance with interagency memoranda of understanding/agreement, if applicable. For example, specific approval and notification requirements exist for CIA domestic activities.

**2. (U) Approval**

(U//FOUO) Prior SSA approval is required for providing assistance to the USIC when the assistance uses investigative methods beyond those authorized in assessments. Assistance to other agencies using an investigative method authorized only for predicated investigations requires supervisory approval at the same level required for the respective investigative method if used in an FBI investigation. Specifically, higher supervisory approval and notification requirements may exist for conducting a joint operation (e.g., investigative operations with the Department of Defense [DoD], Department of Homeland Security), a sensitive investigative matter, and using particular investigative methods as noted in Sections 10 and 11, and the Division policy guides. Assistance for investigative methods beyond those authorized in assessments must be documented in the FD-999. Approval for use of specific technologies is set forth in Section 12.6 below and the OTD Manual.

**B. (U) United States Federal Agencies**

**1. (U) Authorities**

- a. (U//FOUO) The FBI may provide assistance to any other federal agency in the investigation of federal crimes or threats to the national security or in the collection of positive foreign intelligence. (Pursuant to Section 9, collection of positive foreign intelligence requires prior approval from FBIHQ CMS.) The FBI may provide investigative assistance to any federal agency for any other purpose that may be legally authorized, including investigative assistance to the Secret Service in support of its protective responsibilities. (AGG-Dom, Part III.B.1) See DIOG Section 12.6 below for guidance in providing technical assistance to federal agencies.

**UNCLASSIFIED - FOR OFFICIAL USE ONLY**  
**Domestic Investigations and Operations Guide**

- b. (U//FOUO) The FBI must follow MOU/MOA with other federal agencies where applicable. Specific approval and notification requirements exist for CIA and DoD domestic activities.
- c. (U) **Actual or Threatened Domestic Civil Disorders**
  - i. (U) At the direction of the Attorney General, the Deputy Attorney General, or the Assistant Attorney General for the Criminal Division, the FBI shall collect information relating to actual or threatened civil disorders to assist the President in determining (pursuant to the authority of the President under 10 U.S.C. §§ 331-33) whether use of the armed forces or militia is required and how a decision to commit troops should be implemented. The information sought shall concern such matters as: (AGG-Dom, Part III.B.2)
    - (a) (U) The size of the actual or threatened disorder, both in number of people involved or affected and in a geographic area;
    - (b) (U) The potential for violence;
    - (c) (U) The potential for expansion of the disorder in light of community conditions and underlying causes of the disorder;
    - (d) (U) The relationship of the actual or threatened disorder to the enforcement of federal law or court orders and the likelihood that state or local authorities will assist in enforcing those laws or orders; and
    - (e) (U) The extent of state or local resources available to handle the disorder.
  - ii. (U) Civil disorder investigations will be authorized only for a period of 30 days, but the authorization may be renewed for subsequent 30 day periods.
  - iii. (U) The only investigative methods that may be used during a civil disorder investigation are:
    - (a) (U) Obtain publicly available information;
    - (b) (U) Access and examine FBI and other DOJ records, and obtain information from any FBI or other DOJ 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 nonprofit or commercial);
    - (e) (U) Interview members of the public and private entities; and  
(U//FOUO) **Note:** Such interviews may only be conducted if the FBI employee identifies himself or herself as an FBI employee and accurately discloses the purpose of the interview.
    - (f) (U) Accept information voluntarily provided by governmental or private entities.

**UNCLASSIFIED - FOR OFFICIAL USE ONLY**  
**Domestic Investigations and Operations Guide**

(U) Other methods may be used only if authorized by the Attorney General, the Deputy Attorney General, or the Assistant Attorney General for the Criminal Division.

d. (U) **Public Health and Safety Authorities in Relation to Demonstrations**

- i. (U) At the direction of the Attorney General, the Deputy Attorney General, or the Assistant Attorney General for the Criminal Division, the FBI shall collect information relating to demonstration activities that are likely to require the federal government to take action to facilitate the activities and provide public health and safety measures with respect to those activities. The information sought in such an investigation shall be that needed to facilitate an adequate federal response to ensure public health and safety and to protect the exercise of First Amendment rights, such as:
    - (a) (U) The time, place, and type of activities planned.
    - (b) (U) The number of persons expected to participate.
    - (c) (U) The expected means and routes of travel for participants and expected time of arrival.
    - (d) (U) Any plans for lodging or housing of participants in connection with the demonstration.
  - ii. (U) The only investigative methods that may be used in an investigation under this paragraph are:
    - (a) (U) Obtain publicly available information;
    - (b) (U) Access and examine FBI and other DOJ records, and obtain information from any FBI or other DOJ 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 nonprofit or commercial);
    - (e) (U) Interview of members of the public and private entities; and  
(U//FOUO) Note: Such interviews may only be conducted if the FBI employee identifies himself or herself as an FBI employee and accurately discloses the purpose of the interview.
    - (f) (U) Accept information voluntarily provided by governmental or private entities.
- (U) Other methods may be used only if authorized by the Attorney General, the Deputy Attorney General, or the Assistant Attorney General for the Criminal Division.

2. (U) **Approval**

(U//FOUO) Prior SSA approval is required for assistance to another federal agency when the assistance uses investigative methods beyond those authorized in assessments.

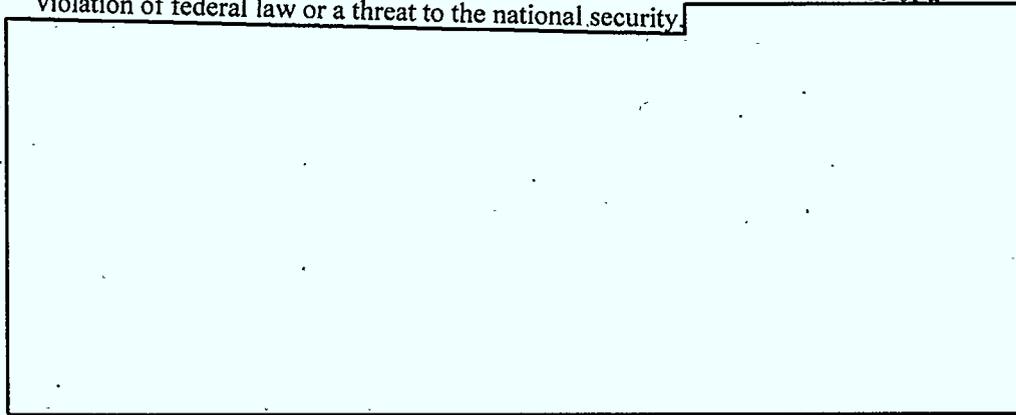
**UNCLASSIFIED - FOR OFFICIAL USE ONLY**  
**Domestic Investigations and Operations Guide**

Assistance to other agencies using an investigative method authorized only for predicated investigations requires supervisory approval at the same level required for the respective investigative method if used in an FBI investigation, as provided in Section 11. Specifically, higher supervisory approval and notification requirements may exist for conducting a joint operation, a sensitive investigative matter, and using particular investigative methods, as noted in Sections 10 and 11 and in the Division policy guides. Assistance for investigative methods beyond those authorized in assessments must be documented in the FD-999. Approval for use of specific technologies is set forth in Section 12.6, below and the OTD Manual.

**C. (U) State, Local, or Tribal Agencies**

**1. (U) Authorities**

- a. (U) The FBI may provide investigative assistance to state, local, or tribal agencies in the investigation of matters that may involve federal crimes or threats to the national security, or for other legally authorized purposes. Legally authorized purposes include, but are not limited to, a specific federal statutory grant of authority such as that provided by 28 U.S.C. §§ 540—felonious killing of state and local law enforcement officer; 540A—violent crime against travelers; 540B—serial killings. (AGG-Dom, Part III.C) The FBI is further authorized to provide other material, scientific and technical assistance to state, local, and tribal agencies. (See 28 C.F.R. § 0.85[g] and DIOG Section 12.6, below.)
- b. (U//FOUO) The FBI must follow applicable MOU/MOA and/or treaties when it provides assistance to state, local, and tribal agencies.
- c. (U//FOUO) As a federal agency, the FBI's authority to investigate criminal offenses derives from federal statutes and is generally limited to violations of federal law. See 18 U.S.C. § 3052, 28 U.S.C. § 533 (1) and 28 C.F.R. § 0.85. With limited exceptions, such as those cited in Section 12.2.E., above, the FBI does not have any federal authority to investigate state crimes. FBI employees can assist in the investigation of other criminal matters with state and local authorities only if there is a reasonable basis to believe that the investigation will prevent, detect or lead to evidence of a violation of federal law or a threat to the national security.



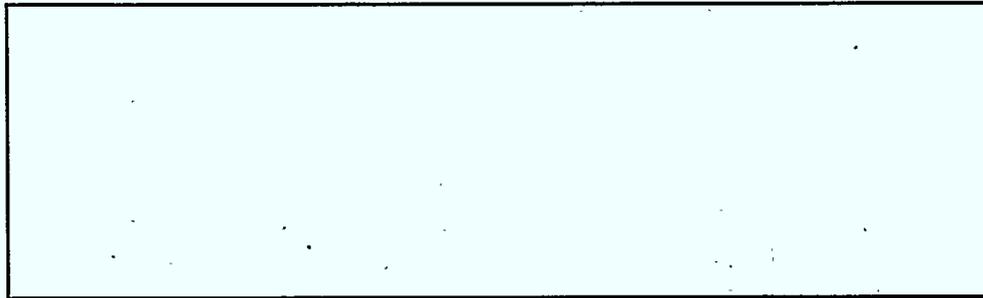
b2  
b7E

**d. (U//FOUO)**



b2  
b7E

UNCLASSIFIED - FOR OFFICIAL USE ONLY  
Domestic Investigations and Operations Guide



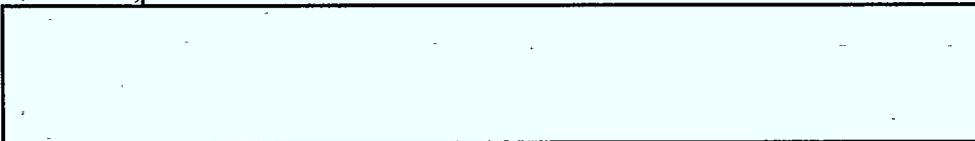
b2  
b7E

e. (U//FOUO) [Redacted]



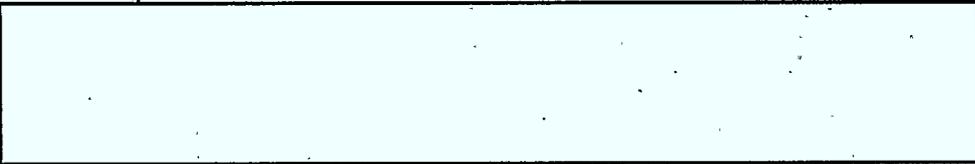
b2  
b7E

f. (U//FOUO) [Redacted]



b2  
b7E

g. (U//FOUO) [Redacted]



b2  
b7E

h. (U//FOUO) [Redacted]



b2  
b7E

i. (U//FOUO) When credible information is received by an FBI employee concerning serious criminal activity not within the FBI's investigative jurisdiction, the FBI employee must promptly transmit the information or refer the complainant to a law enforcement agency having jurisdiction, except when disclosure would jeopardize an ongoing investigation, endanger the safety of an individual, disclose the identity of a human source, interfere with a human source's cooperation, or reveal legally privileged information. If full disclosure is not made for any of the reasons indicated, then, whenever feasible, the FBI employee must make at least limited disclosure to a law enforcement agency or agencies having jurisdiction, and full disclosure must be made as soon as the need for restricting the information is no longer present. Where

**UNCLASSIFIED - FOR OFFICIAL USE ONLY**  
**Domestic Investigations and Operations Guide**

disclosure is not made to the appropriate law enforcement agencies within 180 days, the FBI employee/Field Office must notify the appropriate substantive Unit at FBI Headquarters in writing concerning the facts and circumstances concerning the criminal activity. FBI Headquarters is required to make periodic reports to the Deputy Attorney General on such non-disclosure and incomplete disclosures. (AGG-Dom, Part VI.C.2)

**2. (U) Approval**

(U//FOUO) Prior SSA approval is required for assistance to state, local, or tribal agencies when the assistance uses investigative methods beyond those authorized in assessments. Assistance to other agencies using an investigative method authorized only for predicated investigations requires supervisory approval at the same level required for the respective investigative method if used in an FBI investigation. Specifically, higher supervisory approval and notification requirements may exist for conducting a joint operation, a sensitive investigative matter, and using particular investigative methods, as noted in Sections 10 and 11 and in the Division policy guides. Assistance for investigative methods beyond those authorized in assessments must be documented in the FD-999. Approval for use of specific technologies is set forth in Section 12.6, below and the OTD Manual.

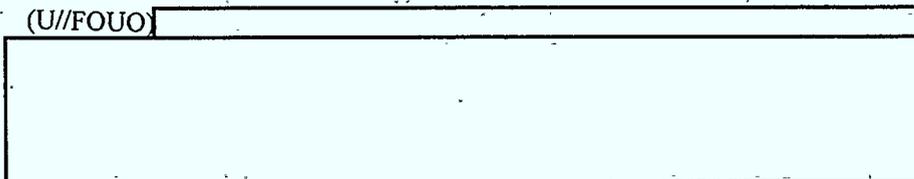
**D: (U) Foreign Agencies**

1. (U//FOUO) **General:** The foundation of the FBI's international program is the Legat. Each Legat is the Director's personal representative in the foreign countries in which he/she resides or has regional responsibilities. The Legat's job is to respond to the FBI's domestic and foreign investigative needs. The Legat can accomplish this because he or she has developed partnerships and fostered cooperation with his or her foreign counterparts on every level and is familiar with investigative rules, protocols, and practices that differ from country to country. This is the Legat's primary responsibility. As such, foreign agency requests for assistance will likely come to the FBI through the Legat. If, however, foreign agency requests for assistance bypass the Legat, the FBI employee must notify the Legat and OIO, as discussed in greater detail below.

**2. (U) Authorities**

a. (U//FOUO) At the request of foreign law enforcement, intelligence, or security agencies, the FBI may conduct investigations or provide assistance to investigations by such agencies, consistent with the interests of the United States (including national security interests) and with due consideration of the effect on any United States person. (AGG-Dom, Part III.D.1) The FBI must follow applicable MOUs, MOAs, Mutual Legal Assistance Treaties (MLAT) and other treaties when it provides assistance to foreign governments.

i. (U//FOUO)



b2  
b7E

**UNCLASSIFIED - FOR OFFICIAL USE ONLY**  
**Domestic Investigations and Operations Guide**

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

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

c. (U//FOUO) The FBI may not provide assistance to foreign law enforcement, intelligence, or security officers conducting investigations within the United States unless such officers have provided prior written notification to the Attorney General of their status as an agent of a foreign government, as required by 18 U.S.C. § 951. (AGG-Dom, Part III.D.2) The notification required by 18 U.S.C. § 951 is not applicable to diplomats, consular officers or attachés.

d. (U//FOUO) Upon the request of a foreign government agency, the FBI may conduct background inquiries concerning individuals whose consent is documented. (AGG-Dom, Part III.D.3)

e. (U//FOUO) The AGG-Dom, Part III.D.4 authorizes the FBI to provide other material and technical assistance to foreign governments to the extent not otherwise prohibited by law. AG Order 2954-2008 authorizes the FBI to provide technical assistance to foreign governments, as referenced below in Section 12.6.

3. (U) Approval

a. (U//FOUO) Prior SSA approval is required for all assistance to foreign agencies. All assistance must be documented in the FD-999 and that approval should be documented in the file.

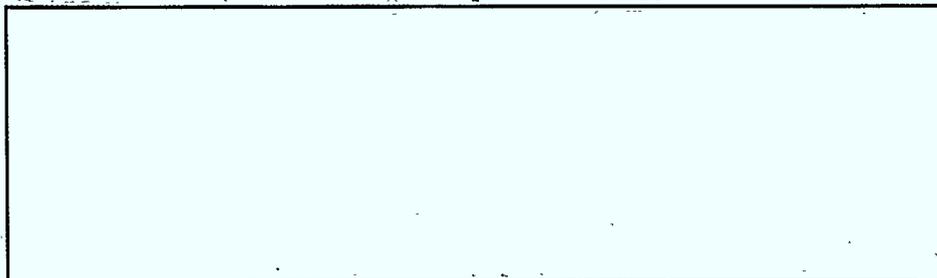
b. (U//FOUO) [Redacted] b2  
[Redacted] b7E

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

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

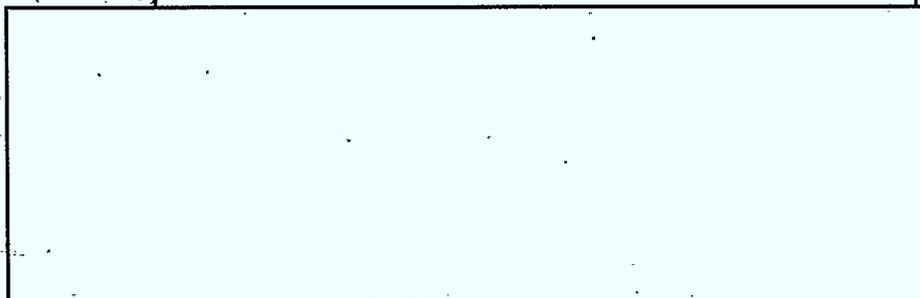
[Redacted] b2  
[Redacted] b7E

**UNCLASSIFIED - FOR OFFICIAL USE ONLY**  
**Domestic Investigations and Operations Guide**



b2  
b7E

ii. (U//FOUO)



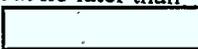
b2  
b7E

4. (U) Notice

a. (U//FOUO)



b2  
b7E

b. (U) The FBI must notify the DOJ NSD concerning investigation or assistance where both: (i) FBIHQs approval for the activity is required (e.g., FBIHQ approval required to use a particular investigative method); and (ii) the activity relates to a threat to the United States national security. The FBIHQ Division approving the use of the investigative method must notify DOJ NSD as soon as practicable, but no later than 30 calendar days after FBIHQ approval (see classified appendix for ). (AGG-Dom, Part III.D.1)

b2  
b7E

5. (U) Dissemination

(U//FOUO) All dissemination of FBI information to foreign agencies must be conducted according to the FBI Foreign Dissemination Manual, dated May 23, 2008

12.6. (U//FOUO) Standards for Providing and Approving Technical Assistance to Foreign, State, Local and Tribal Agencies

A. (U) Authority

1. (U//FOUO)



b2  
b7E

UNCLASSIFIED - FOR OFFICIAL USE ONLY  
Domestic Investigations and Operations Guide

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

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

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

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

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

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

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

B. (U) Approval

(U//FOUO) All technical assistance must be approved by the Director or his designated senior executive FBI official, as provided in the OTD manual. All technical assistance must be documented in an FBI assessment file, predicated investigation file, a domestic police cooperation file, a foreign police cooperation file, or other investigative/technical assistance control file. Additionally, all technical assistance must be documented in the FD-999 or its successor.

### 13. (U) Extraterritorial Provisions

#### 13.1. (U) Overview

(U//FOUO) The FBI may conduct investigations abroad, participate with foreign officials in investigations abroad, or otherwise conduct activities outside the United States. The guidelines for conducting investigative activities outside of the United States are currently contained in: (i) *The Attorney General's Guidelines for Extraterritorial FBI Operations and Criminal Investigations*; (ii) *The Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection*; and (iii) *The Attorney General Guidelines on the Development and Operation of FBI Criminal Informants and Cooperative Witnesses in Extraterritorial Jurisdictions* (collectively, the Extraterritorial Guidelines). The *Attorney General's Guidelines for Extraterritorial FBI Operations* are currently being drafted, as discussed in DIOG Section 2.1, and will supercede the above listed guidelines, or applicable provisions thereof.

#### 13.2. (U) Purpose and Scope

(U//FOUO) As a general rule, the Extraterritorial Guidelines apply when FBI personnel or confidential human sources are actively engaged in investigative activity outside the borders of the United States.

[Redacted]

b2  
b7E

A. (U//FOUO) [Redacted]

b2  
b7E

B. (U//FOUO) [Redacted]

b2  
b7E

C. (U//FOUO) [Redacted]

b2  
b7E

D. (U//FOUO) [Redacted]

b2  
b7E

E. (U//FOUO) [Redacted]

b2  
b7E

F. (U//FOUO) [Redacted]

b2  
b7E

G. (U//FOUO) [Redacted]

b2  
b7E

H. (U//FOUO) [Redacted]

b2  
b7E

I. (U//FOUO) [Redacted]

b2  
b7E

J. (U//FOUO) [Redacted]

b2  
b7E

**UNCLASSIFIED - FOR OFFICIAL USE ONLY**  
**Domestic Investigations and Operations Guide**

(U//FOUO) FBI personnel planning to engage in any of the investigative activities described in the subsection above must obtain the concurrence of the appropriate Legat and must comply with the remaining procedural requirement of the Extraterritorial Guidelines. For additional information consult the Extraterritorial Section of the OGC website.

**13.3. (U) Legal Attache Program**

(U//FOUO) The foundation of the FBI's international program is the Legat. Each Legat is the Director's personal representative in the foreign countries in which he/she resides or has regional responsibilities. The Legat's job is to respond to the FBI's domestic and extraterritorial investigative needs. Legats can accomplish this mission because they have developed partnerships and fostered cooperation with their foreign counterparts on every level and are familiar with local investigative rules, protocols, and practices which differ from country to country. For additional information consult the FBIHQ OIO website.

UNCLASSIFIED - FOR OFFICIAL USE ONLY  
Domestic Investigations and Operations Guide

## 14. (U) Retention and Sharing of Information

---

### 14.1. (U) Purpose and Scope

(U//FOUO) Every FBI component is responsible for the creation and maintenance of authentic, reliable, and trustworthy records. Without complete and accessible records, the FBI cannot conduct investigations, gather and analyze intelligence, assist with the prosecution of criminals, or perform any of its critical missions effectively.

(U//FOUO) The FBI is committed to ensuring that its records management program accomplishes the following goals:

- A. (U//FOUO) Facilitates the documentation of official decisions, policies, activities, and transactions;
- B. (U//FOUO) Facilitates the timely retrieval of needed information;
- C. (U//FOUO) Ensures continuity of FBI business;
- D. (U//FOUO) Controls the creation and growth of FBI records;
- E. (U//FOUO) Reduces operating costs by managing records according to FBI business needs and by disposing of unneeded records in a timely manner;
- F. (U//FOUO) Improves efficiency and productivity through effective records storage and retrieval methods;
- G. (U//FOUO) Ensures compliance with applicable laws and regulations;
- H. (U//FOUO) Safeguards the FBI's mission-critical information;
- I. (U//FOUO) Preserves the FBI's corporate memory and history; and
- J. (U//FOUO) Implements records management technologies to support all of the goals listed above.

### 14.2. (U) The FBI's Records Retention Plan, and Documentation

(U//FOUO) The FBI must retain records relating to investigative activities according to a records retention plan approved by the NARA. (AGG-Dom, Part VI.A.1)

(U//FOUO) The FBI's disposition authorities provide specific instructions about the length of time that records must be maintained. In some instances, records may be destroyed after a prescribed period of time has elapsed. Other records are never destroyed and are transferred to NARA a certain number of years after a case was closed.

- A. (U//FOUO) The FBI must maintain a database or records system that permits, with respect to each predicated investigation, the prompt retrieval of the status of the investigation (open or closed), the dates of opening and closing, and the basis for the investigation. (AGG-Dom, Part VI.A.2)

(U//FOUO) The FBI has updated its official File Classification System to cover records related to all investigative and intelligence collection activities, including assessments. Records are maintained in the FBI's Central Records System or other designated systems of records, that provide the required maintenance and retrieval functionality.

**UNCLASSIFIED - FOR OFFICIAL USE ONLY**  
**Domestic Investigations and Operations Guide**

- B. (U//FOUO) Assessments must also adhere to the standards as set forth in the Records Management Division Disposition Plan and Retention Plan. All records, including assessments, may be destroyed or expunged earlier than the destruction schedule through proper authority.

(U//FOUO) All Bureau records are maintained for their full retention periods, except under certain circumstances under which they may be either destroyed earlier or retained longer. Records may be retained for a longer period than their disposition authority specifies, if they are subject to a litigation freeze. Court orders may direct that certain records be expunged from a case file, or (more rarely) that the entire case file be expunged. Under certain circumstances, individuals may also request that certain records be expunged. Expungement of records may mean the physical removal and destruction of some or all of the record or, depending on the court order and the governing statute or program, it may mean the removal, sealing, and secure storage of records away from the remaining file. In most instances, only certain documents, not the entire file, are subject to expungement.

**14.3. (U) Information Sharing**

(U//FOUO) The FBI 2008 National Information Sharing Strategy (NISS) provides the common vision, goals, and framework needed to guide information sharing initiatives with our federal, state, local, and tribal agency partners; foreign government counterparts, and private sector stakeholders. The FBI NISS addresses the cultural and technological changes required to move the FBI to "a responsibility to provide" culture. This will be accomplished by using the best practices and technology standards of both communities as we support the intelligence and law enforcement communities in collection, dissemination, analysis, collaboration, and operational efforts.

**A. (U) Permissive Sharing**

(U//FOUO) Consistent with the Privacy Act and any other applicable laws and memoranda of understanding or agreement with other agencies concerning the dissemination of information, the FBI may disseminate information obtained or produced through activities under the AGG-Dom:

1. (U//FOUO) Within the FBI and to all other components of the Department of Justice if the recipients have need of the information in the performance of their official duties.
2. (U//FOUO) To other federal agencies if disclosure is compatible with the purpose for which the information was collected and it is related to their responsibilities. In relation to other USIC agencies, the determination whether the information is related to the recipient responsibilities may be left to the recipient.
3. (U//FOUO) To state, local, or Indian tribal agencies directly engaged in the criminal justice process where access is directly related to a law enforcement function of the recipient agency.
4. (U//FOUO) To congressional committees as authorized by the DOJ Office of Legislative Affairs.
5. (U//FOUO) To foreign agencies if the FBI determines that the information is related to their responsibilities; the dissemination is consistent with the interests of the United

**UNCLASSIFIED - FOR OFFICIAL USE ONLY**  
**Domestic Investigations and Operations Guide**

States (including national security interests); and where the purpose of the disclosure is compatible with the purpose for which the information was collected.

6. (U//FOUO) If the information is publicly available, does not identify United States persons, or is disseminated with the consent of the person whom it concerns.
7. (U//FOUO) If the dissemination is necessary to protect the safety or security of persons or property, to protect against or prevent a crime or imminent threat to the national security, or to obtain information for the conduct of an authorized FBI investigation.
8. (U//FOUO) If dissemination of the information is otherwise permitted by the Privacy Act (5 U.S.C. § 552a) (AGG-Dom, Part VI.B.1)

(U//FOUO) All FBI information sharing activities under this section shall be according to Corporate Policy Directive 12D, "FBI Sharing Activities with Other Government Agencies," 95D "Protecting Privacy in the Information Sharing Environment," and any amendments thereto and applicable succeeding policy directives.

**B. (U) Required Sharing**

(U//FOUO) The FBI must share and disseminate information as required by statutes, treaties, Executive Orders, Presidential directives, National Security Council directives, Homeland Security Council directives, DNI directives, Attorney General-approved policies, and MOUs or MOAs, as consistent with the Privacy Act.

**14.4. (U) Information Related to Criminal Matters**

**A. (U) Coordinating with Prosecutors**

(U//FOUO) In an investigation relating to possible criminal activity in violation of federal law, the FBI employee conducting the investigation must maintain periodic written or oral contact with the appropriate federal prosecutor, as circumstances warrant and as requested by the prosecutor. When, during such an investigation, a matter appears arguably to warrant prosecution, the FBI employee must present the relevant facts to the appropriate federal prosecutor. Information on investigations that have been closed must be available on request to a United States Attorney or his or her designee or an appropriate Department of Justice official. (AGG-Dom, Part VI.C)

**B. (U) Criminal Matters Outside FBI Jurisdiction**

(U//FOUO) When credible information is received by an FBI employee concerning serious criminal activity not within the FBI's investigative jurisdiction, the FBI employee must promptly transmit the information or refer the complainant to a law enforcement agency having jurisdiction, except where disclosure would jeopardize an ongoing investigation, endanger the safety of an individual, disclose the identity of a CHS, interfere with the cooperation of a CHS, or reveal legally privileged information. If full disclosure is not made for the reasons indicated, then, whenever feasible, the FBI employee must make at least limited disclosure to a law enforcement agency or agencies having jurisdiction, and full disclosure must be made as soon as the need for restricting disclosure is no longer present. Where full disclosure is not made to the appropriate law enforcement agencies within 180 days, the FBI employee/Field Office must promptly notify FBIHQ in writing of the facts and circumstances concerning the criminal activity. The FBI must make periodic reports to the

**UNCLASSIFIED - FOR OFFICIAL USE ONLY**  
**Domestic Investigations and Operations Guide**

Deputy Attorney General on such non-disclosures and incomplete disclosures, in a form suitable to protect the identity of a CHS. (AGG-Dom, Part VI.C)

**C. (U) Reporting of Criminal Activity**

(U//FOUO) When it appears that an FBI employee has engaged in criminal activity in the course of an investigation under the AGG-Dom, the FBI must notify the USAO or an appropriate DOJ Division. When it appears that a CHS has engaged in criminal activity in the course of an investigation under the AGG-Dom, the FBI must proceed as provided in the AGG-CHS. When information concerning possible criminal activity by any other person appears in the course of an investigation under the AGG-Dom, the FBI must initiate an investigation of the criminal activity if warranted. (AGG-Dom, Part VI.C.3)

(U//FOUO) The reporting requirements under this paragraph relating to criminal activity by an FBI employee or a CHS do not apply to otherwise illegal activity that is authorized in conformity with the AGG-Dom or other Attorney General guidelines or to minor traffic offenses. (AGG-Dom, Part VI.C.3)

**14.5. (U) Information Related to National Security and Foreign Intelligence Matters**

(U//FOUO) All information sharing with a foreign government related to classified national security and foreign intelligence must adhere to the FBI Foreign Dissemination Manual effective 05/23/2008 and effective policies governing MOUs.

(U//FOUO) The general principle reflected in current law and policy is that there is a responsibility to provide information as consistently and fully as possible to agencies with relevant responsibilities to protect the United States and its people from terrorism and other threats to the national security, except as limited by specific constraints on such sharing. The FBI's responsibility in this area includes carrying out the requirements of the MOU Between the Intelligence Community, Federal Law Enforcement Agencies, and the Department of Homeland Security Concerning Information Sharing (March 4, 2003), or any successor memorandum of understanding or agreement. Specific requirements also exist for internal coordination and consultation with other DOJ components, and for sharing national security and foreign intelligence information with White House agencies, as provided in the ensuing paragraphs. (AGG-Dom, Part VI.D)

**(U) Department of Justice**

- A. (U//FOUO) The DOJ NSD must have access to all information obtained by the FBI through activities relating to threats to the national security or foreign intelligence. The Director of the FBI and the Assistant Attorney General for National Security must consult concerning these activities whenever requested by either of them, and the FBI must provide such reports and information concerning these activities as the Assistant Attorney General for National Security may request. In addition to any reports or information the Assistant Attorney General for National Security may specially request under this subparagraph, the FBI must provide annual reports to the NSD concerning its foreign intelligence collection program, including information concerning the scope and nature of foreign intelligence collection activities in each FBI Field Office. (AGG-Dom, Part VI.D.1)
- B. (U//FOUO) The FBI must keep the NSD apprised of all information obtained through activities under the AGG-Dom that is necessary to the ability of the United States to investigate or protect against threats to the national security, that includes regular

**UNCLASSIFIED - FOR OFFICIAL USE ONLY**  
**Domestic Investigations and Operations Guide**

consultations between the FBI and the NSD to exchange advice and information relevant to addressing such threats through criminal prosecution or other means. (AGG-Dom, Part VI.D.1)

- C. (U//FOUO) Except for counterintelligence investigations, a relevant USAO must have access to and must receive information from the FBI relating to threats to the national security, and may engage in consultations with the FBI relating to such threats, to the same extent as the NSD. The relevant USAO must receive such access and information from the FBI Field Offices. (AGG-Dom, Part VI.D.1)
- D. (U//FOUO) In a counterintelligence investigation – e.g., an investigation relating to a matter described in Part VII.S.2 of the AGG-Dom – the FBI's providing information to and consultation with a relevant USAO is subject to authorization by the NSD. In consultation with the Executive Office for United States Attorneys and the FBI, the NSD must establish policies setting forth circumstances in which the FBI will consult with the NSD prior to informing a relevant USAO about such an investigation. The policies established by the NSD must (among other things) provide that:
1. (U//FOUO) The NSD will, within 30 days, authorize the FBI to share with the USAO information relating to certain espionage investigations, as defined by the policies, unless such information is withheld because of substantial national security considerations; and
  2. (U//FOUO) The FBI may consult freely with the USAO concerning investigations within the scope of this subparagraph during an emergency, so long as the NSD is notified of such consultation as soon as practicable after the consultation. (AGG-Dom, Part VI.D.1)
- E. (U//FOUO) Information shared with a USAO pursuant to DIOG subparagraph 14.5 (National Security) must be disclosed only to the United States Attorney or any AUSA designated by the United States Attorney as points of contact to receive such information. The United States Attorney and designated AUSA must have an appropriate security clearance and must receive training in the handling of classified information and information derived from FISA, including training concerning the secure handling and storage of such information and training concerning requirements and limitations relating to the use, retention, and dissemination of such information. (AGG-Dom, Part VI.D.1)
- F. (U//FOUO) The disclosure and sharing of information by the FBI under this paragraph is subject to any limitations required in orders issued by the FISC, controls imposed by the originators of sensitive material, and restrictions established by the Attorney General or the Deputy Attorney General in particular cases. The disclosure and sharing of information by the FBI under this paragraph that may disclose the identity of a CHS is governed by the relevant provisions of the AGG-CHS. (AGG-Dom, Part VI.D.1)

**(U) White House**

(U//FOUO) In order to carry out their responsibilities, the President, the Vice President, the Assistant to the President for National Security Affairs, the Assistant to the President for Homeland Security Affairs, the National Security Council (NSC) and its staff, the Homeland Security Council (HSC) and its staff, and other White House officials and offices require information from all federal agencies, including foreign intelligence, and information relating to international terrorism and other threats to the national security. The FBI accordingly may

**UNCLASSIFIED - FOR OFFICIAL USE ONLY**  
**Domestic Investigations and Operations Guide**

disseminate to the White House foreign intelligence and national security information obtained through activities under the AGG-Dom, subject to the following standards and procedures.

- A. (U//FOUO) White House must request such information through the NSC staff or HSC staff including, but not limited to, the NSC Legal and Intelligence Directorates and Office of Combating Terrorism, or through the President's Intelligence Advisory Board or the Counsel to the President. (AGG-Dom, Part VI.D.2.a)

(U//FOUO) If the White House sends a request for such information to the FBI without first sending the request through the entities described above, the request must be returned to the White House for resubmission.

- B. (U//FOUO) Compromising information concerning domestic officials or political organizations, or information concerning activities of United States persons intended to affect the political process in the United States, may be disseminated to the White House only with the approval of the Attorney General, based on a determination that such dissemination is needed for foreign intelligence purposes, for the purpose of protecting against international terrorism or other threats to the national security, or for the conduct of foreign affairs. However, such approval is not required for dissemination to the White House of information concerning efforts of foreign intelligence services to penetrate the White House, or concerning contacts by White House personnel with foreign intelligence service personnel. (AGG-Dom, Part VI.D.2.b)

- C. (U//FOUO) Examples of types of information that are suitable for dissemination to the White House on a routine basis include, but are not limited to (AGG-Dom, Part VI.D.2.c):

1. (U//FOUO) Information concerning international terrorism;
2. (U//FOUO) Information concerning activities of foreign intelligence services in the United States;
3. (U//FOUO) Information indicative of imminent hostilities involving any foreign power;
4. (U//FOUO) Information concerning potential cyber threats to the United States or its allies;
5. (U//FOUO) Information indicative of policy positions adopted by foreign officials, governments, or powers, or their reactions to United States foreign policy initiatives;
6. (U//FOUO) Information relating to possible changes in leadership positions of foreign governments, parties, factions, or powers;
7. (U//FOUO) Information concerning foreign economic or foreign political matters that might have national security ramifications; and
8. (U//FOUO) Information set forth in regularly published national intelligence requirements.

- D. (U//FOUO) Communications by the FBI to the White House that relate to a national security matter and concern a litigation issue for a specific pending case must be made known to the Office of the Attorney General, the Office of the Deputy Attorney General, or the Office of the Associate Attorney General. White House policy may limit or prescribe the White House personnel who may request information concerning such issues from the FBI. (AGG-Dom Part VI.D.2.d)

**UNCLASSIFIED - FOR OFFICIAL USE ONLY**  
**Domestic Investigations and Operations Guide**

- E. (U//FOUO) The limitations on dissemination of information by the FBI to the White House under the AGG-Dom do not apply to dissemination to the White House of information acquired in the course of an FBI investigation requested by the White House into the background of a potential employee or appointee, or responses to requests from the White House under E.O. 10450 relating to security requirements for government employment. (AGG-Dom, Part VI.D.2.e)

**14.6. (U) Special Statutory Requirements**

- A. (U) Dissemination of information acquired under the FISA is, to the extent provided in that Act, subject to minimization procedures and other requirements specified in that Act. (AGG-Dom, Part VI.D.3.a)
- B. (U) Information obtained through the use of NSLs under 15 U.S.C. § 1681v (NSLs to obtain full credit reports) may be disseminated in conformity with the general standards of AGG-Dom, Part VI, and DIOG Section 11.9.3.G. Information obtained through the use of NSLs under other statutes may be disseminated in conformity with the general standards of the AGG-Dom, Part VI, subject to any applicable limitations in their governing statutory provisions (see DIOG Section 11.9.3.G): 12 U.S.C. § 3414(a)(5)(B); 15 U.S.C. § 1681u(f); 18 U.S.C. § 2709(d); 50 U.S.C. § 436(e). (AGG-Dom, Part VI.D.3.b)

UNCLASSIFIED - FOR OFFICIAL USE ONLY  
Domestic Investigations and Operations Guide

## 15. (U) Intelligence Analysis and Planning

### 15.1. (U) Overview

(U//FOUO) The AGG-Dom provide specific guidance and authorization for intelligence analysis and planning. This authority enables the FBI to identify and understand trends, causes, and potential indicia of criminal activity and other threats to the United States that would not be apparent from the investigation of discrete matters alone. By means of intelligence analysis and planning, the FBI can more effectively discover criminal threats, threats to the national security, and other matters of national intelligence interest, and can provide the critical support needed for the effective discharge of its investigative responsibilities and other authorized activities. (AGG-Dom, Part IV)

(U//FOUO) In carrying out its intelligence functions under Part IV of the AGG-Dom, the FBI is authorized to collect information using all assessment investigative methods authorized in Part II of the AGG-Dom as described in the DIOG Section 5.

Investigative activities under the AGG-Dom and other legally authorized activities through which the FBI acquires information, data, or intelligence may properly be utilized, structured, and prioritized to support and effectuate the FBI's intelligence mission. (AGG-Dom, Part II.A.3.d and Part IV, Intro.)

(U//FOUO) **Note:** In the DIOG, the word "assessment" has two distinct meanings. The AGG-Dom authorizes as an investigative activity an "assessment," which requires an authorized purpose as discussed in Section 5. The USIC, however, also uses the word "assessment" to describe written intelligence products, as discussed in Section 15.7.B.

### 15.2. (U) Purpose and Scope

- A. (U//FOUO) **Functions Authorized:** The AGG-Dom authorizes the FBI to engage in intelligence analysis and planning to facilitate and support investigative activities and other authorized activities. The functions authorized include:
1. (U//FOUO) Development of overviews and analyses concerning threats to and vulnerabilities of the United States and its interests, such as domain management as related to the FBI's responsibilities;
  2. (U//FOUO) Research and analysis to produce reports and assessments (analytical products) concerning matters derived from or relevant to investigative activities or other authorized FBI activities; and
  3. (U//FOUO) The operation of intelligence and information systems that facilitate and support investigations and analysis through the compilation and analysis of data and information on an ongoing basis. (AGG-Dom, Introduction B)
- B. (U//FOUO) **Integration of Intelligence Activities:** In order to protect against national security and criminal threats through intelligence-driven operations, the FBI should integrate intelligence activities into all investigative efforts by:

b2  
b7E

**UNCLASSIFIED - FOR OFFICIAL USE ONLY**  
**Domestic Investigations and Operations Guide**

1. (U//FOUO) Systematically assessing particular geographic areas or sectors to identify potential threats, vulnerabilities, gaps, and collection opportunities in response to FBI collection requirements that support the broad range of FBI responsibilities;
  2. (U//FOUO) Pro-actively directing resources to collect against potential threats and other matters of interest to the nation and the FBI, and developing new collection capabilities where needed;
  3. (U//FOUO) Continuously validating collection capabilities to ensure information integrity;
  4. (U//FOUO) Deliberately gathering information in response to articulated priority intelligence requirements using all available collection resources, then expeditiously preparing the collected information for analysis and dissemination and promptly disseminating it to appropriate partners at the local, state, national and foreign level; and
  5. (U//FOUO) Purposefully evaluating the implications of collected information on current and emerging threat issues.
- C. (U//FOUO) **Analysis and Planning not Requiring the Initiation of an AGG-Dom Part II Assessment, (see DIOG Section 5):**

[Redacted]

b2  
b7E

As part of such analysis, an FBI employee can analyze historical information already contained within: (i) FBI data systems; (ii) USIC systems to which the FBI employee has access (e.g., [Redacted]); (iii) any other United States Government data system to which the FBI employee has access; and (iv) the FBI employee can also conduct open-source Internet searches. Open-source Internet searches do not include any paid-for-service databases such as Lexis-Nexis and Choicepoint.

b2  
b7E

[Redacted]

b2  
b7E

**15.3. (U) Civil Liberties and Privacy**

(U) The FBI must collect intelligence critical to the FBI's ability to carry out its intelligence and law enforcement mission. While conducting intelligence analysis and planning, the FBI will conduct its activities in compliance with the Constitution, federal laws, the AGG-Dom and other relevant authorities in order to protect civil liberties and privacy.

**15.4. (U) Legal Authority**

(U) The FBI is an intelligence agency as well as a law enforcement agency. Accordingly, its basic functions extend beyond limited investigations of discrete matters, and include broader analytic and planning functions. The FBI's responsibilities in this area derive from various administrative and statutory sources. See, e.g., E.O. 12333 § 1.7(g); 28 U.S.C. §§ 532 note (incorporating P.L. 108-458 §§ 2001-2003) and 534 note (incorporating P.L. 109-162 § 1107).

(U//FOUO) The scope of authorized activities under Part II of the AGG-Dom is not limited to "investigation" in a narrow sense, such as solving particular cases or obtaining evidence for use

**UNCLASSIFIED - FOR OFFICIAL USE ONLY**  
**Domestic Investigations and Operations Guide**

in particular criminal prosecutions. Rather, the investigative activities authorized under the AGG-Dom may be properly used to provide critical information needed for broader analytic and intelligence purposes to facilitate the solution and prevention of crime, protect the national security, and further foreign intelligence objectives. These purposes include use of the information in intelligence analysis and planning under AGG-Dom, Part IV, and dissemination of the information to other law enforcement, USIC, and White House agencies under AGG-Dom, Part VI. Accordingly, information obtained at all stages of investigative activity is to be retained and disseminated for these purposes as provided in the AGG-Dom, or in FBI policy consistent with the AGG-Dom, regardless of whether it furthers investigative objectives in a narrower or more immediate sense. (AGG-Dom, Part II)

**15.5. (U//FOUO) Standards for Initiating or Approving Intelligence Analysis and Planning**

(U//FOUO) If an FBI employee wishes to engage in Intelligence Analysis and Planning that requires the collection or examination of information not available: (i) through an open-source Internet search; (ii) in the FBI's existing files; (iii) in the USIC data systems to which the FBI employee has access; or (iv) in any other United States Government data system to which the FBI employee has access, an assessment must be initiated. An FBI employee or approving official must determine that:

- A. (U//FOUO) An authorized purpose and objective exists for the conduct of an assessment (e.g., information is needed in order to conduct appropriate intelligence analysis and planning);
- B. (U//FOUO) The assessment is based on factors other than the exercise of First Amendment activities or on the race, ethnicity, national origin or religion of the subject; and
- C. (U//FOUO) The assessment is an appropriate use of personnel and financial resources.

**15.6. (U//FOUO) Standards for Initiating or Approving the Use of an Authorized Investigative Method in Intelligence Analysis and Planning**

- A. (U//FOUO) The use of the particular investigative method is likely to further an objective of the assessment;
- B. (U//FOUO) The investigative method selected is the least intrusive method, reasonable under the circumstances;
- C. (U//FOUO) If the assessment relates to positive foreign intelligence, the FBI must operate openly and consensually with United States persons, to the extent practicable.
- D. (U//FOUO) The anticipated value of the assessment justifies the use of the selected investigative method or methods; and
- E. (U//FOUO) The investigative method is an appropriate use of personnel and financial resources.

**15.7. (U) Authorized Activities in Intelligence Analysis and Planning**

(U) The FBI may engage in intelligence analysis and planning to facilitate or support investigative activities authorized by the AGG-Dom or other legally authorized activities. Activities the FBI may carry out as part of Intelligence Analysis and Planning include:

**UNCLASSIFIED - FOR OFFICIAL USE ONLY**  
**Domestic Investigations and Operations Guide**

**A. (U//FOUO) Strategic Intelligence Analysis**

(U//FOUO) The FBI is authorized to develop overviews and analyses of threats to and vulnerabilities of the United States and its interests in areas related to the FBI's responsibilities, including domestic and international criminal threats and activities; domestic and international activities, circumstances, and developments affecting the national security. FBI overviews and analyses may encompass present, emergent, and potential threats and vulnerabilities, their contexts and causes, and identification and analysis of means of responding to them. (AGG-Dom, Part IV)

**1. (U//FOUO) Domain Management by Field Offices**

(U//FOUO) As part of Strategic Analysis Planning activities, the FBI may collect information in order to improve or facilitate "domain awareness" and may engage in "domain management." "Domain management" is the systematic process by which the FBI develops cross-programmatic domain awareness and leverages its knowledge to enhance its ability to: (i) proactively identify threats, vulnerabilities, and intelligence gaps; (ii) discover new opportunities for needed intelligence collection and prosecution; and (iii) set tripwires to provide advance warning of national security and criminal threats. Effective domain management enables the FBI to identify significant threats, detect vulnerabilities within its local and national domain, identify new sources and threat indicators, and recognize new trends so that resources can be appropriately allocated at the local level in accordance with national priorities.

(U//FOUO) Through a properly authorized assessment, domain management is undertaken at the local and national levels. All National Domain Assessments are initiated and coordinated by the DI. Examples of domain management activities include, but are not limited to: [redacted] census crime statistics, case information, domain entities, trend analysis, source development, and placement of tripwires. Further guidance regarding domain management and examples of intelligence products are contained in the [redacted]

b2  
b7E

(U//FOUO) The Field Office "domain" is the territory and issues for which a Field Office exercises responsibility, also known as the Field Office's area-of-responsibility (AOR). Domain awareness is the: (i) strategic understanding of national security and criminal threats and vulnerabilities; (ii) FBI's positioning to collect against these threats and vulnerabilities; and (iii) the existence of intelligence gaps related to the domain.

(U//FOUO) All information collected for domain management must be documented in an [redacted] as directed in the [redacted]

b2  
b7E

[redacted] 1. Additionally, at any time that [redacted] a separate substantive classification assessment file or subfile, according to the investigative matter, must be opened on the individual.

FBIHQ DI provides specific guidance in its [redacted] regarding, but not limited to: the initiation, opening, coordination and purpose for Field Office and National Domain Assessments.

b2  
b7E

**UNCLASSIFIED - FOR OFFICIAL USE ONLY**  
**Domestic Investigations and Operations Guide**

**2. (U//FOUO) Collection Management**

(U//FOUO) Collection Management is a formal business process through which Intelligence Information Needs and Intelligence Gaps (e.g., unknowns) are expressed as Intelligence Collection Requirements (questions or statements requesting information) and prioritized in a comprehensive, dynamic Intelligence Collection Plan. Results are monitored, and collectors are re-tasked as required.

**B. (U) Written Intelligence Products**

(U//FOUO) The FBI is authorized to conduct research, analyze information, and prepare reports and intelligence assessments (analytical products) concerning matters relevant to authorized FBI activities, such as: (i) reports and intelligence assessments (analytical product) concerning types of criminals or criminal activities; (ii) organized crime groups, terrorism, espionage, or other threats to the national security; (iii) foreign intelligence matters; or (iv) the scope and nature of criminal activity in particular geographic areas or sectors of the economy. (AGG-Dom, Part IV)

(U//FOUO) **United States Person Information:** Reports, Intelligence Assessments, and other FBI intelligence products should not contain United States person information including the names of United States corporations, if the pertinent intelligence can be conveyed without including identifying information.

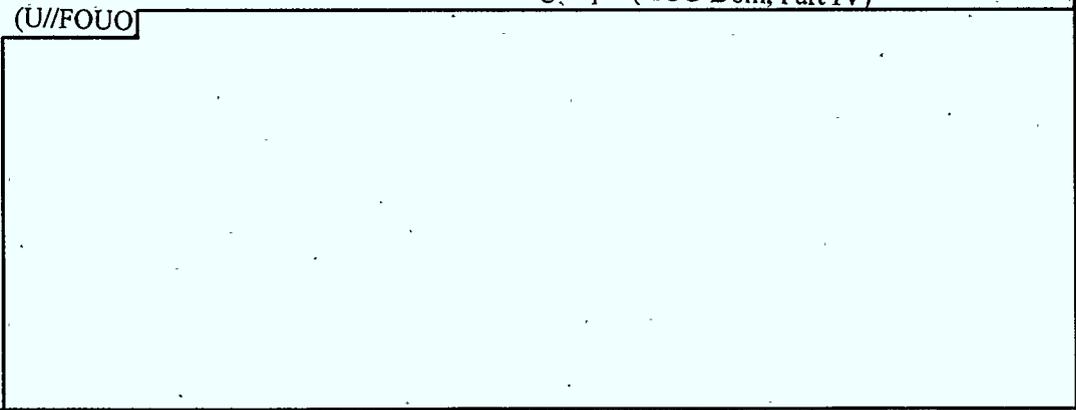
(U//FOUO) FBI intelligence products, both raw and finished, serve a wide range of audiences from national-level policy and decision-makers, intelligence agencies, and state, local and tribal law enforcement agencies.

(U//FOUO) Intelligence products prepared pursuant to this Section include, but are not limited to: Domain Management, Special Events Management Threat Assessments, Intelligence Assessments, Intelligence Bulletins, Intelligence Information Reports, WMD Scientific and Technical Assessments, and Regional Field Office Assessments.

**C. (U) Intelligence Systems**

(U//FOUO) The FBI is authorized to operate intelligence, identification, tracking, and information systems in support of authorized investigative activities, or for such other or additional purposes as may be legally authorized, such as intelligence and tracking systems relating to terrorists, gangs, or organized crime groups. (AGG-Dom, Part IV)

(U//FOUO)



b2  
b7E

**UNCLASSIFIED - FOR OFFICIAL USE ONLY**  
**Domestic Investigations and Operations Guide**

(U//FOUO) When developing a new database, the FBI OGC Privacy and Civil Liberties Unit must be consulted to determine if a Privacy Impact Assessment (PIA) must be prepared.

b2  
b7E

D. (U) [Redacted]

(U//FOUO) [Redacted]

b2  
b7E

(U//FOUO) [Redacted]

b2  
b7E

UNCLASSIFIED - FOR OFFICIAL USE ONLY  
Domestic Investigations and Operations Guide

**16. (U) Undisclosed Participation (UDP)**

**16.1. (U) Overview**

(U//FOUO) Undisclosed participation (UDP) takes place when anyone acting on behalf of the FBI, including but not limited to an FBI employee or confidential human source (CHS), becomes a member or participates in the activity of an organization on behalf of the U.S. Government without disclosing FBI affiliation to an appropriate official of the organization.

A. (U) **Authorities.** The FBI derives its authority to engage in UDP in organizations as part of its investigative and intelligence collection missions from two primary sources.

(U) First, Executive Order (E.O.) 12333 broadly establishes policy for the United States Intelligence Community (USIC). Executive Order 12333 requires the adoption of procedures for undisclosed participation in organizations on behalf of elements of the USIC within the United States. Specifically, the Order provides "... [n]o one acting on behalf of the Intelligence Community may join or otherwise participate in any organization in the United States on behalf of the any element of the Intelligence Community without first disclosing such person's intelligence affiliation to appropriate officials of the organization, except in accordance with procedures established by the head of the Intelligence Community element concerned .... Such participation shall be authorized only if it is essential to achieving lawful purposes as determined by the Intelligence Community element head or designee." (E.O. 12333, Section 2.9, Undisclosed Participation in Organizations Within the United States). The Order also provides, at Section 2.2, that "[n]othing in [E.O. 12333] shall be construed to apply to or interfere with any authorized civil or criminal law enforcement responsibility of any department or agency."

(U) Second, in addition to its role as member of the USIC, the FBI is also the primary criminal investigative agency of the federal government with authority and responsibility to investigate all violations of federal law that are not exclusively assigned to another federal agency. This includes the investigation of crimes involving international terrorism and espionage. As a criminal investigative agency, the FBI has the authority to engage in UDP as part of a predicated investigation or an assessment.

(U//FOUO) The FBI's UDP policy is designed to incorporate the FBI's responsibilities as both a member of the USIC and as the primary criminal investigative agency of the federal government and, therefore, applies to all investigative and information collection activities of the FBI. It is intended to provide uniformity and clarity so that FBI employees have one set of standards to govern all UDP. As is the case throughout the DIOG, however, somewhat different constraints exist if the purpose of the activity is the collection of positive foreign intelligence that falls outside the FBI's law enforcement authority. Those constraints are reflected where applicable below.

B. (U//FOUO) **Mitigation of Risk.**



b2  
b7E

**UNCLASSIFIED - FOR OFFICIAL USE ONLY**  
**Domestic Investigations and Operations Guide**

[Redacted]

b2  
b7E

(U//FOUO)  
[Redacted]

b2  
b7E

**16.2. (U) Purpose, Scope, and Definitions**

A. (U//FOUO)  
[Redacted]

b2  
b7E

B. (U//FOUO)  
[Redacted]

b2  
b7E

C. (U//FOUO)  
[Redacted]

b2  
b7E

UNCLASSIFIED - FOR OFFICIAL USE ONLY  
Domestic Investigations and Operations Guide

1. (U//FOUO) [Redacted]

b2  
b7E

2. (U//FOUO) [Redacted]

b2  
b7E

3. (U//FOUO) [Redacted]

b2  
b7E

4. (U//FOUO) [Redacted]

b2  
b7E

D. (U//FOUO) [Redacted]

b2  
b7E

E. (U//FOUO) [Redacted]

b2  
b7E

F. (U//FOUO) [Redacted]

b2  
b7E

G. (U//FOUO) [Redacted]

b2  
b7E

UNCLASSIFIED - FOR OFFICIAL USE ONLY  
Domestic Investigations and Operations Guide

b2  
b7E

[Redacted]

H. (U//FOUO)

[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

I. (U//FOUO)

[Redacted]

b2  
b7E

16.3. (U) Requirements for Approval

A. (U//FOUO)

[Redacted]

b2  
b7E

UNCLASSIFIED - FOR OFFICIAL USE ONLY  
Domestic Investigations and Operations Guide

1. (U//FOUO) [Redacted]

b2  
b7E

2. (U//FOUO) [Redacted]

b2  
b7E

3. (U//FOUO) [Redacted]

b2  
b7E

B. (U//FOUO) Specific Requirements for General Undisclosed Participation (Non-sensitive UDP):

1. (U//FOUO) [Redacted]

b2  
b7E

a. (U//FOUO) [Redacted]

b2  
b7E

b. (U//FOUO) [Redacted]

b2  
b7E

2. (U//FOUO) [Redacted]

b2  
b7E

(U//FOUO) [Redacted]

b2  
b7E

a. (U//FOUO) [Redacted]

b2  
b7E

UNCLASSIFIED - FOR OFFICIAL USE ONLY  
Domestic Investigations and Operations Guide

b. (U//FOUO) [Redacted]

b2  
b7E

c. (U//FOUO) [Redacted]

b2  
b5  
b7E

d. (U//FOUO) [Redacted]

b2  
b5  
b7E

C. (U//FOUO) [Redacted]

b2  
b7E

I. (U//FOUO) [Redacted]

b2  
b7E

a. (U//FOUO) [Redacted]

b2  
b7E

b. (U//FOUO) [Redacted]

b2  
b5  
b7E

c. (U//FOUO) [Redacted]

b2  
b7E

UNCLASSIFIED - FOR OFFICIAL USE ONLY  
Domestic Investigations and Operations Guide

[Redacted]

b2  
b7E

2. (U//FOUO)

[Redacted]

b2  
b7E

(U//FOUO)

[Redacted]

b2  
b5  
b7E

3. (U//FOUO)

[Redacted]

b2  
b7E

(U//FOUO)

[Redacted]

b2  
b7E

a. (U//FOUO)

[Redacted]

b2  
b7E

b. (U//FOUO)

[Redacted]

b2  
b5  
b7E

a. (U//FOUO)

[Redacted]

b2  
b5  
b7E

16.4. (U) Supervisory Approval Not Required

(U//FOUO)

[Redacted]

b2  
b7E

A. (U//FOUO)

[Redacted]

b2  
b7E

B. (U//FOUO)

[Redacted]

b2  
b7E

UNCLASSIFIED - FOR OFFICIAL USE ONLY  
Domestic Investigations and Operations Guide

[Redacted]

b2  
b7E

C. (U//FOUO)

[Redacted]

b2  
b7E

D. (U//FOUO)

[Redacted]

b2  
b7E

E. (U//FOUO)

[Redacted]

b2  
b7E

16.5. (U//FOUO) Standards for Review and Approval

A. (U//FOUO)

[Redacted]

b2  
b7E

1. (U//FOUO)

[Redacted]

b2  
b7E

2. (U//FOUO)

[Redacted]

b2  
b7E

3. (U//FOUO)

[Redacted]

b2  
b7E

4. (U//FOUO)

[Redacted]

b2  
b7E

5. (U//FOUO)

[Redacted]

b2  
b7E

B. (U//FOUO)

[Redacted]

b2  
b7E

1. (U//FOUO)

[Redacted]

b2  
b7E

2. (U//FOUO)

[Redacted]

b2  
b7E

UNCLASSIFIED - FOR OFFICIAL USE ONLY  
Domestic Investigations and Operations Guide

C. (U//FOUO)

[Redacted]

b2  
b7E

D. (U//FOUO)

[Redacted]

b2  
b7E

E. (U//FOUO)

[Redacted]

b2  
b7E

16.6. (U) Requests for Approval of Undisclosed Participation

A. (U//FOUO)

[Redacted]

b2  
b7E

B. (U//FOUO)

[Redacted]

b2  
b7E

1. (U//FOUO)

[Redacted]

b2  
b7E

2. (U//FOUO)

[Redacted]

b2  
b7E

3. (U//FOUO)

[Redacted]

b2  
b7E

4. (U//FOUO)

[Redacted]

b2  
b7E

5. (U//FOUO)

[Redacted]

b2  
b7E

UNCLASSIFIED - FOR OFFICIAL USE ONLY  
Domestic Investigations and Operations Guide

6. (U//FOUO) [Redacted]

b2  
b7E

C. (U//FOUO) [Redacted]

b2  
b7E

16.7. (U) Duration

(U//FOUO) [Redacted]

b2  
b7E

16.8. (U//FOUO) [Redacted]

b2  
b5  
b7E

A. (U//FOUO) [Redacted]

b2  
b5  
b7E

1. (U//FOUO) [Redacted]

b2  
b5  
b7E

2. (U//FOUO) [Redacted]

b2  
b5  
b7E

(U//FOUO) [Redacted]

b2  
b5  
b7E

B. (U//FOUO) [Redacted]

[Redacted]

b2  
b5  
b7E

UNCLASSIFIED - FOR OFFICIAL USE ONLY  
Domestic Investigations and Operations Guide

16.9. (U//FOUO) UDP EXAMPLES

A. (U//FOUO) [Redacted]

b2  
b7E

(U//FOUO) [Redacted]

b2  
b5  
b7E

B. (U//FOUO) [Redacted]

b2  
b7E

(U//FOUO) [Redacted]

b2  
b5  
b7E

C. (U//FOUO) [Redacted]

b2  
b7E

UNCLASSIFIED - FOR OFFICIAL USE ONLY  
Domestic Investigations and Operations Guide

(U//FOUO) [Redacted]

b2  
b5  
b7E

D. (U//FOUO) [Redacted]

b2  
b7E

(U//FOUO) [Redacted]

b2  
b5  
b7E

E. (U//FOUO) [Redacted]

b2  
b7E

(U//FOUO) [Redacted]

b2  
b5  
b7E

F. (U//FOUO) [Redacted]

b2  
b7E

UNCLASSIFIED - FOR OFFICIAL USE ONLY  
Domestic Investigations and Operations Guide

(U//FOUO)

[Redacted]

b2  
b5  
b7E

G. (U//FOUO)

[Redacted]

b2  
b7E

(U//FOUO)

[Redacted]

b2  
b5  
b7E

H. (U//FOUO)

[Redacted]

b2  
b7E

(U//FOUO)

[Redacted]

b2  
b5  
b7E

I. (U//FOUO)

[Redacted]

b2  
b7E

(U//FOUO)

[Redacted]

b2  
b5  
b7E

**UNCLASSIFIED - FOR OFFICIAL USE ONLY**  
**Domestic Investigations and Operations Guide**

b2  
b7E

J. (U//FOUO) [Redacted]  
[Redacted]

b2  
b5  
b7E

(U//FOUO) [Redacted]  
[Redacted]

K. (U//FOUO) [Redacted]  
[Redacted]

b2  
b7E

(U//FOUO) [Redacted]  
[Redacted]

b2  
b5  
b7E

UNCLASSIFIED - FOR OFFICIAL USE ONLY  
Domestic Investigations and Operations Guide

## 17. (U) Otherwise Illegal Activity

---

### 17.1. (U) Overview

(U//FOUO) Otherwise Illegal Activity (OIA) is conduct in the course of duties by an FBI employee (to include a UCE) or CHS which constitutes a crime under local, state, or federal law if engaged in by a person acting without authorization. Under limited circumstances, OIA can be authorized for an FBI employee or CHS to obtain information or evidence necessary for the success of an investigation under the following circumstances: (i) when that information or evidence is not reasonably available without participation in the OIA; [redacted] or (ii) [redacted] when necessary to prevent serious bodily injury or death. Certain types of OIA are not authorized such as participation in an act of violence, except in self-defense, or participation in conduct that would constitute an unlawful investigative technique such as an illegal wiretap.

b2  
b7E

### 17.2. (U) Purpose and Scope

(U//FOUO) The use of OIA may be approved in the course of undercover activities or operations that involve an FBI employee or that involve use of a CHS. When approved, OIA should be limited or minimized in scope to only that which is reasonably necessary under the circumstances including the duration and geographic area to which approval applies, if appropriate.

### 17.3. (U//FOUO) OIA in Undercover Activity

- A. (U//FOUO) **General.** The use of the undercover method is discussed in the DIOG Section 11.8. OIA is often proposed as part of an undercover scenario or in making the initial undercover contacts before the operation is approved. Specific approval for OIA must be obtained in the context of these undercover activities or operations in addition to general approval of the scenario or the operation.
- B. (U//FOUO) **OIA by an FBI employee in an undercover operation relating to activity in violation of federal criminal law that does not concern a threat to the national security or foreign intelligence:** must be approved in conformity with the AGG-UCO. Approval of OIA in conformity with the AGG-UCO is sufficient and satisfies any approval requirement that would otherwise apply under the AGG-Dom. Additional discussion is provided in the Field Guide for FBI Undercover and Sensitive Operations. An SAC may approve the OIA described in subsection 17.5.
1. (U//FOUO) When a UCE provides goods and service (reasonably unavailable to the subject except as provided by the United States government) that facilitate a felony, or its equivalent under federal, state, or local law, it is a sensitive circumstance. In these sensitive circumstances, additional authorization by an Assistant Director is required after review by the Criminal Undercover Operations Review Committee (CUORC).
  2. (U//FOUO) Participation in otherwise illegal activity that involves a significant risk of violence or physical injury requires authorization by the Director, Deputy Director, or designated Executive Assistant Director after review by the CUORC.
- C. (U//FOUO) **OIA by an FBI employee in an undercover operation relating to a threat to the national security or foreign intelligence collection** must conform to the AGG-Dom.

**UNCLASSIFIED - FOR OFFICIAL USE ONLY**  
**Domestic Investigations and Operations Guide**

The DOJ NSD is the approving component for OIA that requires approval beyond that authorized for SAC approval described in DIOG subsection 17.5, below. However, as authorized by the Assistant Attorney General for NSD, officials in other DOJ components may approve OIA in such investigations.

**17.4. (U//FOUO) OIA for a Confidential Human Source**

(U//FOUO) OIA by a CHS must be approved in conformity with the AGG-CHS and the FBI CHSPM.

**17.5. (U//FOUO) Approval of OIA by a Special Agent in Charge**

(U//FOUO) An SAC may authorize the following OIA for an FBI employee when consistent with other requirements of this section, the AGG-UCO, and other FBI policy:

- A. (U//FOUO) Otherwise illegal activity that would not be a felony under federal, state, local, or tribal law;
- B. (U//FOUO) Consensual monitoring of communications, even if a crime under state, local, or tribal law;

(U//FOUO) **Note:** Other approvals for the consensual monitoring may apply such as that required when the consensual monitoring involves a sensitive monitoring circumstance. See DIOG Section 11.5.4.

(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.

- C. (U//FOUO) The controlled purchase, receipt, delivery, or sale of drugs, stolen property, or other contraband;
- D. (U//FOUO) The payment of bribes;  
(U//FOUO) **Note:** the payment of bribes and the amount of such bribes in a public corruption matter may be limited by other FBI policy; see the CID PG.
- E. (U//FOUO) The making of false representations in concealment of personal identity or the true ownership of a proprietary; and
- F. (U//FOUO) Conducting a money laundering transaction or transactions involving an aggregate amount not exceeding \$1 million.

(U//FOUO) **Exception:** An SAC may not authorize an activity that may constitute material support to terrorism, a violation of export control laws, or a violation of laws that concern proliferation of weapons of mass destruction. In such an investigation, an SAC may authorize an activity that may otherwise violate prohibitions of material support to terrorism only according to standards established by the Director of the FBI and agreed to by the Assistant Attorney General for National Security. (AGG-Dom, Part V.C.3)

**UNCLASSIFIED - FOR OFFICIAL USE ONLY**  
**Domestic Investigations and Operations Guide**

**17.6. (U//FOUO) Standards for Review and Approval of OIA**

(U//FOUO) No official may recommend or approve participation by an FBI employee in OIA unless the participation is justified:

- A. (U//FOUO) To obtain information or evidence necessary for the success of the investigation and not reasonably available without participation in the otherwise illegal activity;
- B. (U//FOUO)  or b2  
b7E
- C. (U//FOUO) To prevent death or serious bodily injury.

**17.7. (U//FOUO) OIA not authorized**

(U//FOUO) The following activities may not be authorized for an FBI employee:

- A. (U//FOUO) Directing or participating in acts of violence;

(U//FOUO) Note: Self-defense and defense of others. FBI employees are authorized to engage in any lawful use of force, including the use of force in self-defense or defense of others in the lawful discharge of their duties.

- B. (U//FOUO) Activities whose authorization is prohibited by law, including unlawful investigative methods, such as illegal, non-consensual, electronic surveillance or illegal searches.

(U//FOUO) Note: Subparagraph B includes activities that would violate protected constitutional or federal statutory rights in the absence of a court order or warrant such as illegal wiretaps and searches.

**17.8. (U//FOUO) Emergency Situations**

(U//FOUO) Without prior approval, an FBI employee may engage in OIA that could be authorized under this section only if necessary to meet an immediate threat to the safety of persons or property or to the national security, or to prevent the compromise of an investigation or the loss of a significant investigative opportunity. In such a case, prior to engaging in the OIA, every effort should be made by the FBI employee to consult with the SAC, and by the SAC to consult with the USAO or appropriate DOJ Division where the authorization of that office or Division would be required unless the circumstances preclude such consultation. Cases in which OIA occur pursuant to this paragraph without the authorization required must be reported as soon as possible to the SAC, and by the SAC to FBIHQ and to the USAO or appropriate DOJ Division.