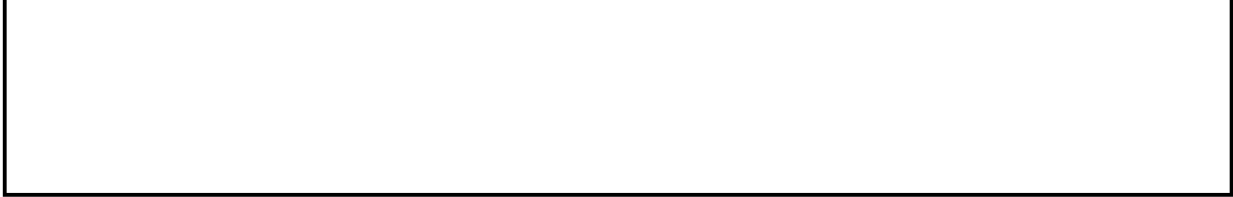


18.6.12.6 (U) **STANDARDS FOR USE AND APPROVAL REQUIREMENTS RETRIEVAL OF
DISCARDED OR ABANDONED PROPERTY, ADMINISTRATIVE SEARCHES OF
LOST OR MISPLACED PROPERTY AND INVENTORY SEARCHES GENERALLY**

(U//~~FOUO~~)



b7E

This Page is Intentionally Blank

UNCLASSIFIED – ~~FOR OFFICIAL USE ONLY~~

Domestic Investigations and Operations Guide

§18

b6
b7C

18.6.13 (U) *INVESTIGATIVE METHOD: UNDERCOVER OPERATIONS*

18.6.13.1 (U) SUMMARY

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

b7E

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

(U//~~FOUO~~) *Application:* [REDACTED]

b7E

18.6.13.2 (U) LEGAL AUTHORITY

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

B) (U) AGG-UCO

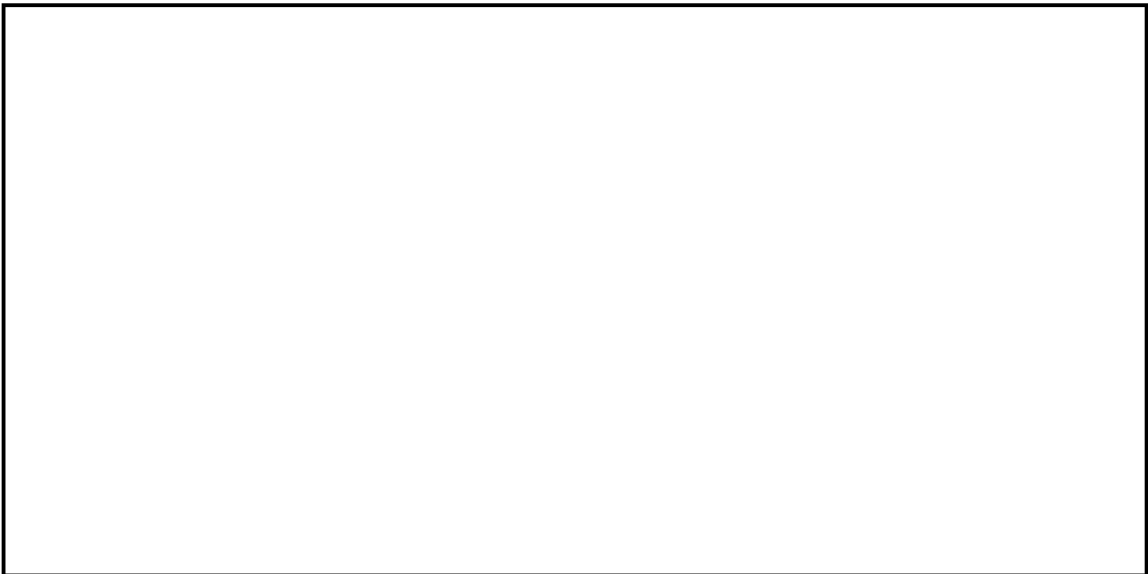
18.6.13.3 (U) DEFINITION OF INVESTIGATIVE METHOD

A) (U//~~FOUO~~) *Undercover Activity:* [REDACTED]

b7E

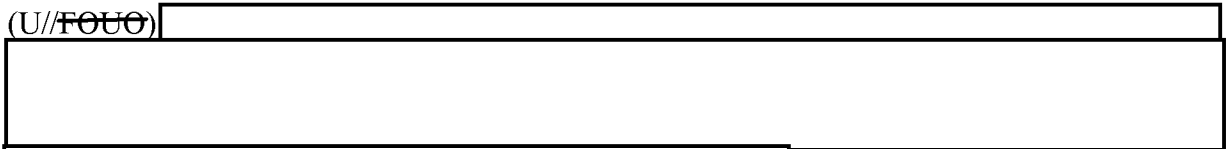
B) (U//~~FOUO~~) [REDACTED]

C) (U//~~FOUO~~) *Undercover Operation:* [REDACTED]

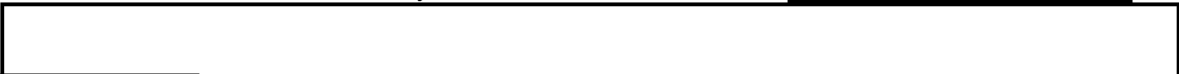


18.6.13.3.1 (U) ***DISTINCTION BETWEEN SENSITIVE CIRCUMSTANCE AND SENSITIVE INVESTIGATIVE MATTER***

(U//~~FOUO~~)



in the AGG-UCO and the USOPG and for national security matters in the NSUCOPG.



The detailed policy for undercover operations is described in this section of the DIOG, the USOPG, the NSUCOPG, and the FBIHQ operational division PGs.

18.6.13.4 (U//~~FOUO~~) ***STANDARDS FOR USE AND APPROVAL REQUIREMENTS FOR INVESTIGATIVE METHOD***

18.6.13.4.1 (U) ***STANDARDS FOR USE OF INVESTIGATIVE METHOD***

(U//~~FOUO~~) An official considering approval or authorization of a proposed undercover application must weigh the risks and benefits of the operation, giving careful consideration to the following:

- A) (U//~~FOUO~~) The risks of personal injury to individuals, property damage, financial loss to persons or business, damage to reputation, or other harm to persons;
- B) (U//~~FOUO~~) The risk of civil liability or other loss to the government;
- C) (U//~~FOUO~~) The risk of invasion of privacy or interference with privileged or confidential relationships and any potential constitutional concerns or other legal concerns;
- D) (U//~~FOUO~~) The risk that individuals engaged in undercover operations may become involved in illegal conduct; and
- E) (U//~~FOUO~~) The suitability of government participation in the type of activity that is expected to occur during the operation. See AGG-UCO, Part IV.A.

F) (U//~~FOUO~~) [REDACTED]
[REDACTED]

b7E

18.6.13.4.2 (U//~~FOUO~~) **APPROVAL REQUIREMENTS FOR UCOs (INVESTIGATIONS OF VIOLATIONS OF FEDERAL CRIMINAL LAW THAT DO NOT CONCERN THREATS TO NATIONAL SECURITY OR FOREIGN INTELLIGENCE)**

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

b7E

A) (U//~~FOUO~~) [REDACTED]
[REDACTED]

B) [REDACTED]

C) (U//~~FOUO~~) [REDACTED]
[REDACTED]

D) [REDACTED]

b7E

[REDACTED]

E) (U//~~FOUO~~) [REDACTED]
[REDACTED]

F) (U//~~FOUO~~) [REDACTED]
[REDACTED]

G) (U//~~FOUO~~) [REDACTED]
[REDACTED]

H) (U//~~FOUO~~) [REDACTED]
[REDACTED]

[REDACTED]

b7E

I) (U//~~FOUO~~) [REDACTED]
[REDACTED]

18.6.13.4.3 (U//~~FOUO~~) **APPROVAL REQUIREMENTS FOR UCOS** [REDACTED]
[REDACTED]
[REDACTED]

b7E

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

A) (U//~~FOUO~~) [REDACTED]
[REDACTED]

B) (U//~~FOUO~~) [REDACTED]
[REDACTED]

C) (U//~~FOUO~~) [REDACTED]
[REDACTED] If the matter involves religious or political
organizations, the review must include participation by a representative of the DOJ NSD. See
AGG-Dom, Section V; and [REDACTED]

D) (U//~~FOUO~~) [REDACTED]
[REDACTED]

E) (U//~~FOUO~~) [REDACTED]
[REDACTED]

18.6.13.5 (U) [REDACTED] **OIA IN UNDERCOVER OPERATIONS**

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

A) (U) [REDACTED]
[REDACTED]

b7E

B) (U) [REDACTED]
[REDACTED]

C) (U) [REDACTED]
[REDACTED]

D) (U) [REDACTED]
[REDACTED]

⁴⁷ (U) [REDACTED]
[REDACTED]

E) (U) [REDACTED]
[REDACTED]

b7E

F) (U) [REDACTED]
[REDACTED]

G) (U) [REDACTED]

(U) [REDACTED]
[REDACTED]

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

18.6.13.6 (U) **DURATION OF APPROVAL**

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

b7E

18.6.13.7 (U) **ADDITIONAL GUIDANCE**

A) (U//~~FOUO~~) [REDACTED]
[REDACTED]

B) (U//~~FOUO~~) [REDACTED]
[REDACTED]

C) (U//~~FOUO~~) [REDACTED]
[REDACTED]

18.6.13.8 (U) **COMPLIANCE AND MONITORING, AND REPORTING REQUIREMENTS**

(U//~~FOUO~~) All UCOs must provide an [REDACTED] using the
[REDACTED] to appropriate [REDACTED]

This Page is Intentionally Blank

18.7 (U) AUTHORIZED INVESTIGATIVE METHODS IN FULL INVESTIGATIONS

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

(U) In Full Investigations, to include Enterprise Investigations, the authorized investigative methods include:

A) (U) The investigative methods authorized for Assessments.

- 1) (U) Public information. (See Section 18.5.1)
- 2) (U) Records or information - FBI and DOJ. (See Section 18.5.2)
- 3) (U) Records or information - Other federal, state, local, tribal, or foreign government agency. (See Section 18.5.3)
- 4) (U) On-line services and resources. (See Section 18.5.4)
- 5) (U) CHS use and recruitment. (See Section 18.5.5)
- 6) (U) Interview or request information from the public or private entities. (See Section 18.5.6)
- 7) (U) Information voluntarily provided by governmental or private entities. (See Section 18.5.7)
- 8) (U) Physical Surveillance (not requiring a court order). (See Section 18.5.8)

B) (U) The investigative methods authorized for Preliminary Investigations.

- 1) (U) Consensual monitoring of communications, including electronic communications. (See Section 18.6.1)
- 2) (U) Intercepting the communications of a computer trespasser. (See Section 18.6.2)
- 3) (U) Closed-circuit television/video surveillance, direction finders, and other monitoring devices. (See Section 18.6.3)
- 4) (U) Administrative subpoenas. (See Section 18.6.4)
- 5) (U) Grand jury subpoenas. (See Section 18.6.5)
- 6) (U) National Security Letters. (See Section 18.6.6)
- 7) (U) FISA Order for business records. (See Section 18.6.7)
- 8) (U) Stored wire and electronic communications and transactional records. (See Section 18.6.8)⁴⁸
- 9) (U) Pen registers and trap/trace devices. (See Section 18.6.9)
- 10) (U) Mail covers. (See Section 18.6.10)
- 11) (U) Polygraph examinations. (See Section 18.6.11)
- 12) (U) Trash Covers (Searches that do not require a warrant or court order). (See Section 18.6.12)
- 13) (U) Undercover operations. (See Section 18.6.13)

⁴⁸ (U//~~FOUO~~) The use of Search Warrants to obtain this information in Preliminary Investigations is prohibited. (See DIOG Section 18.6.8.4.2.3)

C) (U) Searches – with a warrant or court order (reasonable expectation of privacy). (See Section 18.7.1 below)

D) (U) Electronic surveillance – Title III. (See Section 18.7.2 below)

E) (U) Electronic surveillance – FISA and FISA Title VII (acquisition of foreign intelligence information). (See Section 18.7.3 below)

(U//~~FOUO~~) Not all investigative methods are authorized while collecting foreign intelligence as part of a Full Investigation. See DIOG Section 9 for more information.

This Page is Intentionally Blank

18.7.1 (U) *INVESTIGATIVE METHOD: SEARCHES – WITH A WARRANT OR COURT ORDER (REASONABLE EXPECTATION OF PRIVACY)*

(U) See AGG-Dom, Part V.A.12 and the Attorney General's Guidelines On Methods Of Obtaining Documentary Materials Held By Third Parties, Pursuant to Title II, Privacy Protection Act of 1980 (Pub. L. 96-440, Sec. 201 et seq.; 42 U.S.C. § 2000aa-11, et seq.).

18.7.1.1 (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. Although an unlawful search may not preclude a prosecution, it can have serious consequences for the government. These include adverse publicity, civil liability against the employee or the government and the suppression of evidence from the illegal seizure.

(U//~~FOUO~~) Application:

[REDACTED]

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.

(U//~~FOUO~~) There are special rules that must be followed prior to obtaining a search warrant that might intrude upon professional, confidential relationships.

18.7.1.2 (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.

18.7.1.3 (U) DEFINITION OF INVESTIGATIVE METHOD

(U) ***Physical Search defined:*** 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 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.

18.7.1.3.1 (U) REQUIREMENT FOR REASONABLENESS

(U) By the terms of the Fourth Amendment, a search must be reasonable at its inception and reasonable in its execution.

b7E

18.7.1.3.2 (U) REASONABLE EXPECTATION OF PRIVACY

(U) 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.

18.7.1.3.3 (U) ISSUANCE OF SEARCH WARRANT

(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.

(U) Physical searches related to a national security purpose may be authorized by the FISC. (50 U.S.C. §§ 1821-1829)

18.7.1.3.4 (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:

18.7.1.3.4.1 (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.

18.7.1.3.4.2 (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 [REDACTED]

b7E

18.7.1.3.4.3 (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.

18.7.1.3.4.4 (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 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.

18.7.1.3.4.4.1 (U) SEARCH WARRANT

(U//~~FOUO~~) Investigators can obtain the full contents of a network account with a search warrant. ECPA does not require the government to notify the customer or subscriber when it obtains information from a provider using a search warrant. Warrants issued under 18 U.S.C. § 2703 must either comply with FRCP Rule 41 or be an equivalent state warrant. Warrants issued pursuant to 18 U.S.C. § 2703 do not require personal service on the customer; the warrants are only be served on the electronic communication service or a remote computing service. FRCP Rule 41 requires a copy of the warrant be left with the provider, and a return and inventory be made. Federal courts have nationwide jurisdiction to issue these search warrants (see below).

(U) With a search warrant issued based on probable cause pursuant to FRCP Rule 41 or an equivalent state warrant, the government may obtain:

A) (U) The contents of a wire or electronic communication that has been in electronic storage in an electronic communications system for one hundred and eighty days or less, and

B) (U) Everything that can be obtained using a 18 U.S.C. § 2703(d) court order with notice.

(U) In other words, every record and all of the stored contents of an account—including opened and unopened e-mail/voice mail— can be obtained with a search warrant based on probable cause pursuant to FRCP Rule 41. Moreover, because the warrant is issued by a neutral magistrate based on a finding of probable cause, obtaining a search warrant effectively insulates the process from challenge under the Fourth Amendment.

18.7.1.3.4.4.2 (U) *NATIONWIDE SCOPE*

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

18.7.1.3.4.4.3 (U) *SERVICE OF PROCESS*

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

18.7.1.3.4.4.4 (U) *COURT ORDER WITH PRIOR NOTICE TO THE SUBSCRIBER OR CUSTOMER*

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

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

A) (U) "The contents of a wire or electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days." 18 U.S.C. § 2703(a).

B) (U) "The contents of any wire or electronic communication" held by a provider of remote computing service "on behalf of . . . a subscriber or customer of such remote computing service," 18 U.S.C. §§ 2703(b)(1)(B)(ii), 2703 (b)(2); and

C) (U) Everything that can be obtained using a 18 U.S.C. § 2703(d) court order without notice.

(U)

[REDACTED]

(U)

[REDACTED]

b7E

18.7.1.3.4.4.5 (U) *LEGAL STANDARD*

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

18.7.1.3.4.4.6 (U) *NATIONWIDE SCOPE*

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

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

18.7.1.3.4.4.7 (U) *COURT ORDER WITHOUT PRIOR NOTICE TO THE SUBSCRIBER OR CUSTOMER*

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

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

18.7.1.4 (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 . This form should be completed by the case agent.
- C) (U//~~FOUO~~) **Sensitive Investigative Matters (SIM):** Notice to the appropriate FBIHQ operational 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.

D) (U//~~FOUO~~)

b7E

(U) 28 C.F.R. § 50.10(b)(1)(ii) provides guidance on categories of individuals and entities not by, and therefore not entitled to the protections of the DOJ policy set out above.

18.7.1.5 (U) DURATION OF APPROVAL

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

18.7.1.6 (U) SPECIFIC PROCEDURES

18.7.1.6.1 (U) OBTAINING A WARRANT UNDER FRCP RULE 41

18.7.1.6.1.1 (U) PROBABLE CAUSE

(U//~~FOUO~~) 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 sizable 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.

18.7.1.6.1.2 (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 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.

18.7.1.6.1.3 (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.

18.7.1.6.1.4 (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 14 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.

18.7.1.6.1.5 (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.
- 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.

18.7.1.6.1.6 (U) WRITTEN OPERATION ORDERS FOR SEARCH OPERATIONS

(U) The ADIC/SAC is responsible to ensure that careful and thorough planning is conducted for the successful execution of a high risk search operation involving a potentially dangerous situation or subject. The plan must be adapted to each situation and must include relevant details to enhance the safety and effectiveness of the agents and

officers involved in the search operation. The planning and execution of arrests, raids, and searches should be assigned to experienced Agents. All plans must be approved by ASACs or their designees.

(U) Prior to conducting a search operation deemed a high risk, the agent must prepare a written operation order (OPORDER) to include the five critical categories: Situation, Mission, Execution, Administration and Equipment, and Control and Communication (SMEAC), and must utilize the Law Enforcement Operations Order (OPORDER), FD-888. In situations where an FBI SWAT Team(s) or the Critical Incident Response Group's (CIRG), Tactical Section is involved, the Operations Order Template must be used in lieu of the FD-888. See the [REDACTED] and [REDACTED] for more on the use of the SWAT Teams and CIRG, Tactical Section in high risk operations.

b7E

(U) The written OPORDER must be presented in an oral briefing to all personnel involved in the execution of the search warrant prior to the operation. During the briefing, the briefing agent should stress to the participants of the operation that the search has the potential to become dangerous. At the discretion of the field office approving official, the CDC/ADC may review the OPORDER (FD-888) and/or participate in providing the FBI deadly force briefing to the search operation participants.

(U) Exigent circumstances (i.e., emergency, pressing necessity requiring immediate action) may necessitate an oral briefing in lieu of the written OPORDER. The ASAC or designee must approve the use of an oral briefing in lieu of a written and approved OPORDER in exigent circumstances. An oral briefing must follow the requirements of a written OPORDER to address the SMEAC categories identified above. Documentation of the oral briefing must occur as soon as possible following the operation by preparing and filing the FD-888 or the Operations Order Template, whichever is appropriate for the situation.

(U) The agent may consider utilizing, and/or alerting local authorities to the planned search, if appropriate under the circumstances. Although the time of notification is left to the discretion of the agent, he/she must consider the jurisdiction of local law enforcement, its responsibility to its community and its need to be aware of law enforcement actions in its jurisdiction.

18.7.1.6.1.7 (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.

18.7.1.6.1.8 (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)

18.7.1.6.1.9 (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 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).

18.7.1.6.1.10 (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.

18.7.1.6.2 (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).

18.7.1.6.2.1 (U) CERTIFICATE BY THE DIRECTOR OF THE FBI

- (U) Each FISA application must be accompanied by 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 obtained by normal investigative techniques; that the information sought is "foreign intelligence information" as defined by FISA. The certification must include a statement explaining the certifier's basis for the certification.
- (U) 50 U.S.C. § 1823 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. The FBI Director has represented to Congress that the FBI deputy Director will only certify FISA's when the FBI Director is not available to do so.

18.7.1.6.2.2 (U) LENGTH OF PERIOD OF AUTHORIZATION FOR FISC ORDERS

(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 a non-USPER agent of a foreign power, with renewals for up to one.

18.7.1.6.2.3 (U) EXTENSION OF PHYSICAL SEARCH AUTHORITY

(U//~~FOUO~~) 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.

18.7.1.6.2.4 (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.
- 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,

b7E

18.7.1.6.2.5 (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 (USPER); 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 USPERs acquired through unconsented physical searches may only be used according to minimization procedures. See: 50 U.S.C. §§ 1824(d)(4) and 1825(a).

18.7.1.6.2.6 (U) REQUIRED NOTICE

(U) If an authorized search involves the premises of an USPER, 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 USPER that the premises was searched and the identification of any property seized, altered, or reproduced during the search.

18.7.1.6.2.7 (U//~~FOUO~~) FISA VERIFICATION OF ACCURACY PROCEDURES

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

b7E

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

A) (U//~~FOUO~~) [REDACTED] submission to the FISC must include [REDACTED] This FISA [REDACTED] must be used for copies of all of the supporting documentation relied upon when making the certifications contained on the [REDACTED] must include:

- 1) (U//~~FOUO~~) [REDACTED]
- 2) (U//~~FOUO~~) [REDACTED]
- 3) (U//~~FOUO~~) [REDACTED]

b7E

B) (U//~~FOUO~~) [REDACTED]

18.7.1.6.2.8 (U) USE OF FISA DERIVED INFORMATION IN OTHER PROCEEDINGS

(U//~~FOUO~~) There are statutory (50 U.S.C. Sections 1806, 1825, and 1845) and Attorney General (AG) policy restrictions on the use of information derived from a FISA ELSUR, physical search, or PR/TT. These restrictions apply to and must be followed by anyone “who may seek to use or disclose FISA information in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States. . . .” See DIOG Appendix E for the AG Memo, Revised Policy on the Use or Disclosure of FISA Information, dated 01-10-2008. The guidance in the AG’s Memo establishes notification/approval procedures which must be strictly followed. Though not contained in the AG Memo, FBI policy requires that [REDACTED]

b7E

(U//~~FOUO~~) The United States must, prior to the trial, hearing, or other proceeding or at a reasonable time prior to an effort to disclose or use that information or submit it into evidence, notify the “aggrieved person” [as defined in 50 U.S.C. Sections 1801(k), 1821(2), or 1841(2)], and the court or other authority in which the information is to be disclosed or used, that the United States intends to disclose or use such information. See 50 U.S.C. Sections 1806(c), 1825(d), and 1845(c).

18.7.1.6.2.9 (U//~~FOUO~~)

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

A) (U//~~FOUO~~) [REDACTED]
and

B) (U//~~FOUO~~) [REDACTED]
[REDACTED]

b7E

18.7.1.6.2.10 (U//~~FOUO~~) FISA RENEWALS

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

b7E

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

(U//~~FOUO~~)18.7.1.6.2.10.1 (U) *APPEALING THE DECISION OF THE REVIEW BOARD*(U//~~FOUO~~)18.7.1.6.2.11 (U) **COMPLIANCE AND MONITORING FOR FISA**(U//~~FOUO~~)18.7.1.6.2.12 (U) **FISA OVERCOLLECTION**(U//~~FOUO~~)

[redacted] contact NSLB for further guidance regarding the handling of any FISA overcollection.

This Page is Intentionally Blank.

18.7.2 (U) *INVESTIGATIVE METHOD: ELECTRONIC SURVEILLANCE – TITLE III*

18.7.2.1 (U) SUMMARY

(U//~~FOUO~~) Electronic Surveillance (ELSUR) under Title III 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. 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. [REDACTED]

b7E

[REDACTED] Title III 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:* [REDACTED]

18.7.2.2 (U) LEGAL AUTHORITY

(U) Title III ELSUR is authorized by chapter 119, 18 U.S.C. §§ 2510-2522 (Title III of the Omnibus and Safe Streets Act of 1968).

18.7.2.3 (U) DEFINITION OF INVESTIGATIVE METHOD

(U) Title III 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.

18.7.2.4 (U) TITLE III GENERALLY

(U) With the prior approval of the Attorney General, or Attorney General's designee, the United States Attorney, by and through an AUSA, or the Strike Force Attorney, may apply to a federal judge for a court order authorizing the interception of wire, oral, or electronic communications relating to one or more of the offenses listed in Title III (18 U.S.C. § 2516). Judicial oversight continues throughout the operational phase of the electronic surveillance including the installation, monitoring, and handling of recording media.

(U) For purposes of obtaining review and approval for use of the method, Title III applications are considered to be either "sensitive" or "non-sensitive." The requirements for each are set forth below.

18.7.2.5 (U) STANDARDS FOR USE AND APPROVAL REQUIREMENTS FOR NON-SENSITIVE TITLE IIIS

(U//~~FOUO~~) An SAC is the authorizing official to approve all requests for "non-sensitive" Title III orders, including original, extension, and renewal applications. SAC approval of all

extensions and renewals is required to ensure that field office managers will allocate the resources necessary to use this method. Any delegation of SAC approval authority to an ASAC under this section must be in writing (See DIOG Section 3.4.3).

(U//~~FOUO~~) Prior to SAC approval referred to above, CDC or OGC review is required for the initial “non-sensitive” Title III order. Extensions and renewals sought within 30 days after the expiration of the original Title III order in non-sensitive Title IIIs do not require CDC review, unless requested by the SAC or designee. The CDC must review renewals sought more than 30 days after the expiration of the original Title III order.

(U//~~FOUO~~) There may be situations or unusual circumstances requiring the FBI to adopt an already existing Title III from another federal law enforcement agency. Such adoptions may only be done on a case-by-case basis, in exceptional circumstances, and subject to the requirements set forth herein relating to CDC review and SAC approval. Should the Title III proposed for adoption involve sensitive circumstances, it must also be handled in accordance with the approval and review requirements set forth below.

18.7.2.6 (U) STANDARDS FOR USE AND APPROVAL REQUIREMENTS FOR SENSITIVE TITLE IIIs

(U//~~FOUO~~) All Title III applications involving one of the seven “sensitive circumstances,” listed below, including all extensions and renewals, must be reviewed by OGC and approved by FBIHQ. The SAC, with the recommendation of the CDC, must determine whether the request involves sensitive circumstances. The term “sensitive circumstances” as used in this section relating to electronic surveillance under Title III is different from the term “sensitive investigative matters,” as used in conjunction with approval requirements for opening Assessments and Predicated Investigations, and is different from the term “sensitive monitoring circumstances” as used in conjunction with the approval requirements for consensual monitoring.

(U//~~FOUO~~) The field office must include a copy of the completed CDC checklist (FD-926) when forwarding the initial sensitive Title III applications to OGC and FBIHQ for review. After the initial submission, the CDC checklist must be completed by the appropriate OGC unit for all subsequent extensions or renewals of sensitive Title IIIs.

(U//~~FOUO~~) Although ultimate approval for sensitive Title IIIs is at the FBIHQ level, the SAC or ASAC must continue to review and approve the use of the method for all sensitive Title III applications as it relates to the allocation of resources within their field office.

(U//~~FOUO~~) The following five sensitive circumstances require the approval of a Deputy Assistant Director (DAD) or a higher level official from the Criminal Investigative Division (CID), Cyber Division, Counterterrorism Division (CTD), Weapons of Mass Destruction Directorate (WMDD), or Counterintelligence Division (CD), as appropriate, and such approvals must be documented in an EC:

- A) (U//~~FOUO~~) Significant privilege issues or First Amendment concerns (e.g., attorney-client privilege or other privileged conversations or interception of news media representatives);
- B) (U//~~FOUO~~) Significant privacy concerns are anticipated (e.g., placing a microphone in a bedroom or bathroom);

C) (U//~~FOUO~~) Application is based on “relaxed specificity” (i.e., “roving” interception) under 18 U.S.C. § 2518(11)(a) and (b);

D) (U//~~FOUO~~) Application concerns a Domestic Terrorism (DT), International Terrorism, or Espionage investigation; or

E) (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 Executive Assistant Director (EAD) for the Criminal Cyber Response and Services Branch or National Security Branch, or the respective Assistant Director for Criminal Investigative Division (CID), Cyber Division, Counterterrorism Division (CTD), Weapons of Mass Destruction Directorate (WMDD), or Counterintelligence Division (CD), and such approvals must be documented in an EC:

A) (U//~~FOUO~~) "Emergency" Title III interceptions (i.e., interceptions conducted prior to judicial approval under 18 U.S.C. § 2518(7)); or

B) (U//~~FOUO~~) It is anticipated that conversations of members of Congress, federal judges, high-level federal officials, high-level state executives, or members of a state judiciary or legislature will be intercepted.

(U//~~FOUO~~) “Sensitive circumstances” may develop at any point in time during the course of a Title III. For example, while an initial application for interceptions might not be considered sensitive, conversations intercepted thereafter of a high-level state executive would render any subsequent spinoffs, extensions, or renewals “sensitive” Title III requests.

18.7.2.7 (U) PROCEDURES FOR EMERGENCY TITLE III INTERCEPTIONS

(U//~~FOUO~~) 18 U.S.C. § 2518(7) provides that any investigative or law enforcement officer, specially designated by the Attorney General, Deputy Attorney General, or the Associate Attorney General, who reasonably determines that an emergency situation exists that requires communications to be intercepted before an order authorizing such interception can, with due diligence, be obtained, and there are grounds upon which an order could be entered authorizing interception, may intercept such communications.

(U//~~FOUO~~) Section 2518(7) postpones, rather than eliminates the need for judicial authorization. If the Attorney General, Deputy Attorney General, or the Associate Attorney General authorizes an appropriate FBI official to approve an emergency Title III interception, an after-the-fact application for an order approving the interception must be made in accordance with Title III to the appropriate Court, and an order obtained, within 48 hours after the interception has occurred or begins to occur.

(U//~~FOUO~~)

b7E

(U) 18 U.S.C. § 2518(7) defines an emergency situation as one involving:

- A) (U) immediate danger of death or serious physical injury to any person,
- B) (U) conspiratorial activities threatening the national security interest, or
- C) (U) conspiratorial activities characteristic of organized crime.

(U//~~FOUO~~) In all but the most unusual circumstances, the only situations likely to constitute an emergency by the Department of Justice (DOJ) are those involving an imminent threat to life, e.g., a kidnapping, hostage taking, or imminent terrorist activity.

18.7.2.7.1 (U) *OBTAINING EMERGENCY AUTHORIZATION*

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

b7E

[REDACTED]

A) (U//~~FOUO~~) [REDACTED]

[REDACTED]

B) (U//~~FOUO~~) [REDACTED]

[REDACTED]

C) (U//~~FOUO~~) [REDACTED]

[REDACTED]

D) (U//~~FOUO~~) [REDACTED]

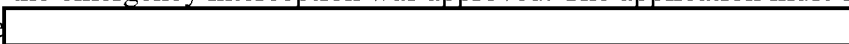
(U//~~FOUO~~) [REDACTED]

[REDACTED]



18.7.2.7.2 (U) *POST-EMERGENCY AUTHORIZATION*

(U//~~FOUO~~) Once the AG or his designee has authorized the Director, or his designee to make the determination whether to proceed with the emergency Title III, the government has 48 hours (including weekends and holidays) from the time the AG granted authorization to apply for a court order approving the interception. The field office, in coordination with the AUSA, must immediately begin preparing an affidavit, application and proposed order for court authorization.

(U//~~FOUO~~) The affidavit in support of the after-the-fact application to the court for an order approving the emergency interception must contain only those facts known to the AG or his designee at the time the emergency interception was approved. The application must be accompanied by the  form, which must reflect the date and time of the emergency authorization.

(U//~~FOUO~~) The government may also request, at the time it files for court-authorization for the emergency, court-authorization to continue the interception beyond the initial 48 hour period. If continued authorization is sought at the same time, one affidavit may be submitted in support of both requests. However, the affidavit must clearly indicate what information was communicated to the AG or his designee at the time the emergency interception was approved and what information was developed thereafter. Two separate applications and proposed orders should be submitted to the court in this situation – one set for the emergency and one set for the extension. If continued interceptions are not being sought, no further authorization is needed from OEO. The AUSA should, however, still submit the application, affidavit, and order to OEO for review. If continued interceptions are sought, that application, affidavit, and order must be reviewed by OEO and approved by DOJ like any other Title III request. In either situation, the affidavit must also be submitted through the operational unit for OGC review, when time allows.

(U//~~FOUO~~)



(U//~~FOUO~~) Pursuant to 18 U.S.C. § 2518(7), in the absence of a court order, interception shall immediately terminate when the communication sought is obtained or when the application for the order is denied, whichever is earlier. In the event an application for approval is denied, or in any other case where the interception is terminated without an order having been issued, the contents of any wire, oral, or electronic communication intercepted

shall be treated as having been obtained in violation of Title III, and an inventory shall be served on the person named in the application.

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

b7E

- A) (U//~~FOUO~~) [REDACTED]
- B) (U//~~FOUO~~) [REDACTED]
- C) (U//~~FOUO~~) [REDACTED]

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

- A) (U//~~FOUO~~) [REDACTED]
[REDACTED]
- B) (U//~~FOUO~~) [REDACTED]
[REDACTED]
- C) (U//~~FOUO~~) [REDACTED]
[REDACTED]

18.7.2.8 (U) **PRE-TITLE III ELECTRONIC SURVEILLANCE (ELSUR) SEARCH POLICY**

(U//~~FOUO~~) 18 U.S.C § 2518(1)(e) requires that each application for an order to intercept wire, oral, or electronic communications (hereinafter “Title III”) contain a statement describing all previous applications for Title III surveillance of the same persons, facilities, or places named in the current application. [REDACTED]

b7E

(U) For specific details on how to conduct and document such ELSUR searches, see DIOG Appendix H.

18.7.2.9 (U) **DURATION OF APPROVAL FOR TITLE III**

(U) Court orders issued pursuant to Title III are for a period not to exceed 30 days. 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 and facilities identified in the original order. 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.

18.7.2.10 (U) **SPECIFIC PROCEDURES FOR TITLE III AFFIDAVITS**

(U//~~FOUO~~) The requirements in 18 U.S.C. § 2518 must be followed in the preparation of a Title III affidavit. The employee drafting the Title III affidavit and approving officials must consider the following requirements:

- A) (U//~~FOUO~~) The identity and qualifications of the affiant must be articulated;

- B) (U//~~FOUO~~) For the interception of wire or oral communications, the affidavit must establish probable cause to believe a violation of at least one of the offenses enumerated in 18 U.S.C. § 2516(1) has been, is being, or will be committed. For the interception of electronic communications, the affidavit must establish probable cause to believe that some federal felony has been, is being, or will be committed;
- C) (U//~~FOUO~~) The affidavit must set forth the identities of those persons, if known, for whom there is probable cause to believe they are committing the alleged offenses, even if it is not believed they will be intercepted over the target facility. This group of individuals is often referred to as the "Subjects." "Interceptees" may be listed separately; "interceptee" are those Subjects who are expected to be intercepted;
- D) (U//~~FOUO~~) Probable cause must be current and relevant to the use of the particular facilities for which interception is sought;
- E) (U//~~FOUO~~) The necessity for the Title III must be articulated. There must be a factual basis for concluding that alternative 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);
- F) (U//~~FOUO~~) Interceptions must be minimized, as statutorily required;
- G) (U//~~FOUO~~) The facility or premises to be intercepted must be described fully, including a diagram, if possible, if microphone installation is contemplated (surreptitious entries may not be conducted for the purpose of preparing a diagram); and
- H) (U//~~FOUO~~) A statement describing all previous applications for Title III surveillance of the same persons (both subjects and interceptees), facilities or places named in the current affidavit. To comply with this requirement, a "search," e.g., an automated indices search of the FBI's [REDACTED] system and the systems of other appropriate agencies, must be conducted prior to submitting the Title III affidavit to the DOJ OEO (non-sensitive circumstances) or to the responsible FBIHQ operational unit (sensitive circumstances). The squad SSA is responsible for verifying that pre-Title III ELSUR checks have been completed before the affidavit is sent to the court. The ELSUR Operations Technician (EOT) and the ELSUR supervisor are responsible for confirming that ELSUR searches were properly conducted as set forth in the final application submitted to the court.

b7E

(U//~~FOUO~~) Note: When drafting the Title III Affidavit, the agent must determine whether the proposed Title III intercept involves any of the DOJ-designated seven "sensitive circumstances" listed in DIOG Section 18.7.2.6. If the proposed Title III will involve one or more of the seven "sensitive circumstances," the agent must consult with the assigned AUSA to determine how the "sensitive circumstance(s)" will be addressed and how/when the federal judge will be notified.

(U//~~FOUO~~) Note: It is also recommended that the application include how the FBI will address any sensitive circumstances as listed in DIOG Section 18.7.2.6, if they exist.

(U//~~FOUO~~) At least 10 calendar days prior to submitting the original Title III request to DOJ OEO, the field office must forward an electronic communication to FBIHQ setting forth by separate subheading: a synopsis of the investigation; the priority of the investigation within the office; the anticipated manpower and/or linguistic requirements and outside support, if any, that will be needed; a synopsis of the probable cause supporting the Title III application; the prosecutive opinion of the USAO; and description of the interceptees. If a field office is unable to submit the EC 10 calendar days prior to submitting the request to DOJ OEO, the

field office must advise the operational unit immediately and note the circumstances that prevent timely notification.

(U//~~FOUO~~) Case agents must use the [REDACTED]

b7E

18.7.2.11 (U) **DISPUTE RESOLUTION FOR TITLE III APPLICATIONS**

(U//~~FOUO~~) When there are legal questions/concerns that cannot be resolved through discussions with reviewing officials at DOJ, the responsible FBIHQ operational division supervisors or executives must forward the application to OGC for its review, advice, and recommendation.

18.7.2.12 (U) **REPORTING AND NOTICE REQUIREMENTS – TITLE III**

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

b7E

[REDACTED]

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

b7E

[REDACTED]

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

[REDACTED]

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

b7E

[REDACTED]

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

[REDACTED]

(U//~~FOUO~~)

b7E

(U//~~FOUO~~)

b7E

(U//~~FOUO~~)

18.7.2.12.1 (U//~~FOUO~~) **NOTICE REQUIREMENTS FOR SENSITIVE INVESTIGATIVE MATTERS (SIM) THAT INVOLVE TITLE III INTERCEPTIONS**

(U//~~FOUO~~) The anticipated interception of conversations related to a “Sensitive Investigative Matter” (SIM) as defined in DIOG Section 10 requires notice to the appropriate FBIHQ Unit Chief and Section Chief, and DOJ Criminal Division. Note: A sensitive investigative matter (SIM) is not the same as a sensitive circumstance described in DIOG Section 18.7.2.6.

18.7.2.13 (U) **JOINT TITLE III OPERATIONS WITH OTHER LAW ENFORCEMENT AGENCIES**

18.7.2.13.1 (U) **FEDERAL LAW ENFORCEMENT AGENCIES**

(U//~~FOUO~~) In joint FBI operations with other federal law enforcement agencies wherein electronic surveillance is conducted through a Title III installation, the federal agency administering the electronic surveillance will assume overall responsibility for ELSUR indexing and recordkeeping. The fact that the investigation is a joint operation with another federal law enforcement agency must be stated in the affidavit and application for the court order. The joint federal agency must provide the FBI case agent with a copy of the court order and application.

(U//~~FOUO~~)

b7E

18.7.2.13.2 (U) **STATE AND LOCAL LAW ENFORCEMENT AGENCIES**

(U//~~FOUO~~) In joint FBI operations involving state and local law enforcement agencies wherein electronic surveillance is conducted through a federal Title III installation, any state

officer being used as an affiant must be federally deputized. The FBI will be the administering agency responsible for the indexing and recordkeeping.

(U//~~FOUO~~) In joint FBI operations involving state and local law enforcement agencies wherein electronic surveillance is conducted pursuant to the authorization of a state court (i.e., a wiretap authorized by a state court, as opposed to a federal court),

b7E



18.7.2.14 (U) EVIDENCE HANDLING

(U//~~FOUO~~) All ELSUR downloading, processing, and handling of original, derivative, and copies of original or derivative ELSUR evidence must be conducted by an ELSUR operations technician (EOT) or other designated employee (e.g. an agent who has successfully completed ELSUR training in Virtual Academy). ELSUR evidence must not be uploaded into

This Page is Intentionally Blank

18.7.3 (U) **INVESTIGATIVE METHOD: ELECTRONIC SURVEILLANCE – FISA AND FISA TITLE VII (ACQUISITION OF FOREIGN INTELLIGENCE INFORMATION)**

18.7.3.1 (U) **SUMMARY**

(U//~~FOUO~~) ELSUR conducted pursuant to the Foreign Intelligence Surveillance Act (FISA) is a valuable investigative method. It is, also, a very intrusive means of acquiring information relevant to the effective execution of the FBI's national security and intelligence missions. To ensure that due consideration is given to the competing interests between national security 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. FISA ELSUR is only authorized as an investigative method in the conduct of Full Investigations. FISA ELSUR requires administrative or judicial authorization prior to its use.

(U//~~FOUO~~) Coordination:

b7E

(U//~~FOUO~~) Application:

b7E

(U) This section is divided below into FISA (18.7.3.2) and FISA Title VII (18.7.3.3).

18.7.3.2 (U) **FOREIGN INTELLIGENCE SURVEILLANCE ACT (FISA)**

18.7.3.2.1 (U) **LEGAL AUTHORITY**

(U) 50 U.S.C. §§ 1801-1811 (FISA) and E.O. 12333 § 2.5.

(U) FISA Amendments Act of 2008 (P.L.No. 110-261).

18.7.3.2.2 (U) DEFINITION OF INVESTIGATIVE METHOD

(U) FISA 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.

18.7.3.2.3 (U) STANDARDS FOR USE AND APPROVAL REQUIREMENTS FOR FISA**18.7.3.2.3.1 (U) FISA REQUEST FORM**

(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 [REDACTED] 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.

b7E

(U//~~FOUO~~) See [REDACTED] for additional guidance.

18.7.3.2.3.2 (U) CERTIFICATE BY THE DIRECTOR OF THE FBI

(U) Each FISA application must be accompanied by 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 information cannot reasonably be obtained by normal investigative techniques; that the information sought is "foreign intelligence information" as defined by FISA. The certification must include a statement explaining the certifier's basis for the certification.

(U) 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. The FBI Director has represented to Congress that the FBI Deputy Director will only certify FISA's when the FBI Director is not available to do so.

18.7.3.2.3.3 (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 opened, 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 USPER 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~~)

b7E

18.7.3.2.4 (U) *DURATION OF APPROVAL FOR FISA*

(U//~~FOUO~~)

18.7.3.2.5 (U//~~FOUO~~) *SPECIFIC PROCEDURES FOR FISA*

(U//~~FOUO~~) FISA related initiation and renewal procedures are contained within the FISA Initiation Form which can be found within [REDACTED] or on the Forms section of the NSLB library.

18.7.3.2.5.1 (U//~~FOUO~~) *FISA VERIFICATION OF ACCURACY PROCEDURES*

(U//~~FOUO~~)

b7E

(U//~~FOUO~~)

(U//~~FOUO~~)

A) (U//~~FOUO~~)

1) (U//~~FOUO~~)

2) (U//~~FOUO~~)

[REDACTED]

3) (U//~~FOUO~~) [REDACTED]

b7E

[REDACTED]

B) (U//~~FOUO~~) [REDACTED]

[REDACTED]

18.7.3.2.5.2 (U) **USE OF FISA DERIVED INFORMATION IN OTHER PROCEEDINGS**

(U//~~FOUO~~) There are statutory (50 U.S.C. Sections 1806, 1825, and 1845) and Attorney General (AG) policy restrictions on the use of information derived from a FISA ELSUR, physical search, or PR/TT. These restrictions apply to and must be followed by anyone “who may seek to use or disclose FISA information in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States. . . .” See DIOG Appendix E for the AG Memo, Revised Policy on the Use or Disclosure of FISA Information, dated 01-10-2008. The guidance in the AG’s Memo establishes notification/approval procedures which must be strictly followed. Though not contained in the AG Memo, FBI policy requires that [REDACTED]

b7E

[REDACTED]

(U//~~FOUO~~) The United States must, prior to the trial, hearing, or other proceeding or at a reasonable time prior to an effort to disclose or use that information or submit it into evidence, notify the “aggrieved person” [as defined in 50 U.S.C. Sections 1801(k), 1821(2), or 1841(2)], and the court or other authority in which the information is to be disclosed or used, that the United States intends to disclose or use such information. See 50 U.S.C. Sections 1806(c), 1825(d), and 1845(c).

18.7.3.2.5.3 (U//~~FOUO~~) **FISA ELECTRONIC SURVEILLANCE ADMINISTRATIVE (FISA ELSUR) SUB-FILE**

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

[REDACTED]

[REDACTED]

b7E

A) (U//~~FOUO~~) [REDACTED]

[REDACTED]

B) (U//~~FOUO~~) [REDACTED]

18.7.3.2.5.4 (U//~~FOUO~~) FISA REVIEW BOARD

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

b7E

[REDACTED]

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

[REDACTED]

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

[REDACTED]

18.7.3.2.5.4.1 (U) *APPEALING THE DECISION OF THE REVIEW BOARD*

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

[REDACTED]

18.7.3.2.6 (U) *NOTICE AND REPORTING REQUIREMENTS FOR FISA*

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

[REDACTED]

18.7.3.2.7 (U) *COMPLIANCE AND MONITORING FOR FISA*

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

b7E

[REDACTED]

18.7.3.2.8 (U) *SPECIAL CIRCUMSTANCES FOR 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 USPERs are parties.

18.7.3.2.9 (U) *FISA OVERCOLLECTION*

(U//~~FOUO~~)

[REDACTED]

b7E

contact NSLB for guidance regarding the handling of any FISA overcollection.

18.7.3.2.10 (U) *OTHER APPLICABLE POLICIES*

18.7.3.2.10.1 (U) *FISA*

A) (U//~~FOUO~~) Counterintelligence Division Policy Guide, 0717DPG

B) (U//~~FOUO~~) Counterterrorism Policy Guide, 0775DPG

C) (U//~~FOUO~~) Investigative Law Unit Library

D) (U//~~FOUO~~) Foreign Intelligence Surveillance Act (FISA) Unit

18.7.3.2.11 (U) *COLLECTION HANDLING*

(U//~~FOUO~~) All ELSUR downloading, processing, and handling of original, derivative, and copies of original or derivative ELSUR evidence must be conducted by an ELSUR operations technician (EOT) or other designated official (e.g. an agent who has successfully completed ELSUR training in Virtual Academy). ELSUR evidence must not be uploaded into [REDACTED]

b7E

18.7.3.2.11.1 (U) *DOWNLOADING, HANDLING, AND STORAGE OF FISA
INTERCEPT MEDIA FOR USE AS ORIGINAL EVIDENCE*

(U//~~FOUO~~)

[REDACTED]

b7E

(U//~~FOUO~~)

[REDACTED]

(U//~~FOUO~~)

[REDACTED]

(U//~~FOUO~~)

b7E

1) (U//~~FOUO~~)

2) (U)

3) (U//~~FOUO~~)

18.7.3.3 (U) FISA TITLE VII (ACQUISITION OF FOREIGN INTELLIGENCE INFORMATION)**18.7.3.3.1 (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 USPERs and non-USPERs) and foreign establishments inside the United States. Title VII of FISA, “Additional Procedures Regarding Certain Persons Outside the United States,” provides the means to target non-USPERs reasonably believed to be located outside the United States.

18.7.3.3.2 (U) LEGAL AUTHORITY

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

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

18.7.3.3.3 (U) DEFINITION OF INVESTIGATIVE METHOD

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

18.7.3.3.4 (U//~~FOUO~~) STANDARDS FOR USE AND APPROVAL REQUIREMENTS FOR INVESTIGATIVE METHOD

(U//~~FOUO~~) See requirements under DIOG Sections 18.7.1, 18.7.2, and 18.7.3 and requirements specified above.

18.7.3.3.5 (U) DURATION OF APPROVAL

(U//~~FOUO~~) See requirements under DIOG Sections 18.7.1, 18.7.2, and 18.7.3 above.

18.7.3.3.6 (U//~~FOUO~~) SPECIFIC COLLECTION PROCEDURES FOR TITLE VII

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

18.7.3.3.6.1 (U) SECTION 702 - PROCEDURES FOR TARGETING NON-U.S.**PERSONS (NON-USPERs) WHO ARE OUTSIDE THE UNITED STATES**

(U//~~FOUO~~) Under Section 702, the Government has the authority to target non-USPERs who are located outside the United States if the collection is effected with the assistance of an electronic communication service provider, as that term is defined in FISA. This section does not require a traditional FISA request. Rather, under this section, the Attorney General and the Director of National Intelligence may authorize, for periods of up to one year, the targeting of non-United States persons reasonably believed to be located outside the United States to acquire foreign intelligence information, provided they execute a Certification that is submitted to and approved by the FISC. The Certifications are accompanied by an affidavit signed by the FBI Director. In addition, the FBI is required to file "Targeting Procedures" that ensure that only non-U.S. persons (non-USPERs) reasonably believed to be located outside the United States will be targeted for collection 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." Additionally, the statute prohibits targeting any person reasonably believed to be located outside the United States for the purpose of obtaining

the communications of a particular, known person reasonably believed to be in the United States. Finally, the FBI is also required to follow 702-specific minimization procedures.

18.7.3.3.6.2 (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 USPERs who are reasonably believed to be 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, e.g., non-consensual collection. FISA 703 is an alternative to traditional FISA electronic surveillance (Title I) or physical search (Title III) authority when the facts meet the 703 criteria. There are two notable differences between Section 703 and traditional FISA authorities. First, although the application must identify any electronic communication service provider necessary to effect the acquisition, the application is not required to identify the specific facilities, places, premises, or property at which the acquisition will be directed. Second, Section 703 allows for the targeting of a USPER who is “an officer or employee of a foreign power,” even if the target is not knowingly engaging in clandestine intelligence gathering activities, sabotage, or international terrorism. To obtain authority to collect information under this section, the FBI must submit a FISA request and obtain a FISC order and secondary orders, as needed. The process to obtain that order is the same as the standard FISA process. Refer to the FISA Unit's website for further information. Section 703 also allows for emergency authorization. Unlike traditional FISA orders, however, surveillance authorized pursuant to this section must cease immediately if the target enters the United States. If the FBI wishes to continue surveillance of the USPER 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 conduct electronic surveillance or a physical search of that USPER while the person is located in the United States. The use of any information collected using FISA 703 authority must comply with the applicable minimization procedures.

18.7.3.3.6.3 (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 USPERs who are reasonably believed to be located outside the United States if the collection occurs outside the United States (i.e. without the assistance of a United States' electronic communication service provider). The statute requires that the FISA court issue an order finding probable cause to believe that the USPER target is a foreign power, an agent of a foreign power, or an officer or employee of a foreign power and is 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." To obtain authority to collect information under this section, the FBI must submit a FISA request and obtain a FISC order (the order will not include secondary orders). The

process to obtain a FISA 704 order is similar to, but more streamlined than, that for obtaining a traditional FISA under the standard FISA process. There are two notable differences between Section 704 and traditional FISA authorities. First, the application is not required to identify the specific facilities, places, premises, or property at which the acquisition will be directed. Second, Section 704 allows for the targeting of “an officer or employee of a foreign power” even if the target is not knowingly engaging in clandestine intelligence gathering activities, sabotage, or international terrorism. Refer to the FISA Unit's intranet website for further information. Section 704 also allows for emergency authorization. Unlike traditional FISA orders, however, surveillance authorized pursuant to this section must cease if the USPER 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. If there is a need to continue surveillance while the target is located inside the United States a separate court order must be obtained. The use of any information collected using FISA 704 authority must comply with the applicable minimization procedures.

(U//~~FOUO~~)

b7E

18.7.3.3.6.4 (U) SECTION 705 - JOINT APPLICATIONS AND CONCURRENT AUTHORIZATIONS

(U//~~FOUO~~) Section 705(a) “joint applications” allow the FISC, upon request of the FBI, to approve a joint application targeting an USPER under both Sections 703 and 704 (authority to collect both when the facilities are located inside and outside the United States).

(U//~~FOUO~~) Section 705(b) provides 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 the USPER target 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, when the FISA Court authorizes surveillance of an USPER target, the Attorney General, under Section 705(b) and E.O 12333 § 2.5, can simultaneously authorize surveillance to continue if the target travels outside the United States during the authorized period of the surveillance. According to Section 705(b), there is no need for a separate order pursuant to Section 703 or 704. During the FISA drafting process, an FBI employee should determine whether surveillance or physical search may occur for purpose of acquiring foreign intelligence while the person is reasonably believed to be outside the United States. If so, the FBI employee should consult with an OGC or DOJ-NSD attorney to ensure that appropriate language is added to the application.

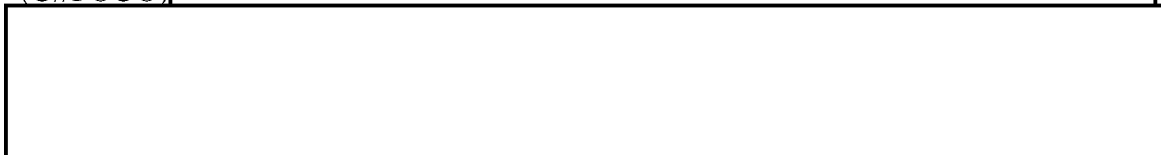
(U//~~FOUO~~)

b7E

18.7.3.3.6.5 (U) FISA OVERCOLLECTION

(U//~~FOUO~~)

b7E



This Page is Intentionally Blank

19 (U) ARREST PROCEDURE POLICY

19.1 (U) ARREST WARRANTS

19.1.1 (U) COMPLAINTS

(U) A complaint is a written statement of the facts necessary to establish probable cause to believe that an offense has been committed and that the defendant committed it. A complaint is presented under oath before a magistrate judge, who may issue an arrest warrant or a summons for the defendant if he/she finds the complaint establishes probable cause to believe the defendant committed the charged offense.

19.1.2 (U) ARREST WARRANTS

(U) Any justice, judge or magistrate judge of the United States has the authority to issue arrest warrants for any offense against the United States. In addition, if a federal magistrate judge is not reasonably available a state or local judicial officer where the offender may be found can issue the warrant. Copies of warrants issued under this authority are returned to the court of the United States that has jurisdiction over the offense.

19.1.3 (U) JURISDICTION

(U) Federal rules do not limit the application for an arrest warrant to any specified district. Usually, an application for a warrant will be made in the district where the offense was committed, but it may also be issued by a magistrate judge in the district where the offender is located.

19.1.4 (U) PERSON TO BE ARRESTED

(U) An arrest warrant must contain the name of the defendant or, if his/her name is unknown, any name or description by which the defendant can be identified with reasonable certainty. There is no requirement to determine the defendant's true name before a warrant can be issued. It is sufficient to develop facts which provide a reasonable belief that a particular individual is the offender. A warrant can be based on facts that provide a distinguishing physical description or describe the particular circumstances in which the defendant can be found.

19.2 (U) ARREST WITH WARRANT

19.2.1 (U) POLICY

(U) Whenever possible, an arrest warrant must be obtained prior to an arrest. SSAs may authorize agents⁴⁹ to execute arrest warrants and, in extraordinary circumstances, FBIHQ should be notified in advance of the arrest. For example, SSAs should notify FBIHQ when the arrest may have a significant impact on an investigation in another field office or when the arrest is

⁴⁹ (U) The term "agent" in the context of this section includes FBI special agents and other federal, state, tribal, or local law enforcement officers who have been deputized under either Title 18 or 21 of the United States Code and are working on behalf of or at the direction of the FBI, e.g. task force officer, JTTF, etc.

likely to cause widespread publicity due to the identity or status of the arrestee or the nature of the crime.

(U) Upon the execution of an arrest warrant, the apprehending field office/division must promptly enter a “locate” within NCIC. The Office of Origin (OO) of the warrant must enter a “clear” within NCIC within 24 hours of the “locate.” See the National Crime Information Center (NCIC) Field Office Guide, 0145PG for detailed NCIC policy. Also see DIOG subsection 19.4.4 (Initial Processing) below.

19.2.2 (U) **PROMPT EXECUTION**

(U) While there is no time limit on the execution of arrest warrants (unlike search warrants), as a general rule agents should make the arrest without prolonged delay after obtaining the warrant.

19.2.3 (U) **ARREST PLANS**

(U) The ADIC/SAC is responsible to ensure that careful and thorough planning is conducted for the successful execution of any high risk arrest operation involving a potentially dangerous situation or subject. The arrest plan must be adapted to each situation with relevant details for the safety and effectiveness of all agents and officers involved. The planning and execution of arrests, raids, and searches should be assigned to experienced agents. All arrest plans must be approved by ASACs or their designees.

(U) Prior to conducting an arrest operation deemed a high risk, the agent must prepare a written operation order (OPORDER) to include the five critical categories: Situation, Mission, Execution, Administration and Equipment, and Control and Communication (SMEAC), and must utilize the Law Enforcement Operations Order (OPORDER), FD-888 in situations where an FBI SWAT Team(s) or the Critical Incident Response Group’s (CIRG), Tactical Section is involved, the Operations Order Template must be used in lieu of the FD-888. See the [REDACTED]

[REDACTED] and [REDACTED] for more on the use of the SWAT Teams and CIRG’s Tactical Section in high risk operations.

(U) The written OPORDER must be presented in an oral briefing to all personnel involved in the execution of the arrest warrant(s) prior to the operation. During the briefing, the briefing agent should stress to the participants of the operation that the arrest(s) has the potential to become dangerous. At the discretion of the field office approving official, the CDC/ADC may review the OPORDER (FD-888) and/or participate in providing the FBI deadly force briefing to the arrest operation participants.

(U) Exigent circumstances (i.e., emergency, pressing necessity requiring immediate action) may necessitate an oral briefing in lieu of the written OPORDER. The ASAC or designee must approve the use of an oral briefing in lieu of a written and approved OPORDER in exigent circumstances. An oral briefing must follow the requirements of a written OPORDER and include the SMEAC categories identified above. Documentation of the oral briefing must occur as soon as possible following the operation by preparing and filing the FD-888 or the Operations Order Template, whichever is appropriate for the situation.

(U) The SSA may consider utilizing, and/or alerting local authorities to the planned arrest, if appropriate under the circumstances. Although the time of notification is left to the discretion of

b7E

the SSA, he/she must consider the jurisdiction of local law enforcement, its responsibility to its community and its need to be aware of law enforcement actions in its jurisdiction.

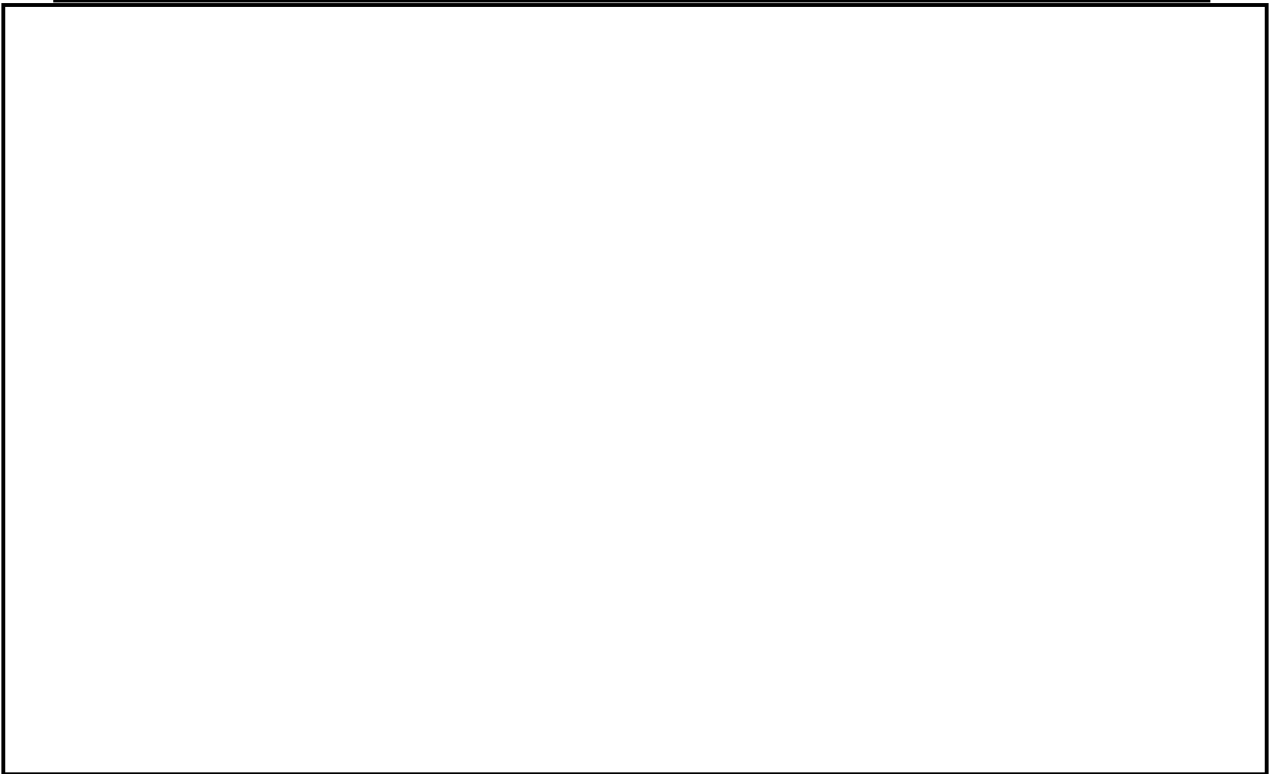
(U) The squad supervisor must be notified of the presence in FBI office space of any person(s) under arrest or of the presence of any suspect(s) for whom arrest is contemplated.

19.2.4 (U) *ARREST TECHNIQUES – GENERAL*

(U)

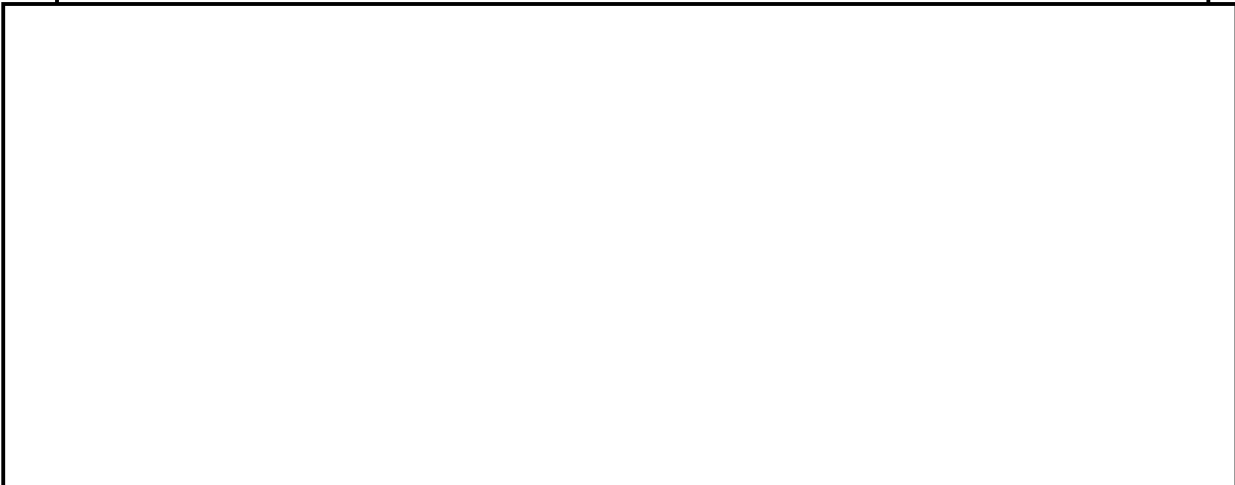


b7E



19.2.4.1 (U) *INITIAL APPROACH DURING AN ARREST OPERATION*

(U)



[REDACTED]

b7E

(U) [REDACTED]

[REDACTED]

19.2.4.2 (U) POSSESSION AND DISPLAY OF WARRANT

(U) If time permits, the arresting agent should have the arrest warrant in his/her possession and show it to the defendant at the time of arrest. If the agent does not have the warrant with him/her at the time of arrest, the agent must inform the defendant of the offense(s) charged and that a warrant has been issued. The agent must, at the defendant's request, obtain the warrant and show it to the defendant as soon as practicable.

19.2.4.3 (U) HANDCUFFING

(U) [REDACTED]

b7E

[REDACTED]

19.2.4.4 (U) SEARCH OF THE PERSON INCIDENT TO ARREST

19.2.4.4.1 (U) *HIGH-RISK SEARCH/FULL-BODY SEARCH*

(U) [REDACTED]

b7E

[REDACTED]

(U) [REDACTED]

[REDACTED]

[Redacted]

(U) [Redacted]

[Redacted]

19.2.4.4.2 (U) *FINAL SEARCH AND COLLECTION OF EVIDENCE*

b7E

(U) [Redacted]

[Redacted]

(U) [Redacted]

[Redacted]

19.2.4.5 (U) *TRANSPORTATION OF ARRESTED PERSONS*

(U) [Redacted]

b7E

[Redacted]

(U) [Redacted]

[Redacted]



(U)



19.2.4.6 (U) **JOINT ARRESTS**

(U) An SSA may authorize a joint arrest with state and local authorities, United States Marshals Service (USMS), or other federal law enforcement agencies. In circumstances of joint arrests, the SAC remains responsible to ensure that there is a well-considered arrest plan.

19.2.4.7 (U) **EYEWITNESS IDENTIFICATIONS**

(U) See  for guidance on gathering eyewitness identifications of suspects during an investigation.

b7E

19.3 (U) **ARREST WITHOUT WARRANT**

19.3.1 (U) **FEDERAL CRIMES**

(U) Whenever possible, SAC and USAO authority must be obtained before making a warrantless arrest. Agents are authorized to make warrantless arrests for any federal crime (felony or misdemeanor) committed in their presence. Agents also have authority to make warrantless felony arrests for a crime not committed in the presence of the agent if there is probable cause to believe the person to be arrested committed a federal felony. A warrantless arrest must only be made when sound judgment indicates obtaining a warrant would unduly burden the investigation or substantially increase the potential for danger or escape. See DIOG subsection 19.3.3. (Non-Federal Crimes below.)

19.3.2 (U) **NOTIFICATION TO U.S. ATTORNEY**

(U) When a warrantless arrest has been made, the USAO must be contacted immediately for authorization to prosecute.

19.3.3 (U) *NON-FEDERAL CRIMES*

(U) There is no federal statutory authority for agents to intervene in non-federal (state) crimes. However, FBI policy permits certain types of non-federal arrests in exigent circumstances.

(U) As a general rule, an agent should only make an arrest for a state crime if a serious offense (felony or violent misdemeanor) has been committed in his or her presence and immediate action by the agent is necessary to prevent escape, serious bodily injury, or destruction of property.

(U) Agents are also authorized to arrest a person who is the subject of an FBI Predicated Investigation when a state or local arrest warrant for that person is outstanding, and the person is encountered during the investigation and would likely escape if not arrested. Similarly, an agent working with state or local law enforcement officers who request assistance to apprehend a non-federal fugitive who has been encountered during the course of a federal investigation is authorized to provide the requested assistance when intervention is otherwise permitted for a state crime as described in the preceding paragraph.

(U) In some states, there is legislative authority for an agent to intervene in certain types of state crimes as a peace officer rather than as a private citizen. Deputation or statutory recognition as a state peace officer allows a federal agent to make arrests for state offenses with the authority and immunities of a law enforcement officer of the state or one of its subdivisions. Of greater significance is whether intervention by an agent in a particular non-federal crime falls within the scope of employment. Agents who intervene in serious nonfederal crimes committed in their presence or who arrest a state fugitive under the circumstances previously described will normally be considered to be acting within the scope of their employment. While the determination to provide legal representation depends on the facts and circumstances of each circumstance, the DOJ, as a general rule, will provide legal representation to agents who act in accordance with this policy.

(U) It is important to note that the DOJ has indicated that efforts to enforce minor infractions of the law, such as shoplifting or traffic violations, are not generally considered to be within the scope of employment. Civil actions against federal personnel concerning acts which fall outside the scope of employment will not be removed to federal courts, and employees in such circumstances will not be eligible for legal representation provided for by the DOJ. An agent's status with respect to civil liability in such circumstances will depend on a particular state's law, which may require an employee to defend himself/herself as an ordinary citizen.

19.3.4 (U) *ADHERENCE TO FBI POLICY*

(U) If any official in the USAO instructs an agent to arrest or detain a subject in any manner contrary to FBI rules and regulations, the agent must not comply with such instructions and must immediately inform the SSA. (See the special rules in DIOG 19.12 below for the arrest of juveniles.)

19.4 (U) **PROMPT APPEARANCE BEFORE MAGISTRATE**

(U) When a federal arrest is made, the arrestee must be taken before a federal magistrate judge without unnecessary delay. If a federal magistrate judge is not available, the arrestee may be brought before a state or local judicial officer authorized by 18 U.S.C. § 3041 after consultation with the USAO.

(U) Special Considerations for Unlawful Flight to Avoid Prosecution (UFAP) Arrests: If the arrestee was arrested on a warrant charging only a violation of UFAP, the arrestee can be transferred without unnecessary delay to the custody of the appropriate state or local authorities in the district of arrest. The USAO in the originating district will move promptly to dismiss the UFAP warrant. It is not necessary to wait until the UFAP warrant has been dismissed to release the subject to state or local authorities, but it is important for the agent to ensure that the USAO dismisses the UFAP warrant promptly after the arrest.

(U) If an agent makes a warrantless arrest, a complaint must be filed setting forth the probable cause. The complaint is generally submitted when the arrestee is brought before the magistrate. A personal, telephonic, or electronic presentation to the magistrate of the facts setting forth the probable cause must occur within 48 hours of a warrantless arrest if the arrestee is detained and an initial appearance cannot be held within that 48-hour period.

19.4.1 (U) *DEFINITION OF UNNECESSARY DELAY*

(U) Rule 5 of the Federal Rules of Criminal Procedure requires the arresting agent to bring the accused before a federal magistrate judge without unnecessary delay. What constitutes “unnecessary delay” is determined in light of all the facts and circumstances. Confessions obtained from defendants during periods of unnecessary delay prior to initial appearance are generally inadmissible at trial. As a general rule, a voluntary confession within six (6) hours of arrest is not considered a product of unnecessary delay. The six-hour period begins when the accused is arrested or taken into custody by federal law enforcement authorities on a federal charge and runs continuously. The six (6) hour safe harbor can be extended to include delays found by the trial judge to be reasonable considering the means of transportation and the distance to be traveled to the nearest available magistrate judge. Delay solely for the purpose of conducting interrogation is not permitted. Delays for many other reasons may be justified and will not result in suppression of a statement, particularly when there is no indication that the purpose of the delay was to extract a confession (See DIOG subsections 19.4.2 and 19.4.3). For example, courts have found delays beyond six hours to be justified when attributable to the defendant’s need for medical treatment, his intoxication, the agents’ need to remain at the scene, the unavailability of a magistrate, and booking or other legitimate law enforcement procedures unrelated to interrogation.

(U) To avoid the risk that a court will determine that delay beyond the safe-harbor period was “unnecessary” and suppress a confession elicited more than six (6) hours after arrest, agents who want to continue or resume an interrogation after six (6) hours must seek a waiver of the right to prompt presentment from the accused. To continue an interrogation after six hours have elapsed, agents must advise the suspect of his Rule 5 rights, and seek an affirmative waiver of those rights from him. The warning and waiver must be substantially in accord with this approved waiver language:

(U) “You have a right to be taken without unnecessary delay to court, where a judge will advise you of the charges against you and provide you with a copy of any affidavit the government has filed in support of these charges. The judge will also advise you of the rights I advised you of previously, namely, that you have a right to an attorney and to have an attorney appointed for you; that you have a right to remain silent and that any statement you make may be used against you. The judge will also tell you if you have a right to a preliminary hearing, and that

if you do, the government will have to establish that the charges in the complaint are supported by probable cause. The judge will also tell you about the factors that will determine whether you can be released from custody prior to trial. Do you understand this right and are you willing to waive it and continue to talk to us?"

(U) It is prudent to obtain a waiver of the right to prompt presentment in any circumstance when interrogation extends beyond the six-hour safe-harbor period.

19.4.2 (U) *EFFECT OF UNNECESSARY DELAY*

(U) Incriminating statements obtained during any period of unnecessary delay after arrest and prior to the initial appearance before a Magistrate Judge are subject to suppression.

19.4.3 (U) *NECESSARY DELAY*

(U) If the delay in bringing an arrested person before the magistrate judge is greater than six hours and a confession is obtained after six hours, the government has the burden of proving the delay was reasonable. Some factors which could contribute to a finding that a delay beyond six hours were reasonable are the means of transportation, the distance to the nearest available magistrate judge and the time and day of the week of the arrest.

19.4.4 (U) *INITIAL PROCESSING*

(U) Following an arrest, the defendant should be brought to the nearest FBI office for fingerprinting, photographing, and an interview, where appropriate. Additionally, arresting agents and TFOs must be cognizant of the custodial recording policy. See DIOG subsection 18.5.6.4.17 for guidance on recording custodial interviews. Other law enforcement agency offices may be used for this purpose if FBI facilities are not reasonably available. This process generally should not exceed six hours, measured from the time of arrest to the time of arrival before the magistrate judge.

19.4.4.1 (U) *REQUESTS OF SUBJECTS IN CUSTODY*

(U) In all cases in which a Bureau subject is incarcerated either prior to or after initial appearance and plea, if the subject makes known to an agent during the course of an interview or otherwise his/her desire to be brought before the district court judge or to see a U.S. Marshal, immediate steps must be taken by the agent to advise the United States Attorney's Office (USAO) or U.S. Marshals Service of the desires of the subject.

19.4.5 (U) *COLLECTION OF DNA AFTER ARREST OR DETENTION*

(U) The Attorney General has directed the FBI to collect DNA samples from all arrestees, other than juveniles, and all non-U.S. persons (non-USPER) lawfully detained. A DNA sample should ordinarily be obtained during initial processing. FBI DNA collection kits should be used to collect a saliva sample from inside the person's mouth.

(U) There is no requirement to obtain a DNA sample from an individual who is arrested on an UFAP warrant when that individual will be turned over to the appropriate state/local agency with the expectation that the UFAP charge will be dismissed. A DNA sample should not be obtained

from an individual arrested on a UFAP warrant when there is no expectation of federal prosecution. For example, when it is anticipated that the UFAP charge will be dismissed and the individual turned over to the appropriate state/local agency, no DNA sample should be obtained.

(U) A DNA sample may not be taken from a juvenile arrestee. A DNA sample may only be taken from a juvenile after he/she has been convicted of certain drug or violent offenses.

(U) Federal law requires covered individuals to provide a DNA sample as a condition of pre-trial release and imposes criminal liability for failing to cooperate in the collection of the sample.

(U) The law also authorizes “such means as are reasonably necessary to detain, restrain, and collect a DNA sample from an individual who refuses to cooperate in the collection of the sample.” If resistance is encountered, agents must seek to elicit the cooperation of the individual to collect the sample. If the individual continues to resist, agents must advise the USAO or the judge and seek a judicial order requiring the individual to cooperate. If the individual still continues to resist after the court order, agents may use reasonable force to overcome resistance and safely obtain the DNA sample.

(U) For additional information on the process of collecting DNA samples from arrestees, see EC dated, 11/20/2009 from Laboratory to All Field Offices (319T-HQ-A1487667-LAB).

19.5 (U) USE OF FORCE

19.5.1 (U) IDENTIFICATION

(U) An arresting agent should identify himself/herself before effecting the arrest, in a clear, audible voice, as a special agent of the FBI and state his/her intention to arrest the subject.

19.5.2 (U) PHYSICAL FORCE

(U) Agents are permitted to use the amount of physical force reasonable and necessary to take custody and overcome all resistance of the arrestee, and to ensure the safety of the arresting agents, the arrestee and others in the vicinity of the arrest.

(U) See FBI Deadly Force Policy - Appendix F: (U) DOJ Policy on Use of Force.

(U) See Less Lethal Devices Policy Guide, 0517DPG.

19.5.3 (U) RESTRAINING DEVICES

(U) Temporary restraining devices, such as handcuffs, shackles and/or belts may be used to secure an arrestee. Use of such devices is lawful and proper, and agents are expected to employ reasonable judgment under the circumstances in the use of these devices and to resolve any doubt in favor of their use.

19.5.4 (U) PREGNANT ARRESTEES

(U) Within the standard operational procedures designed to ensure the successful completion of an operation and its immediate objectives, and while also guarding the safety of all involved, reasonable precautions and techniques should be employed when dealing with an arrestee reasonably believed to be pregnant to avoid harm to the fetus. This caution includes actions

involving confrontation, apprehension, employing restraints, transporting and confining the individual, and responding promptly to needed or requested medical care. In particular, reasonable care or precautions should be considered and used, if appropriate under the circumstances, when employing physical restraints that directly constrict the area of the fetus.

19.6 (U) MANNER OF ENTRY

19.6.1 (U) *KNOCK AND ANNOUNCE*

(U) Pursuant to 18 U.S.C. section 3109 and court decisions, agents are generally required to "knock and announce" their identity, authority and purpose, and demand to enter before entry is made to execute an arrest warrant in a private dwelling. This is part of the "reasonableness" requirement of the Fourth Amendment. The announcement can be given by one agent and need not be lengthy or elaborate but must convey to the person behind the door what is occurring. A loud announcement is essential and electronic devices designed to amplify the voice should be used where communication is anticipated to be difficult.

(U) the "knock and announce" requirement need not be complied with when the agent executing the warrant has a reasonable suspicion of one or more of the following:

(U) to "knock and announce" would cause the agent and/or another to be placed in imminent peril of bodily harm;

(U) to "knock and announce" would be a useless or futile gesture as the persons within the premises already know of the agent's identity, authority, and purpose;

(U) to "knock and announce" would cause the evidence sought under the warrant to be destroyed or removed; or

(U) to "knock and announce" would be reasonably likely to trigger an attempted escape of the person agents seek to arrest.

19.6.2 (U) *SUSPECT'S DWELLING*

(U) In order to lawfully enter a suspect's dwelling to effect an arrest, agents must have either: (i) consent to enter, (ii) an emergency ("hot pursuit") justifying a warrantless entry, or (iii) an arrest warrant and probable cause to believe the suspect is in the dwelling. In determining whether a location is the suspect's dwelling, an apartment, hotel, motel or boardinghouse room becomes the dwelling of the person renting or leasing it. If the suspect is not named on the lease or rental agreement, the dwelling may still be considered the suspect's dwelling if the suspect occupies the dwelling jointly with another.

19.6.3 (U) *THIRD PARTY DWELLING*

(U) In order to lawfully enter a third party's dwelling to arrest a suspect, agents must have either: (i) consent to enter, (ii) an emergency ("hot pursuit") justifying a warrantless entry, or (iii) a search warrant for the third party dwelling describing the person to be arrested. For these purposes, "third party dwelling" is any private dwelling other than the principal dwelling of the person to be arrested. For example, a search warrant would be necessary if the arrestee is a casual visitor, or temporary caller at the dwelling of the third party. In order to enter a private dwelling to effect an arrest, whether pursuant to an arrest warrant, search warrant, or exigent

circumstances, the agent must have probable cause to believe the suspect to be arrested is within the dwelling to be entered.

19.6.4 (U) *EXIGENT CIRCUMSTANCES*

(U) If an agent has a reasonable belief that the subject will flee before a warrant can be obtained, or there is a substantial likelihood that the subject will dispose of evidence before a warrant can be obtained or there is increased danger to agents or others if entry is delayed to obtain a warrant, exigent circumstances exist which may justify entry into a dwelling to make a warrantless arrest or entry into a third party dwelling without a search warrant to make an arrest.

19.7 (U) *SEARCH INCIDENT TO ARREST*

(U) The authority to search incident to an arrest is an exception to the warrant requirement. Under this exception, an agent may conduct a full and complete search of the person of the arrestee and the area within the arrestee's "immediate control." Immediate control means "the area from within which an arrestee might gain possession of a weapon or destructible evidence. The purpose for the exception is to protect the arresting agent, prevent escape, and preserve any evidence in possession of the arrestee. The right to search flows from the fact of arrest, not the nature of the crime for which the arrest has been made. A search incident to arrest must be made without delay and "roughly contemporaneous" with the arrest itself.

19.7.1 (U) *PREREQUISITE: LAWFUL ARREST*

(U) A search incident to arrest first requires a lawful custodial arrest based upon probable cause. A warranted arrest is presumptively lawful. As discussed below, authority to enter a subject's dwelling to arrest is limited.

(U) Entry into Suspect's Dwelling: If entering the defendant's dwelling to effect an arrest, agents must have either (i) consent to enter, (ii) an emergency ("hot pursuit"), or (iii) an arrest warrant and probable cause to believe that the defendant is inside the premises.

19.7.2 (U) *SCOPE AND TIMING REQUIREMENT*

19.7.2.1 (U) *SCOPE OF SEARCH*

(U) The agent is entitled to search the person of the arrestee and the area within the arrestee's immediate control for weapons, to prevent concealment or destruction of evidence, and to prevent concealment of any means of escape. The search may extend to any portable personal property in the arrestee's actual possession, such as clothing, purses, briefcases, grocery bags, etc. Items of personal property accessible to the arrestee, such as an unlocked desk drawer or unlocked suitcase, may be searched. Absent exigent circumstances or valid consent, inaccessible or locked items of personal property may not be searched incident to arrest.

(U) In order to search the contents of a cell phone, Agents must obtain a warrant, valid consent or otherwise have exigent circumstances. As such, the search incident to arrest exception to the warrant requirement does not extend to data in a cell phone or other personal electronic device carried on or about the arrestee.

(U) If there is probable cause to believe a cell phone or other personal electronic device contains evidence, it may be seized, but the agent must obtain a search warrant or otherwise rely upon an exception to warrant requirement, e.g. valid consent, exigency, etc. prior to actually searching the cell phone or other electronic device. That electronic evidence may be destroyed remotely does not constitute exigent circumstances unless there is probable cause that remote destruction is actually imminent in the specific situation as to the particular device.

19.7.2.2 (U) VEHICLES

(U) The interior passenger compartment of a vehicle may be searched incident to a recent occupant's arrest only if the arrestee is within reaching distance of the passenger compartment at the time of search or if it is reasonable to believe the vehicle contains evidence of the offense for which the person was arrested. A search incident to arrest of an arrestee's vehicle may not otherwise occur. For example, a search of the vehicle incident to an arrest would not be permitted after the occupant has been removed, handcuffed, and placed in a nearby FBI vehicle if the arrest was based on an outstanding arrest warrant for failure to appear. If a search of a vehicle incident to arrest can be done under the described circumstances, the permissible scope can include unlocked or otherwise accessible containers, such as glove compartments, luggage, bags, clothing, etc.

19.7.2.3 (U) CELL PHONES

(U) The contents of a cell phone have a reasonable expectation of privacy, and therefore, Agents must obtain a warrant to search the cell phone unless they obtain lawful consent or exigent circumstances exist.

(U) In addition, Agents may not search the contents of a cell phone in the possession of the arrestee incident to an arrest. This also includes a search incident to arrest of the contents of a cell phone found in a vehicle occupied by the arrestee. The automobile search exception to the warrant requirement does not apply for a warrantless search of a cell phone in a vehicle.

19.7.2.4 (U) PROTECTIVE SWEEP

(U) Agents may conduct a protective sweep of the areas immediately adjacent to the site of the arrest for the purpose of locating persons that may pose a threat to the safety of the agents or others. Additionally, a protective sweep of other areas beyond those immediately adjacent to the site of the arrest may be conducted if the agents have a reasonable suspicion, based on specific and articulable facts, that an individual who poses a danger to those present is in the area to be swept. Reasonable suspicion must be based on facts known to the agents, such as noises in an attic or the at-large status of a dangerous associate. A protective sweep must be limited to a brief inspection of those areas within the premises in which a person could hide. If an agent observes evidence in plain view while conducting a protective sweep, the evidence may be seized under the plain view doctrine.

19.7.2.5 (U) TIMING

(U) A search incident to arrest must be made contemporaneous to the time and place of arrest and before the arrestee is removed from the area. A more thorough search of the arrestee at the

FBI office or some other place to which the arrestee is transported is also permitted as a search incident to arrest. Additionally, agents may conduct protective sweeps as described above at the time of arrest.

19.7.3 (U) *INVENTORY OF PERSONAL PROPERTY*

(U) [REDACTED]

b7E

(U) [REDACTED]

(U) [REDACTED]

(U) [REDACTED]

(U) [REDACTED]

(U) [REDACTED]

(U) [REDACTED]

(U) [REDACTED]

(U) [REDACTED]

A) [REDACTED]

b7E

B)



(U) The following is an example to illustrate a circumstance under which an inventory search **cannot** not be conducted:

A)



19.8 (U) MEDICAL ATTENTION FOR ARRESTEES

(U) If a person in FBI custody complains of sickness or ill health or if it is reasonably apparent to agents that such a condition exists, arrangements should be made to afford such persons reasonable medical attention without delay. Agents must also be mindful of the health and well-being of any pregnant subject and make arrangements for medical attention when asked or when it is reasonably apparent that the subject or fetus needs medical attention. If the time required to obtain medical care may result in the passing of more than six hours between arrest and presentment, agents must document the basis for and the receipt of any medical attention given to the arrestee.

19.9 (U) ARREST OF FOREIGN NATIONALS

19.9.1 (U) *REQUIREMENTS PERTAINING TO FOREIGN NATIONALS*

(U) When a foreign national is arrested or detained, the arresting agent must advise him/her of the right to have his/her consular officials notified.

(U) In some situations, the nearest consular officials must be notified of the arrest or detention of a foreign national, regardless of the national's wishes.

(U) Consular officials are entitled to access to their nationals in detention and are entitled to provide consular assistance.

**19.9.2 (U) STEPS TO FOLLOW WHEN A FOREIGN NATIONAL IS ARRESTED OR
DETAINED**

(U) The arresting agent must determine the foreign national's country of citizenship. In the absence of other information, the arresting agent must assume that the country of citizenship is the country on whose passport or other travel documents the foreign national travels.

(U) If the foreign national's country is not on the mandatory notification list below:

(U) The arresting agent must promptly offer to notify the foreign national's consular officials of the arrest/detention. For a suggested statement to the foreign national, see Statement 1 below.

(U) If the foreign national asks that consular notification be given, the arresting agent must promptly notify the nearest appropriate consular official of the foreign national's arrest.

(U) If the foreign national's country is on the list of mandatory notification countries:

(U) The arresting agent must promptly notify the nearest appropriate consular official of the arrest/detention.

(U) The arresting agent must tell the foreign national that this notification will be made. A suggested statement to the foreign national is found at Statement 2 below.

(U) The arresting agent must keep a written record (EC or FD-302) in the investigative file that he/she provided appropriate notification to the arrestee and of the actions taken.

(U) Mandatory Notification Countries or Jurisdictions

Algeria	Guyana	Saint Lucia
Antigua and Barbuda	Hong Kong ⁵⁰	Saint Vincent and the Grenadines
Armenia	Hungary	Seychelles
Azerbaijan	Jamaica	Sierra Leone
Bahamas	Kazakhstan	Singapore
Barbados	Kiribati	Slovakia
Belarus	Kuwait	Tajikistan

⁵⁰ (U) Hong Kong reverted to Chinese sovereignty on July 1, 1997, and is now officially referred to as the Hong Kong Special Administrative Region. Under paragraph 3(f) (2) of the March 25, 1997, U.S.-China Agreement on the Maintenance of the U.S. Consulate General in the Hong Kong Special Administrative Region, U.S. officials are required to notify Chinese officials of the arrest or detention of persons bearing Hong Kong passports in the same manner as is required for persons bearing Chinese passports-- i.e., immediately and, in any event, within four days of the arrest or detention.

(U) Mandatory Notification Countries or Jurisdictions

Belize	Kyrgyzstan	Tanzania
Brunei	Malaysia	Tonga
Bulgaria	Malta	Trinidad and Tobago
China ⁵¹	Mauritius	Tunisia
Costa Rica	Moldova	Turkmenistan
Cyprus	Mongolia	Tuvalu
Czech Republic	Nigeria	Ukraine
Dominica	Philippines	United Kingdom ⁵²
Fiji	Poland (non-permanent residents only)	
Gambia	Romania	Uzbekistan
Georgia	Russia	Zambia
Ghana	Saint Kitts and Nevis	Zimbabwe
Grenada		

19.9.3 (U) SUGGESTED STATEMENTS TO ARRESTED OR DETAINED FOREIGN NATIONALS

19.9.3.1 (U) STATEMENT 1: WHEN CONSULAR NOTIFICATION IS AT THE FOREIGN NATIONAL'S OPTION

(U) You are entitled to have us notify your country's consular representatives here in the United States that you have been arrested or detained. A consular official from your country may be able to help you obtain legal counsel and may contact your family and visit you in

⁵¹ (U) Notification is not mandatory in the case of persons who carry "Republic of China" passports issued by Taiwan. Such persons must be informed without delay, that the nearest office of the Taipei Economic and Cultural Representative Office ("TECRO"), the unofficial entity representing Taiwan's interests in the United States, can be notified at their request.

⁵² (U) Mandatory notification is required for nationals of the British dependencies Anguilla, British Virgin Islands, Bermuda, Montserrat, and the Turks and Caicos Islands. Their nationals carry United Kingdom passports.

detention, among other things. If you want us to notify your country's consular officials, you can request notification now or at any time in the future. After your consular officials are notified, they may call or visit you. Do you want us to notify your country's consular officials?

19.9.3.2 (U) STATEMENT 2: WHEN CONSULAR NOTIFICATION IS MANDATORY

(U) Because of your nationality, we are required to notify your country's consular representatives here in the United States that you have been arrested or detained. After your consular officials are notified, they may call or visit you. You are not required to accept their assistance, but they may be able to help you obtain legal counsel and may contact your family and visit you in detention, among other things. We will notify your country's consular officials as soon as possible.

19.9.4 (U) DIPLOMATIC IMMUNITY

(U) Agents may not knowingly or intentionally enter the office or dwelling of a diplomat or a person with diplomatic immunity for the purpose of making an arrest, search, or seizure.

19.9.4.1 (U) TERRITORIAL IMMUNITY

(U) All embassies, legations, and consulates have territorial immunity. Consequently, no agent may attempt to enter any embassy, legation, or consulate for the purpose of making an arrest, search or seizure. This territorial immunity extends to both the offices and residences of ambassadors and ministers, but only to the office of a consul. A consul's residence does not enjoy territorial immunity.

19.9.4.2 (U) PERSONAL IMMUNITY

(U) Ambassadors and ministers, members of their staffs and domestic servants, and the immediate family members of a diplomatic officer have personal immunity, as do the immediate family members of the administrative and technical staff of a diplomatic mission. Consequently, no agent should attempt to arrest or detain any such person. The personal immunity applies to the staffs, domestic servants and immediate family members, regardless of citizenship. Ordinarily, consuls do not have personal immunity from arrest on misdemeanor charges. If the arrest of a consul is contemplated, immediately notify FBIHQ by telephone or electronic communication before any action is taken so that an appropriate check can be made with the Department of State to determine whether the consul involved has any special immunity.

19.10 (U) ARREST OF MEMBERS OF THE NEWS MEDIA

(U) Attorney General authorization is required prior to arresting, or charging a member of the news media regarding criminal conduct he/she is suspected of having committed in the course of, or arising out of, the coverage or investigation of the news or while engaged in the performance of official duties. (U) Requests for the approval must be submitted to the AD of the operational FBIHQ division that is responsible for the investigative classification and the AD of the Office or Public Affairs (OPA) by an EC. The requesting EC must be reviewed by the CDC and approved by the SAC after coordination with the local USAO. The EC must set forth the facts

believed to establish probable cause and the investigative justification for the arrest, consistent with the DOJ regulations set forth in 28 C.F.R. § 50.10.

(U) Note: 28 C.F.R. § 50.10(b)(1)(ii) provides guidance on categories of individuals and entities not covered by, and therefore not entitled to the protections of the DOJ policy set out in 28 C.F.R. § 50.10 .

19.10.1 (U) *EXIGENT CIRCUMSTANCES*

(U) A Deputy Assistant Attorney General (DAAG) for the Criminal Division may authorize the questioning of a member of the news media as described in DIOG subsection 18.5.6.4.8.1.1 above if he/she determines that exigent use of such a technique is necessary [REDACTED]

b7E

[REDACTED]

(U) The requesting field office seeking exigent authority must set out the circumstances that justify seeking exigent approval authority and communicate the basis for the request to [REDACTED]

[REDACTED] is then responsible for seeking DAAG approval as set forth in 28 C.F.R. 50.10(f). If the exigent request was made by oral communication and the AG's approval was obtained, the field office is responsible to submit written documentation to [REDACTED] [REDACTED] as soon as practicable, [REDACTED] after the making the oral request. The [REDACTED] is responsible to prepare the appropriate written documentation to DOJ, including documenting the receipt of AG approval. This documentation must be electronically placed into the case file.

(U) [REDACTED]
[REDACTED]

19.11 (U) *ARREST OF ARMED FORCES PERSONNEL*

(U) The Uniform Code of Military Justice authorizes any commanding officer exercising general court-martial jurisdiction to surrender military personnel under the officer's command to civil authority when the person has been charged with a civil offense. A request for surrender must be accompanied by:

(U) A copy of the indictment, presentment, information, or warrant;

(U) Sufficient information to identify the person sought as the person who allegedly committed the offense; and

(U) A statement of the maximum sentence which may be imposed upon conviction.

(U) Receipts for persons surrendered for civil prosecution should be signed by an official in the USAO, not by an FBI employee.

19.12 (U) **ARREST OF JUVENILES**

19.12.1 (U) **DEFINITION**

(U) A violation of 18 U.S.C. § 922(x)(2) or violation of a federal law which would have been a crime, if committed by an adult, by a person who has not attained his/her 18th birthday is an act of juvenile delinquency. For the purpose of juvenile delinquency proceedings, a juvenile is a person who committed a crime before his/her 18th birthday who has not attained his/her 21st birthday at the time charges are commenced.

19.12.2 (U) **ARREST PROCEDURES**

(U) Pre-arrest procedures applicable to adults (discussion with USAO, filing of complaint, issuance of warrant) also govern arrests of juveniles. After arrest, however, the Federal Juvenile Delinquency Act requires strict compliance with the following procedures:

- A) (U) **Advice of Rights** - The arresting agent must immediately advise the arrested juvenile of his/her "legal rights" in language comprehensible to the juvenile. The rights found on the standard Form FD-395 meet this requirement. The arresting agent may obtain a signature waiving his/her rights only if the Chief Division Counsel (CDC) or the USAO, based on the law of the circuit, has approved interrogation of the juvenile.
- B) (U) **Notification to U.S. Attorney's Office and Juvenile's Parents** - The arresting agent must immediately notify the USAO and the juvenile's parents, guardian, or custodian, that the juvenile has been arrested. The juvenile's parents, guardian, or custodian must also be notified of the juvenile's rights (use the FD-395 for this purpose) and the nature of the alleged offense for which the juvenile was arrested.
- C) (U) **Initial Appearance before Magistrate Judge** - Subsequent to his/her arrest, the juvenile must be taken to a magistrate judge forthwith.
- D) (U) **Record of Notification and Appearance** - Because proof of timely notification to the juvenile's parents and prompt appearance before the magistrate judge is essential, agents must promptly prepare FD-302(s) documenting the time the following events occurred:
 - 1) (U) The juvenile was arrested;
 - 2) (U) The juvenile was advised of his/her rights;
 - 3) (U) The USAO was notified;
 - 4) (U) The juvenile's parents, guardian, or custodian were notified of the arrest and of the juvenile's rights; and
 - 5) (U) The juvenile was taken before a magistrate judge.
- E) (U) **Interrogation and Interviews** - Whether a juvenile may be interrogated between arrest for a federal offense and initial appearance before the magistrate judge depends on the law of the circuit in which the arrest occurs. When an agent interviews a juvenile in custody, after arrest and prior to initial appearance while in a place of

detention with suitable recording equipment, the statement must be recorded in accordance with DIOG subsection 18.5.6.4.17.3. If interrogation is not permitted in the circuit of arrest, information volunteered by the arrested juvenile concerning his/her guilt must be recorded in the agent's FD-302. Clarifying questions may be asked if necessary to be certain what the juvenile intended to convey. The volunteered statement may be reduced to writing if such action does not delay the juvenile's appearance before the magistrate judge. A juvenile may always be questioned concerning the guilt of someone else, if such questioning does not delay bringing him/her before the magistrate judge. These rules apply only when the juvenile has been arrested for a federal offense. They do not apply when the juvenile is suspected of having committed a federal offense but is under arrest by state or local officers on a state or local charge.

- F) (U) **Fingerprinting and Photographing** - Agents may not fingerprint or photograph a juvenile unless he/she is to be prosecuted as an adult. Because it is not known at the time of arrest whether the juvenile will be prosecuted as an adult or a juvenile, agents may not fingerprint or photograph a juvenile without permission of the magistrate judge. Following an adjudication of delinquency based on an offense which, if committed by an adult, would be a felony that is a crime of violence or a violation of 21 U.S.C. § 841 (manufacturing, distributing, dispensing of a controlled substance or possession with the intent to do same), § 955 (possession of controlled substances on board vessels arriving in or departing the United States) or § 959 (manufacture or distribution of controlled substances for purpose of unlawful importation), the juvenile must be fingerprinted and photographed. Agents should coordinate fingerprinting and photographing with the USMS.
- G) (U) **DNA Collection** - Agents must not take DNA samples from juveniles at the time of arrest.
- H) (U) **Press Releases** - Neither the name nor picture of an arrested juvenile may be made public. Accordingly, the arrest of a juvenile may only be announced by a press release that does not contain identifying information

This Page is Intentionally Blank

~~SECRET~~

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

§20

20 (U) OTHER INVESTIGATIVE RESOURCES

CLASSIFIED BY: NSICG [REDACTED]
REASON: 1.4 (C)
DECLASSIFY ON: 12-31-2041
DATE: 07-09-2018

b6
b7C

20.1 (U) OVERVIEW

(U) Other investigative resources described below are available as specified in Assessments and Predicated Investigations. The investigative resources include:

20.1.1 (U//~~FOUO~~) [REDACTED]

b7E

(U) See Section 20.2 below.

20.1.2 (U//~~FOUO~~) [REDACTED]

b7E

(U) See Section 20.3 below.

20.1.3 (U//~~FOUO~~) *BEHAVIORAL ANALYSIS – OPERATIONAL BEHAVIORAL SUPPORT PROGRAM*

(U) See Section 20.4 below.

20.1.4 (U//~~FOUO~~) *SENSITIVE TECHNICAL EQUIPMENT*

(U) See Section 20.5 below.

20.2 (U//~~FOUO~~) [REDACTED]

b7E

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

b7E

20.2.1 (U) *AUTHORIZED INVESTIGATIVE ACTIVITY*

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

b7E

(U) [REDACTED]

b7E

20.3 (U//~~FOUO~~) [REDACTED]

b7E

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

b1
(S) b7E

The program reports the

20.3.1 (U) *AUTHORIZED INVESTIGATIVE ACTIVITY*

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

b7E

~~SECRET~~

(U//~~FOUO~~)

b7E

20.4 (U//~~FOUO~~) OPERATIONAL BEHAVIORAL SUPPORT PROGRAM – CIRG’S BEHAVIORAL ANALYSIS UNITS (BAUs) AND/OR CD’S BEHAVIORAL ANALYSIS PROGRAM

20.4.1 (U) AUTHORIZED INVESTIGATIVE ACTIVITY

(U) The National Center for the Analysis of Violent Crime (NCAVC) manages and directs the FBI’s operational behavioral support across all investigative programs. In addition, the NCAVC’s units provide operational and analytical support, without charge, to federal, state, local, tribal, foreign law enforcement, intelligence and security agencies involved in the investigation of unusual or repetitive violent crimes, communicated threats, terrorism, and other matters. The NCAVC also provides support through expertise and consultation in non-violent matters, such as national security, corruption, and white-collar crime investigations. See DIOG Section 12 for FD-999 documentation and other requirements for Assistance to Other Agencies.

(U) Requests for NCAVC operational assistance should be made to the NCAVC Coordinator in the field office or to the NCAVC unit at Quantico. Requests for service can be coordinated through direct contact, telephone, email or Electronic Communication to the NCAVC. All FBI operational behavioral support requests must be coordinated and approved by the NCAVC.

(U) The appropriate Legal Attaché office (LEGAT) or the International Operations Division (IOD) must coordinate all requests from foreign law enforcement, intelligence and security agencies with NCAVC staff. NCAVC staff will assist the LEGAT or IOD preparation of an appropriate request for service and will facilitate the delivery of the service requested from the foreign agency.

(U) See the NCAVC website for additional information.

20.5 (U//~~FOUO~~) SENSITIVE TECHNICAL EQUIPMENT

(U//~~FOUO~~) *Definition:* Sensitive Technical Equipment (STE) is defined in the

b7E

20.5.1 (U) AUTHORIZED INVESTIGATIVE ACTIVITY

(U)

b7E

(U//~~FOUO~~)

b7E

Refer to the Extraterritorial Guidelines (see DIOG Section 13), appropriate Policy Guides, and OTD policy for additional information.

20.6 (U//~~FOUO~~)

b7E

(U//~~FOUO~~)

b7E

~~SECRET~~

~~UNCLASSIFIED – FOR OFFICIAL USE ONLY~~
Domestic Investigations and Operations Guide

§20

20.6.1 (U) *AUTHORIZED INVESTIGATIVE ACTIVITY*

(U//FOUO)

[REDACTED]

[REDACTED]

b7E

~~SECRET~~

~~SECRET~~

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

This Page is Intentionally Blank

~~UNCLASSIFIED - FOR OFFICIAL USE ONLY~~

~~SECRET~~

21 (U) INTELLIGENCE COLLECTION

21.1 (U) INCIDENTAL COLLECTION

(U//~~FOUO~~) Incidental collection is information derived during the course of a pending investigation, assessment, or [REDACTED] that is responsive to a PFI, FBI, or IC collection requirement, [REDACTED]
[REDACTED]

(U//~~FOUO~~) Incidentally collected information, responsive to the above-mentioned collection requirements, may also be derived from [REDACTED]
[REDACTED]

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

b7E

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

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

[REDACTED] (See DIOG Section 15.6.1.2 - Written Intelligence Products) [REDACTED]
[REDACTED]

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

b7E

21.2 (U) FBI NATIONAL COLLECTION REQUIREMENTS

(U//~~FOUO~~) The FBIHQ DI establishes FBI national collection requirements after coordination with OGC, other FBIHQ operational divisions, and field offices. An FBI national collection requirement describes information needed by the FBI to: (i) identify or obtain information about potential targets of, or vulnerabilities to, Federal criminal activities or threats to the national

security; or (ii) inform or facilitate intelligence analysis and planning pertinent to the FBI's law enforcement or national security missions.

(U//~~FOUO~~)

b7E

(U) For example:

A) (U//~~FOUO~~)

B) (U//~~FOUO~~)

C) (U//~~FOUO~~)

(U//~~FOUO~~) Before any investigative activity is conducted in order to respond to an FBI national collection requirement, an Assessment or Predicated Investigation must be opened or already open. An Assessment cannot be opened solely based upon an FBI national collection requirement. An authorized purpose (national security or criminal threat) and clearly defined objective(s) must exist prior to opening an Assessment. During an Assessment, the FBI is authorized to collect against any FBI national collection requirement that is relevant to the Assessment

b7E

(U//~~FOUO~~)

(U//~~FOUO~~)

b7E

21.3 (U//~~FOUO~~) FBI FIELD OFFICE COLLECTION REQUIREMENTS

(U//~~FOUO~~) An FBI field office collection requirement describes information needed by the field to: (i) identify or obtain information about potential targets of or vulnerabilities to Federal criminal activities or threats to the national security; or (ii) inform or facilitate intelligence analysis and planning pertinent to the FBI's law enforcement or national security missions.

(U//~~FOUO~~) Before any investigative activity may be conducted to respond to an FBI field office collection requirement, an Assessment or Predicated Investigation must be opened or already open. An Assessment cannot be opened solely based upon an FBI field office collection requirement

This Page is Intentionally Blank

UNCLASSIFIED – ~~FOR OFFICIAL USE ONLY~~
Domestic Investigations and Operations Guide

A (U) THE ATTORNEY GENERAL'S GUIDELINES FOR DOMESTIC FBI OPERATIONS

**THE ATTORNEY GENERAL'S GUIDELINES FOR
DOMESTIC FBI OPERATIONS**

[Including subsequent revisions by the Attorney General Orders]

UNCLASSIFIED – ~~FOR OFFICIAL USE ONLY~~
Domestic Investigations and Operations Guide

PREAMBLE

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

UNCLASSIFIED – ~~FOR OFFICIAL USE ONLY~~
Domestic Investigations and Operations Guide

TABLE OF CONTENTS

INTRODUCTION	4
A. FBI RESPONSIBILITIES - FEDERAL CRIMES, THREATS TO THE NATIONAL SECURITY, FOREIGN INTELLIGENCE	5
B. THE FBI AS AN INTELLIGENCE AGENCY	8
C. OVERSIGHT	9
I. GENERAL AUTHORITIES AND PRINCIPLES	11
A. SCOPE	11
B. GENERAL AUTHORITIES	11
C. USE OF AUTHORITIES AND METHODS	11
D. NATURE AND APPLICATION OF THE GUIDELINES	13
II. INVESTIGATIONS AND INTELLIGENCE GATHERING	15
A. ASSESSMENTS	18
B. PREDICTED INVESTIGATIONS	19
C. ENTERPRISE INVESTIGATIONS	22
III. ASSISTANCE TO OTHER AGENCIES	24
A. THE INTELLIGENCE COMMUNITY	24
B. FEDERAL AGENCIES GENERALLY	24
C. STATE, LOCAL, OR TRIBAL AGENCIES	26
D. FOREIGN AGENCIES	26
E. APPLICABLE STANDARDS AND PROCEDURES	27
IV. INTELLIGENCE ANALYSIS AND PLANNING	28
A. STRATEGIC INTELLIGENCE ANALYSIS	28
B. REPORTS AND ASSESSMENTS GENERALLY	28
C. INTELLIGENCE SYSTEMS	28
V. AUTHORIZED METHODS	29
A. PARTICULAR METHODS	29
B. SPECIAL REQUIREMENTS	30
C. OTHERWISE ILLEGAL ACTIVITY	31
VI. RETENTION AND SHARING OF INFORMATION	34
A. RETENTION OF INFORMATION	34
B. INFORMATION SHARING GENERALLY	34
C. INFORMATION RELATING TO CRIMINAL MATTERS	35
D. INFORMATION RELATING TO NATIONAL SECURITY AND FOREIGN INTELLIGENCE MATTERS	36
VII. DEFINITIONS	41

~~UNCLASSIFIED – FOR OFFICIAL USE ONLY~~
Domestic Investigations and Operations Guide

INTRODUCTION

As the primary investigative agency of the federal government, the Federal Bureau of Investigation (FBI) has the authority and responsibility to investigate all violations of federal law that are not exclusively assigned to another federal agency. The FBI is further vested by law and by Presidential directives with the primary role in carrying out investigations within the United States of threats to the national security. This includes the lead domestic role in investigating international terrorist threats to the United States, and in conducting counterintelligence activities to meet foreign entities' espionage and intelligence efforts directed against the United States.

The FBI is also vested with important functions in collecting foreign intelligence as a member agency of the U.S. Intelligence Community. The FBI accordingly plays crucial roles in the enforcement of federal law and the proper administration of justice in the United States, in the protection of the national security, and in obtaining information needed by the United States for the conduct of its foreign affairs. These roles reflect the wide range of the FBI's current responsibilities and obligations, which require the FBI to be both an agency that effectively detects, investigates, and prevents crimes, and an agency that effectively protects the national security and collects intelligence.

The general objective of these Guidelines is the full utilization of all authorities and investigative methods, consistent with the Constitution and laws of the United States, to protect the United States and its people from terrorism and other threats to the national security, to protect the United States and its people from victimization by all crimes in violation of federal law, and to further the foreign intelligence objectives of the United States. At the same time, it is axiomatic that the FBI must conduct its investigations and other activities in a lawful and reasonable manner that respects liberty and privacy and avoids unnecessary intrusions into the lives of law-abiding people. The purpose of these Guidelines, therefore, is to establish consistent policy in such matters. They will enable the FBI to perform its duties with effectiveness, certainty, and confidence, and will provide the American people with a firm assurance that the FBI is acting properly under the law.

The issuance of these Guidelines represents the culmination of the historical evolution of the FBI and the policies governing its domestic operations subsequent to the September 11, 2001, terrorist attacks on the United States. Reflecting decisions and directives of the President and the Attorney General, inquiries and enactments of Congress, and the conclusions of national commissions, it was recognized that the FBI's functions needed to be expanded and better integrated to meet contemporary realities:

[C]ontinuing coordination...is necessary to optimize the FBI's performance in both national security and criminal investigations...[The] new reality requires first that the FBI and other agencies do a better job of gathering intelligence inside the United States, and second that we eliminate the remnants of the old "wall" between foreign intelligence and domestic law enforcement. Both tasks must be accomplished without sacrificing our domestic liberties and the rule of law, and both depend on building a very different FBI from the one we had

UNCLASSIFIED – ~~FOR OFFICIAL USE ONLY~~
Domestic Investigations and Operations Guide

on September 10, 2001. (Report of the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction 466, 452 (2005).)

In line with these objectives, the FBI has reorganized and reoriented its programs and missions, and the guidelines issued by the Attorney General for FBI operations have been extensively revised over the past several years. Nevertheless, the principal directives of the Attorney General governing the FBI's conduct of criminal investigations, national security investigations, and foreign intelligence collection have persisted as separate documents involving different standards and procedures for comparable activities. These Guidelines effect a more complete integration and harmonization of standards, thereby providing the FBI and other affected Justice Department components with clearer, more consistent, and more accessible guidance for their activities, and making available to the public in a single document the basic body of rules for the FBI's domestic operations.

These Guidelines also incorporate effective oversight measures involving many Department of Justice and FBI components, which have been adopted to ensure that all FBI activities are conducted in a manner consistent with law and policy.

The broad operational areas addressed by these Guidelines are the FBI's conduct of investigative and intelligence gathering activities, including cooperation and coordination with other components and agencies in such activities, and the intelligence analysis and planning functions of the FBI.

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

Part II of these Guidelines authorizes the FBI to carry out investigations to detect, obtain information about, or prevent or protect against federal crimes or threats to the national security or to collect foreign intelligence. The major subject areas of information gathering activities under these Guidelines - federal crimes, threats to the national security, and foreign intelligence - are not distinct, but rather overlap extensively. For example, an investigation relating to international terrorism will invariably crosscut these areas because international terrorism is included under these Guidelines' definition of "threat to the national security," because international terrorism subject to investigation within the United States usually involves criminal acts that violate federal law, and because information relating to international terrorism also falls within the definition of "foreign intelligence." Likewise, counterintelligence activities relating to espionage are likely to concern matters that constitute threats to the national security, that implicate violations or potential violations of federal espionage laws, and that involve information falling under the definition of "foreign intelligence."

While some distinctions in the requirements and procedures for investigations are necessary in different subject areas, the general design of these Guidelines is to take a uniform approach wherever possible, thereby promoting certainty and consistency regarding the applicable standards and facilitating compliance with those standards. Hence, these Guidelines do not require that the FBI's information gathering activities be differentially labeled as "criminal investigations," "national security investigations," or "foreign intelligence collections," or that the categories of

~~UNCLASSIFIED – FOR OFFICIAL USE ONLY~~
Domestic Investigations and Operations Guide

FBI personnel who carry out investigations be segregated from each other based on the subject areas in which they operate. Rather, all of the FBI's legal authorities are available for deployment in all cases to which they apply to protect the public from crimes and threats to the national security and to further the United States' foreign intelligence objectives. In many cases, a single investigation will be supportable as an exercise of a number of these authorities - i.e., as an investigation of a federal crime or crimes, as an investigation of a threat to the national security, and/or as a collection of foreign intelligence.

1. Federal Crimes

The FBI has the authority to investigate all federal crimes that are not exclusively assigned to other agencies. In most ordinary criminal investigations, the immediate objectives include such matters as: determining whether a federal crime has occurred or is occurring, or if planning or preparation for such a crime is taking place; identifying, locating, and apprehending the perpetrators; and obtaining the evidence needed for prosecution. Hence, close cooperation and coordination with federal prosecutors in the United States Attorneys' Offices and the Justice Department litigating divisions are essential both to ensure that agents have the investigative tools and legal advice at their disposal for which prosecutorial assistance or approval is needed, and to ensure that investigations are conducted in a manner that will lead to successful prosecution. Provisions in many parts of these Guidelines establish procedures and requirements for such coordination.

2. Threats to the National Security

The FBI's authority to investigate threats to the national security derives from the executive order concerning U.S. intelligence activities, from delegations of functions by the Attorney General, and from various statutory sources. See, e.g., E.O. 12333; 50 U.S.C. 401 et seq.; 50 U.S.C. 1801 et seq. These Guidelines (Part VII.S) specifically define threats to the national security to mean: international terrorism; espionage and other intelligence activities, sabotage, and assassination, conducted by, for, or on behalf of foreign powers, organizations, or persons; foreign computer intrusion; and other matters determined by the Attorney General, consistent with Executive Order 12333 or any successor order.

Activities within the definition of "threat to the national security" that are subject to investigation under these Guidelines commonly involve violations (or potential violations) of federal criminal laws. Hence, investigations of such threats may constitute an exercise both of the FBI's criminal investigation authority and of the FBI's authority to investigate threats to the national security. As with criminal investigations generally, detecting and solving the crimes, and eventually arresting and prosecuting the perpetrators, are likely to be among the objectives of investigations relating to threats to the national security. But these investigations also often serve important purposes outside the ambit of normal criminal investigation and prosecution, by providing the basis for, and informing decisions concerning, other measures needed to protect the national security. These measures may include, for example: excluding or removing persons involved in terrorism or espionage from the United States; recruitment of double agents; freezing

UNCLASSIFIED – ~~FOR OFFICIAL USE ONLY~~
Domestic Investigations and Operations Guide

assets of organizations that engage in or support terrorism; securing targets of terrorism or espionage; providing threat information and warning to other federal, state, local, and private agencies and entities; diplomatic or military actions; and actions by other intelligence agencies to counter international terrorism or other national security threats.

In line with this broad range of purposes, investigations of threats to the national security present special needs to coordinate with other Justice Department components, including particularly the Justice Department's National Security Division, and to share information and cooperate with other agencies with national security responsibilities, including other agencies of the U.S. Intelligence Community, the Department of Homeland Security, and relevant White House (including National Security Council and Homeland Security Council) agencies and entities. Various provisions in these Guidelines establish procedures and requirements to facilitate such coordination.

3. Foreign Intelligence

As with the investigation of threats to the national security, the FBI's authority to collect foreign intelligence derives from a mixture of administrative and statutory sources. See, e.g., E.O. 12333; 50 U.S.C. 401 et seq.; 50 U.S.C. 1801 et seq.; 28 U.S.C. 532 note (incorporating P.L. 108-458 §§ 2001-2003). These Guidelines (Part VII.E) define foreign intelligence to mean "information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations or foreign persons, or international terrorists."

The FBI's foreign intelligence collection activities have been expanded by legislative and administrative reforms subsequent to the September 11, 2001, terrorist attacks, reflecting the FBI's role as the primary collector of foreign intelligence within the United States, and the recognized imperative that the United States' foreign intelligence collection activities become more flexible, more proactive, and more efficient in order to protect the homeland and adequately inform the United States' crucial decisions in its dealings with the rest of the world:

The collection of information is the foundation of everything that the Intelligence Community does. While successful collection cannot ensure a good analytical product, the failure to collect information...turns analysis into guesswork. And as our review demonstrates, the Intelligence Community's human and technical intelligence collection agencies have collected far too little information on many of the issues we care about most. (Report of the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction 351 (2005).)

These Guidelines accordingly provide standards and procedures for the FBI's foreign intelligence collection activities that meet current needs and realities and optimize the FBI's ability to discharge its foreign intelligence collection functions.

The authority to collect foreign intelligence extends the sphere of the FBI's information gathering activities beyond federal crimes and threats to the national security, and permits the FBI to seek information regarding a broader range of matters relating to foreign powers, organizations,

~~UNCLASSIFIED – FOR OFFICIAL USE ONLY~~
Domestic Investigations and Operations Guide

or persons that may be of interest to the conduct of the United States' foreign affairs. The FBI's role is central to the effective collection of foreign intelligence within the United States because the authorized domestic activities of other intelligence agencies are more constrained than those of the FBI under applicable statutes and Executive Order 12333. In collecting foreign intelligence, the FBI will generally be guided by nationally-determined intelligence requirements, including the National Intelligence Priorities Framework and the National HUMINT Collection Directives, or any successor directives issued under the authority of the Director of National Intelligence (DNI). As provided in Part VII.F of these Guidelines, foreign intelligence requirements may also be established by the President or Intelligence Community officials designated by the President, and by the Attorney General, the Deputy Attorney General, or an official designated by the Attorney General.

The general guidance of the FBI's foreign intelligence collection activities by DNI-authorized requirements does not, however, limit the FBI's authority to conduct investigations supportable on the basis of its other authorities -to investigate federal crimes and threats to the national security - in areas in which the information sought also falls under the definition of foreign intelligence. The FBI conducts investigations of federal crimes and threats to the national security based on priorities and strategic objectives set by the Department of Justice and the FBI, independent of DNI-established foreign intelligence collection requirements.

Since the authority to collect foreign intelligence enables the FBI to obtain information pertinent to the United States' conduct of its foreign affairs, even if that information is not related to criminal activity or threats to the national security, the information so gathered may concern lawful activities. The FBI should accordingly operate openly and consensually with U.S. persons to the extent practicable when collecting foreign intelligence that does not concern criminal activities or threats to the national security.

B. THE FBI AS AN INTELLIGENCE AGENCY

The FBI is an intelligence agency as well as a law enforcement agency. Its basic functions accordingly 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; 28 U.S.C. 532 note (incorporating P.L. 108-458 §§ 2001-2003) and 534 note (incorporating P.L. 109-162 § 1107). Enhancement of the FBI's intelligence analysis capabilities and functions has consistently been recognized as a key priority in the legislative and administrative reform efforts following the September 11, 2001, terrorist attacks:

[Counterterrorism] strategy should . . . encompass specific efforts to . . . enhance the depth and quality of domestic intelligence collection and analysis . . . [T]he FBI should strengthen and improve its domestic [intelligence] capability as fully and expeditiously as possible by immediately instituting measures to . . . significantly improve strategic analytical capabilities...(Joint Inquiry into Intelligence Community Activities Before and After the Terrorist Attacks of September 11, 2001, S. Rep. No. 351 & H.R. Rep. No. 792, 107th Cong., 2d Sess. 4-7 (2002) (errata print).)

~~UNCLASSIFIED – FOR OFFICIAL USE ONLY~~
Domestic Investigations and Operations Guide

A "smart" government would *integrate* all sources of information to see the enemy as a whole. Integrated all-source analysis should also inform and shape strategies to collect more intelligence. . . . The importance of integrated, all-source analysis cannot be overstated. Without it, it is not possible to "connect the dots." (Final Report of the National Commission on Terrorist Attacks Upon the United States 401, 408 (2004).)

Part IV of these Guidelines accordingly authorizes the FBI to engage in intelligence analysis and planning, drawing on all lawful sources of information. The functions authorized under that Part include: (i) development of overviews and analyses concerning threats to and vulnerabilities of the United States and its interests, (ii) research and analysis to produce reports and assessments concerning matters relevant to investigative activities or other authorized FBI activities, and (iii) the operation of intelligence systems that facilitate and support investigations through the compilation and analysis of data and information on an ongoing basis.

C. OVERSIGHT

The activities authorized by these Guidelines must be conducted in a manner consistent with all applicable laws, regulations, and policies, including those protecting privacy and civil liberties. The Justice Department's National Security Division and the FBI's Inspection Division, Office of General Counsel, and Office of Integrity and Compliance, along with other components, share the responsibility to ensure that the Department meets these goals with respect to national security and foreign intelligence matters. In particular, the National Security Division's Oversight Section, in conjunction with the FBI's Office of General Counsel, is responsible for conducting regular reviews of all aspects of FBI national security and foreign intelligence activities. These reviews conducted at FBI field offices and headquarter units, broadly examine such activities for compliance with these Guidelines and other applicable requirements.

Various features of these Guidelines facilitate the National Security Division's oversight functions. Relevant requirements and provisions include: (i) required notification by the FBI to the National Security Division concerning full investigations that involve foreign intelligence collection or investigation of United States persons in relation to threats of the national security, (ii) annual reports by the FBI to the National Security Division concerning the FBI's foreign intelligence collection program, including information on the scope and nature of foreign intelligence collection activities in each FBI field office, and (iii) access by the National Security Division to information obtained by the FBI through national security or foreign intelligence activities and general authority for the Assistant Attorney General for National Security to obtain reports from the FBI concerning these activities.

Pursuant to these Guidelines, other Attorney General guidelines, and institutional assignments of responsibility within the Justice Department, additional Department components - including the Criminal Division, the United States Attorneys' Offices, and the Office of Privacy and Civil Liberties - are involved in the common endeavor with the FBI of ensuring that the activities of all Department components are lawful, appropriate, and ethical as well as effective. Examples include the involvement of both FBI and prosecutorial personnel in the

UNCLASSIFIED – ~~FOR OFFICIAL USE ONLY~~
Domestic Investigations and Operations Guide

review of undercover operations involving sensitive circumstances, notice requirements for investigations involving sensitive investigative matters (as defined in Part VII.N of these Guidelines), and notice and oversight provisions for enterprise investigations, which may involve a broad examination of groups implicated in the gravest criminal and national security threats. These requirements and procedures help to ensure that the rule of law is respected in the Department's activities and that public confidence is maintained in these activities.

UNCLASSIFIED – ~~FOR OFFICIAL USE ONLY~~
Domestic Investigations and Operations Guide

I. GENERAL AUTHORITIES AND PRINCIPLES

A. SCOPE

These Guidelines apply to investigative activities conducted by the FBI within the United States or outside the territories of all countries. They do not apply to investigative activities of the FBI in foreign countries, which are governed by the Attorney General's Guidelines for Extraterritorial FBI Operations.

B. GENERAL AUTHORITIES

1. The FBI is authorized to conduct investigations to detect, obtain information about, and prevent and protect against federal crimes and threats to the national security and to collect foreign intelligence, as provided in Part II of these Guidelines.
2. The FBI is authorized to provide investigative assistance to other federal agencies, state, local, or tribal agencies, and foreign agencies as provided in Part II of these Guidelines.
3. The FBI is authorized to conduct intelligence analysis and planning as provided in Part VI of these Guidelines.
4. The FBI is authorized to retain and share information obtained pursuant to these Guidelines as provided in Part VI of these Guidelines.

C. USE OF AUTHORITIES AND METHODS

1. Protection of the United States and Its People

The FBI shall fully utilize the authorities provided and the methods authorized by these Guidelines to protect the United States and its people from crimes in violation of federal law and threats to the national security, and to further the foreign intelligence objectives of the United States.

2. Choice of Methods

- a. The conduct of investigations and other activities authorized by these Guidelines may present choices between the use of different investigative methods that are each operationally sound and effective, but that are more or less intrusive, considering such factors as the effect on the privacy and civil liberties of individuals and potential damage to reputation. The least intrusive method feasible is to be used in such situations. It is recognized, however, that the choice of methods is a matter of judgment. The FBI shall not hesitate to use any lawful method consistent with these Guidelines, even if intrusive, where the degree of intrusiveness is warranted in light of

~~UNCLASSIFIED – FOR OFFICIAL USE ONLY~~
Domestic Investigations and Operations Guide

the seriousness of a criminal or national security threat or the strength of the information indicating its existence, or in light of the importance of foreign intelligence sought to the United States' interests. This point is to be particularly observed in investigations relating to terrorism.

- b. United States persons shall be dealt with openly and consensually to the extent practicable when collecting foreign intelligence that does not concern criminal activities or threats to the national security.

3. Respect for Legal Rights

All activities under these Guidelines must have a valid purpose consistent with these Guidelines, and must be carried out in conformity with the Constitution and all applicable statutes, executive orders, Department of Justice regulations and policies, and Attorney General guidelines. These Guidelines do not authorize investigating or collecting or maintaining information on United States persons solely for the purpose of monitoring activities protected by the First Amendment or the lawful exercise of other rights secured by the Constitution or laws of the United States. These Guidelines also do not authorize any conduct prohibited by the Guidance Regarding the Use of Race by Federal Law Enforcement Agencies.

4. Undisclosed Participation in Organizations

Undisclosed participation in organizations in activities under these Guidelines shall be conducted in accordance with FBI policy approved by the Attorney General.

5. Maintenance of Records under the Privacy Act

The Privacy Act restricts the maintenance of records relating to certain activities of individuals who are United States persons, with exceptions for circumstances in which the collection of such information is pertinent to and within the scope of an authorized law enforcement activity or is otherwise authorized by statute. 5 U.S.C. 552a(e)(7). Activities authorized by these Guidelines are authorized law enforcement activities or activities for which there is otherwise statutory authority for purposes of the Privacy Act. These Guidelines, however, do not provide an exhaustive enumeration of authorized FBI law enforcement activities or FBI activities for which there is otherwise statutory authority, and no restriction is implied with respect to such activities carried out by the FBI pursuant to other authorities. Further questions about the application of the Privacy Act to authorized activities of the FBI should be addressed to the FBI Office of the General Counsel, the FBI Privacy and Civil Liberties Unit, or the Department of Justice Office of Privacy and Civil Liberties.

UNCLASSIFIED – ~~FOR OFFICIAL USE ONLY~~
Domestic Investigations and Operations Guide

D. NATURE AND APPLICATION OF THE GUIDELINES

1. Repealers

These Guidelines supersede the following guidelines, which are hereby repealed:

- a. The Attorney General's Guidelines on General Crimes, Racketeering Enterprise and Terrorism Enterprise Investigations (May 30, 2002) and all predecessor guidelines thereto.
- b. The Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection (October 31, 2003) and all predecessor guidelines thereto.
- c. The Attorney General's Supplemental Guidelines for Collection, Retention, and Dissemination of Foreign Intelligence (November 29, 2006).
- d. The Attorney General Procedure for Reporting and Use of Information Concerning Violations of Law and Authorization for Participation in Otherwise Illegal Activity in FBI Foreign Intelligence, Counterintelligence or International Terrorism Intelligence Investigations (August 8, 1988).
- e. The Attorney General's Guidelines for Reporting on Civil Disorders and Demonstrations Involving a Federal Interest (April 5, 1976).

2. Status as Internal Guidance

These Guidelines are set forth solely for the purpose of internal Department of Justice guidance. They are not intended to, do not, and may not be relied upon to create any rights, substantive or procedural; enforceable by law by any party in any matter, civil or criminal, nor do they place any limitation on otherwise lawful investigative and litigative prerogatives of the Department of Justice.

3. Departures from the Guidelines

Departures from these Guidelines must be approved by the Director of the FBI, by the Deputy Director of the FBI, or by an Executive Assistant Director designated by the Director. If a departure is necessary without such prior approval because of the immediacy or gravity of a threat to the safety of persons or property or to the national security, the Director, the Deputy Director, or a designated Executive Assistant Director shall be notified as soon thereafter as practicable. The FBI shall provide timely written notice of departures from these Guidelines to the Criminal Division and the National Security Division, and those divisions shall notify the Attorney General and the Deputy Attorney

UNCLASSIFIED – ~~FOR OFFICIAL USE ONLY~~
Domestic Investigations and Operations Guide

General. Notwithstanding this paragraph, all activities in all circumstances must be carried out in a manner consistent with the Constitution and laws of the United States.

4. Other Activities Not Limited

These Guidelines apply to FBI activities as provided herein and do not limit other authorized activities of the FBI, such as the FBI's responsibilities to conduct background checks and inquiries concerning applicants and employees under federal personnel security programs, the FBI's maintenance and operation of national criminal records systems and preparation of national crime statistics, and the forensic assistance and administration functions of the FBI Laboratory.

UNCLASSIFIED – ~~FOR OFFICIAL USE ONLY~~
Domestic Investigations and Operations Guide

II. INVESTIGATIONS AND INTELLIGENCE GATHERING

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

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

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

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

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

In the course of activities under these Guidelines, the FBI may incidentally obtain information relating to matters outside of its areas of primary investigative responsibility. For example, information relating to violations of state or local law or foreign law may be incidentally obtained in the course of investigating federal crimes or threats to the national security or in collecting foreign intelligence. These Guidelines do not bar the acquisition of such information in

~~UNCLASSIFIED – FOR OFFICIAL USE ONLY~~
Domestic Investigations and Operations Guide

the course of authorized investigative activities, the retention of such information, or its dissemination as appropriate to the responsible authorities in other agencies or jurisdictions. Part VI of these Guidelines includes specific authorizations and requirements for sharing such information with relevant agencies and officials.

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

Assessments, authorized by Subpart A of this Part, require an authorized purpose but not any particular factual predication. For example, to carry out its central mission of preventing the commission of terrorist acts against the United States and its people, the FBI must proactively draw on available sources of information to identify terrorist threats and activities. It cannot be content to wait for leads to come in through the actions of others, but rather must be vigilant in detecting terrorist activities to the full extent permitted by law, with an eye towards early intervention and prevention of acts of terrorism before they occur. Likewise, in the exercise of its protective functions, the FBI is not constrained to wait until information is received indicating that a particular event, activity, or facility has drawn the attention of those who would threaten the national security. Rather, the FBI must take the initiative to secure and protect activities and entities whose character may make them attractive targets for terrorism or espionage. The proactive investigative authority conveyed in assessments is designed for, and may be utilized by, the FBI in the discharge of these responsibilities. For example, assessments may be conducted as part of the FBI's special events management activities.

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

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

~~UNCLASSIFIED – FOR OFFICIAL USE ONLY~~
Domestic Investigations and Operations Guide

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

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

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

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

UNCLASSIFIED – ~~FOR OFFICIAL USE ONLY~~
Domestic Investigations and Operations Guide

A. ASSESSMENTS

1. Purposes

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

2. Approval

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

3. Authorized Activities

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

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

~~UNCLASSIFIED – FOR OFFICIAL USE ONLY~~
Domestic Investigations and Operations Guide

4. Authorized Methods

Only the following methods may be used in assessments:

- a. Obtain publicly available information.
- b. Access and examine FBI and other Department of Justice records, and obtain information from any FBI or other Department of Justice personnel.
- c. Access and examine records maintained by, and request information from, other federal, state, local, or tribal, or foreign governmental entities or agencies.
- d. Use online services and resources (whether nonprofit or commercial).
- e. Use and recruit human sources in conformity with the Attorney General's Guidelines Regarding the Use of FBI Confidential Human Sources.
- f. Interview or request information from members of the public and private entities.
- g. Accept information voluntarily provided by governmental or private entities.
- h. Engage in observation or surveillance not requiring a court order.
- i. Grand jury subpoenas to providers of electronic communication services or remote computing services (including telephone or electronic mail providers) for the subscriber or customer information listed in 18 U.S.C. 2703(c)(2).

B. PREDICTED INVESTIGATIONS

1. Purposes

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

2. Approval

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

~~UNCLASSIFIED – FOR OFFICIAL USE ONLY~~
Domestic Investigations and Operations Guide

3. Circumstances Warranting Investigation

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

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

4. Preliminary and Full Investigations

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

a. Preliminary investigations

i. Predication Required for Preliminary Investigations

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

ii. Duration of Preliminary Investigations

A preliminary investigation must be concluded within six months of its initiation, which may be extended by up to six months by the Special Agent in Charge¹. Extensions of preliminary investigations beyond a

¹ See Deputy Attorney General's Memorandum for the Heads of Department Components captioned, "Delegation of Certain Special Agent in Charge Functions under the Attorney General's Guidelines for Domestic FBI Operations", dated November 24, 2008.

b7E

UNCLASSIFIED – ~~FOR OFFICIAL USE ONLY~~
Domestic Investigations and Operations Guide

year must be approved by FBI Headquarters.

iii. Methods Allowed in Preliminary Investigations

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

b. Full Investigations

i. Predication Required for Full Investigations

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

ii. Methods Allowed in Full Investigations

All lawful methods may be used in a full investigation.

5. Notice Requirements

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

~~UNCLASSIFIED – FOR OFFICIAL USE ONLY~~
Domestic Investigations and Operations Guide

national security on the ground that the predication for the investigation is insufficient.

C. ENTERPRISE INVESTIGATIONS

1. Definition

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

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

2. Scope

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

3. Notice and Reporting Requirements

- a. The responsible Department of Justice component for the purpose of notification and reports in enterprise investigations is the National Security Division, except that, for the purpose of notifications and reports in an enterprise investigation relating to a pattern of racketeering activity that does not involve an offense or offenses described in 18 U.S.C. 2332b(g)(5)(B), the responsible Department of Justice component is the Organized Crime and Racketeering Section of the Criminal Division.
- b. An FBI field office shall notify FBI Headquarters of the initiation by the field office of an enterprise investigation.

~~UNCLASSIFIED – FOR OFFICIAL USE ONLY~~
Domestic Investigations and Operations Guide

- c. The FBI shall notify the National Security Division or the Organized Crime and Racketeering Section of the initiation of an enterprise investigation, whether by a field office or by FBI Headquarters, and the component so notified shall notify the Attorney General and the Deputy Attorney General. The FBI shall also notify any relevant United States Attorney's Office, except that any investigation within the scope of Part VI.D. 1.d of these Guidelines (relating to counterintelligence investigations) is to be treated as provided in that provision. Notifications by the FBI under this subparagraph shall be provided as soon as practicable, but no later than 30 days after the initiation of the investigation.
- d. The Assistant Attorney General for National Security or the Chief of the Organized Crime and Racketeering Section, as appropriate, may at any time request the FBI to provide a report on the status of an enterprise investigation and the FBI will provide such reports as requested.

~~UNCLASSIFIED – FOR OFFICIAL USE ONLY~~
Domestic Investigations and Operations Guide

III. ASSISTANCE TO OTHER AGENCIES

The FBI is authorized to provide investigative assistance to other federal, state, local, or tribal, or foreign agencies as provided in this Part.

The investigative assistance authorized by this Part is often concerned with the same objectives as those identified in Part II of these Guidelines -investigating federal crimes and threats to the national security, and collecting foreign intelligence. In some cases, however, investigative assistance to other agencies is legally authorized for purposes other than those identified in Part II, such as assistance in certain contexts to state or local agencies in the investigation of crimes under state or local law, see 28 U.S.C. 540, 540A, 540B, and assistance to foreign agencies in the investigation of foreign law violations pursuant to international agreements. Investigative assistance for such legally authorized purposes is permitted under this Part, even if it is not for purposes identified as grounds for investigation under Part II.

The authorities provided by this Part are cumulative to Part II and do not limit the FBI's investigative activities under Part II. For example, Subpart B.2 in this Part authorizes investigative activities by the FBI in certain circumstances to inform decisions by the President concerning the deployment of troops to deal with civil disorders, and Subpart B.3 authorizes investigative activities to facilitate demonstrations and related public health and safety measures. The requirements and limitations in these provisions for conducting investigations for the specified purposes do not limit the FBI's authority under Part II to investigate federal crimes or threats to the national security that occur in the context of or in connection with civil disorders or demonstrations.

A. THE INTELLIGENCE COMMUNITY

The FBI may provide investigative assistance (including operational support) to authorized intelligence activities of other Intelligence Community agencies.

B. FEDERAL AGENCIES GENERALLY

1. In General

The FBI may provide assistance to any federal agency in the investigation of federal crimes or threats to the national security or in the collection of foreign intelligence, and 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.

2. The President in Relation to Civil Disorders

- a. At the direction of the Attorney General, the Deputy Attorney General, or the Assistant Attorney General for the Criminal Division, the FBI shall

UNCLASSIFIED – ~~FOR OFFICIAL USE ONLY~~
Domestic Investigations and Operations Guide

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:

- i. The size of the actual or threatened disorder, both in number of people involved or affected and in geographic area.
 - ii. The potential for violence.
 - iii. The potential for expansion of the disorder in light of community conditions and underlying causes of the disorder.
 - iv. 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.
 - v. The extent of state or local resources available to handle the disorder.
- b. Investigations under this paragraph will be authorized only for a period of 30 days, but the authorization may be renewed for subsequent 30 day periods.
 - c. Notwithstanding Subpart E.2 of this Part, the methods that may be used in an investigation under this paragraph are those described in subparagraphs a.-d., subparagraph f. (other than pretext interviews or requests), or subparagraph g. of Part II.A.4 of these Guidelines. The Attorney General, the Deputy Attorney General, or the Assistant Attorney General for the Criminal Division may also authorize the use of other methods described in Part II.A.4.

3. Public Health and Safety Authorities in Relation to Demonstrations

- a. 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:
 - i. The time, place, and type of activities planned.
 - ii. The number of persons expected to participate.

UNCLASSIFIED – ~~FOR OFFICIAL USE ONLY~~
Domestic Investigations and Operations Guide

- iii. The expected means and routes of travel for participants and expected time of arrival.
- iv. Any plans for lodging or housing of participants in connection with the demonstration.
- b. Notwithstanding Subpart E.2 of this Part, the methods that may be used in an investigation under this paragraph are those described in subparagraphs a.-d., subparagraph f. (other than pretext interviews or requests), or subparagraph g. of Part II.A.4 of these Guidelines. The Attorney General, the Deputy Attorney General, or the Assistant Attorney General for the Criminal Division may also authorize the use of other methods described in Part II.A.4.

C. STATE, LOCAL, OR TRIBAL AGENCIES

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 such other purposes as may be legally authorized.

D. FOREIGN AGENCIES

- 1. 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. Investigations or assistance under this paragraph must be approved as provided by FBI policy. The FBI shall notify the National Security Division concerning investigation or assistance under this paragraph where: (i) FBI Headquarters approval for the activity is required pursuant to the approval policy adopted by the FBI for purposes of this paragraph, and (ii) the activity relates to a threat to the national security. Notification to the National Security Division shall be made as soon as practicable but no later than 30 days after the approval. Provisions regarding notification to or coordination with the Central Intelligence Agency by the FBI in memoranda of understanding or agreements with the Central Intelligence Agency may also apply to activities under this paragraph.
- 2. The FBI may not provide assistance to foreign law enforcement, intelligence, or security officers conducting investigations within the United States unless such officers have provided prior notification to the Attorney General as required by 18 U.S.C. 951

UNCLASSIFIED – ~~FOR OFFICIAL USE ONLY~~
Domestic Investigations and Operations Guide

3. The FBI may conduct background inquiries concerning consenting individuals when requested by foreign government agencies.
4. The FBI may provide other material and technical assistance to foreign governments to the extent not otherwise prohibited by law.

E. APPLICABLE STANDARDS AND PROCEDURES

1. Authorized investigative assistance by the FBI to other agencies under this Part includes joint operations and activities with such agencies.
2. All lawful methods may be used in investigative assistance activities under this Part.
3. Where the methods used in investigative assistance activities under this Part go beyond the methods authorized in assessments under Part II.A.4 of these Guidelines, the following apply:
 - a. Supervisory approval must be obtained for the activity at a level or levels specified in FBI policy.
 - b. Notice must be provided concerning sensitive investigative matters in the manner described in Part II.B.5.
 - c. A database or records system must be maintained that permits, with respect to each such activity, the prompt retrieval of the status of the activity (open or closed), the dates of opening and closing, and the basis for the activity. This database or records system may be combined with the database or records system for predicated investigations required by Part VI.A.2.

UNCLASSIFIED – ~~FOR OFFICIAL USE ONLY~~
Domestic Investigations and Operations Guide

IV. INTELLIGENCE ANALYSIS AND PLANNING

The FBI is authorized to engage in analysis and planning. The FBI's analytic activities enable 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 strategic planning, the FBI can more effectively discover crimes, 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. For example, analysis of threats in the context of special events management, concerning public events or activities that may be targeted for terrorist attack, is an authorized activity under this Part.

In carrying out its intelligence functions under this Part, the FBI is authorized to draw on all lawful sources of information, including but not limited to the results of investigative activities under these Guidelines. Investigative activities under these Guidelines and other legally authorized activities through which the FBI acquires information, data, or intelligence may properly be utilized, structured, and prioritized so as to support and effectuate the FBI's intelligence mission. The remainder of this Part provides further specification concerning activities and functions authorized as part of that mission.

A. STRATEGIC INTELLIGENCE ANALYSIS

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; and matters relevant to the conduct of the United States' foreign affairs. The overviews and analyses prepared under this Subpart may encompass present, emergent, and potential threats and vulnerabilities, their contexts and causes, and identification and analysis of means of responding to them.

B. REPORTS AND ASSESSMENTS GENERALLY

The FBI is authorized to conduct research, analyze information, and prepare reports and assessments concerning matters relevant to authorized FBI activities, such as reports and assessments concerning: types of criminals or criminal activities; organized crime groups; terrorism, espionage, or other threats to the national security; foreign intelligence matters; or the scope and nature of criminal activity in particular geographic areas or sectors of the economy.

C. INTELLIGENCE SYSTEMS

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.

UNCLASSIFIED – ~~FOR OFFICIAL USE ONLY~~
Domestic Investigations and Operations Guide

V. AUTHORIZED METHODS

A. PARTICULAR METHODS

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

1. The methods described in Part II.A.4 of these Guidelines.
2. Mail covers.
3. Physical searches of personal or real property where a warrant or court order is not legally required because there is no reasonable expectation of privacy (e.g., trash covers).
4. Consensual monitoring of communications, including consensual computer monitoring, subject to legal review by the Chief Division Counsel or the FBI Office of the General Counsel. Where a sensitive monitoring circumstance is involved, the monitoring must be approved by the Criminal Division or, if the investigation concerns a threat to the national security or foreign intelligence, by the National Security Division.
5. Use of closed-circuit television, direction finders, and other monitoring devices, subject to legal review by the Chief Division Counsel or the FBI Office of the General Counsel. (The methods described in this paragraph usually do not require court orders or warrants unless they involve physical trespass or non-consensual monitoring of communications, but legal review is necessary to ensure compliance with all applicable legal requirements.)
6. Polygraph examinations.
7. Undercover operations. In investigations relating to activities in violation of federal criminal law that do not concern threats to the national security or foreign intelligence, undercover operations must be carried out in conformity with the Attorney General's Guidelines on Federal Bureau of Investigation Undercover Operations. In investigations that are not subject to the preceding sentence because they concern threats to the national security or foreign intelligence, undercover operations involving religious or political organizations must be reviewed and approved by FBI Headquarters, with participation by the National Security Division in the review process.
8. Compulsory process as authorized by law, including grand jury subpoenas and other subpoenas, National Security Letters (15 U.S.C. 1681u, 1681v; 18 U.S.C. 2709; 12

UNCLASSIFIED – ~~FOR OFFICIAL USE ONLY~~
Domestic Investigations and Operations Guide

U.S.C. 3414(a)(5)(A); 50 U.S.C. 436), and Foreign Intelligence Surveillance Act orders for the production of tangible things (50 U.S.C. 1861-63).

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

B. SPECIAL REQUIREMENTS

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

1. Contacts with Represented Persons

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

2. Use of Classified Investigative Technologies

Inappropriate use of classified investigative technologies may risk the compromise of such technologies. Hence, in an investigation relating to activities in violation of federal criminal law that does not concern a threat to the national

UNCLASSIFIED – ~~FOR OFFICIAL USE ONLY~~
Domestic Investigations and Operations Guide

security or foreign intelligence, the use of such technologies must be in conformity with the Procedures for the Use of Classified Investigative technologies in Criminal Cases.

C. OTHERWISE ILLEGAL ACTIVITY

1. Otherwise illegal activity by an FBI agent or employee in an undercover operation relating to activity in violation of federal criminal law that does not concern a threat to the national security or foreign intelligence must be approved in conformity with the Attorney General's Guidelines on Federal Bureau of Investigation Undercover Operations. Approval of otherwise illegal activity in conformity with those guidelines is sufficient and satisfies any approval requirement that would otherwise apply under these Guidelines.
2. Otherwise illegal activity by a human source must be approved in conformity with the Attorney General's Guidelines Regarding the Use of FBI Confidential Human Sources.
3. Otherwise illegal activity by an FBI agent or employee that is not within the scope of paragraph 1. must be approved by a United States Attorney's Office or a Department of Justice Division, except that (i) an FBI agent or employee may engage in the consensual monitoring of communications in accordance with FBI policy, even if a crime under state, local, territorial, or tribal law, and (ii) a Special Agent in Charge may authorize the following²:
 - a. otherwise illegal activity that would not be a felony under federal, state, local, territorial, or tribal law;
 - b. the controlled³ purchase, receipt, delivery, or sale of drugs, firearms, stolen property, contraband, or other items that are subject to legal or regulatory restrictions on transfer, such as prescription medication or medical devices;
 - c. the delivery or sale of stolen property whose ownership cannot be determined, provided that the property does not pose a significant risk of death or serious injury to any person;
 - d. the payment of bribes or kickbacks;
 - e. the making of false representations in concealment of personal identity or

² [REDACTED]
[REDACTED] See Deputy Attorney General's Memorandum for the Heads of Department Components captioned, "Delegation of Certain Special Agent in Charge Functions under the Attorney General's Guidelines for Domestic FBI Operations", dated November 24, 2008.

³ [REDACTED]
[REDACTED]

b7E

UNCLASSIFIED – ~~FOR OFFICIAL USE ONLY~~
Domestic Investigations and Operations Guide

the true ownership of a proprietary, but not including sworn testimony;

- f. conducting money laundering transactions (including acting as an unlicensed money transmitter or using other methods to conduct the transactions) involving an aggregate amount not exceeding \$1 million;
- g. the advertising or soliciting of unlawful goods or services; and
- h. gambling activities.

However, a Special Agent in Charge may not authorize an activity that may constitute a violation of export control laws, economic sanctions, or laws that concern the proliferation of weapons of mass destruction. In an investigation relating to a threat to the national security or foreign intelligence collection, a Special Agent in Charge may authorize an activity that may otherwise violate prohibitions of material support to terrorism only in accordance with standards established by the Director of the FBI and agreed to by the Assistant Attorney General for National Security.

4. The following activities may not be authorized:

- a. Acts of violence.
- b. Activities whose authorization is prohibited by law, including unlawful investigative methods, such as illegal electronic surveillance or illegal searches.

Subparagraph a., however, does not limit the right of FBI agents or employees to engage in any lawful use of force, including the use of force in self-defense or defense of others or otherwise in the lawful discharge of their duties.

5. An agent or employee may engage in otherwise illegal activity that could be authorized under this Subpart without the authorization required by paragraph 3, 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 otherwise illegal activity, every effort should be made by the agent or employee to consult with the Special Agent in Charge, and by the Special Agent in Charge to consult with the United States Attorney's Office or appropriate Department of Justice Division where the authorization of that office or division would be required under paragraph 3., unless the circumstances preclude such consultation. Cases in which otherwise illegal activity occurs pursuant to this paragraph without the authorization required by paragraph 3. shall be reported as soon as possible to the Special Agent in Charge, and by the Special Agent in Charge to FBI Headquarters and to the United States Attorney's Office or appropriate Department of Justice

UNCLASSIFIED – ~~FOR OFFICIAL USE ONLY~~
Domestic Investigations and Operations Guide

Division.

6. In an investigation relating to a threat to the national security or foreign intelligence collection, the National Security Division is the approving component for otherwise illegal activity for which paragraph 3. requires approval beyond internal FBI approval. However, officials in other components may approve otherwise illegal activity in such investigations as authorized by the Assistant Attorney General for National Security.

~~UNCLASSIFIED – FOR OFFICIAL USE ONLY~~
Domestic Investigations and Operations Guide

VI. RETENTION AND SHARING OF INFORMATION

A. RETENTION OF INFORMATION

1. The FBI shall retain records relating to activities under these Guidelines in accordance with a records retention plan approved by the National Archives and Records Administration.
2. The FBI shall 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.

B. INFORMATION SHARING GENERALLY

1. Permissive Sharing

Consistent with law and with any applicable agreements or understandings with other agencies concerning the dissemination of information they have provided, the FBI may disseminate information obtained or produced through activities under these Guidelines:

- a. within the FBI and to other components of the Department of Justice;
- b. to other federal, state, local, or tribal agencies if related to their responsibilities and, in relation to other Intelligence Community agencies, the determination whether the information is related to the recipient's responsibilities may be left to the recipient;
- c. to congressional committees as authorized by the Department of Justice Office of Legislative Affairs;
- d. to foreign agencies if the information is related to their responsibilities and the dissemination is consistent with the interests of the United States (including national security interests) and the FBI has considered the effect such dissemination may reasonably be expected to have on any identifiable United States person;
- e. if the information is publicly available, does not identify United States persons, or is disseminated with the consent of the person whom it concerns;
- f. if the dissemination is necessary to protect the safety or security of persons or property, to protect against or prevent a crime or threat to the national security, or to obtain information for the conduct of an authorized FBI investigation; or

~~UNCLASSIFIED – FOR OFFICIAL USE ONLY~~
Domestic Investigations and Operations Guide

- g. if dissemination of the information is otherwise permitted by the Privacy Act (5 U.S.C. 552a).

2. Required Sharing

The FBI shall share and disseminate information as required by statutes, treaties, Executive Orders, Presidential directives, National Security Council directives, Homeland Security Council directives, and Attorney General-approved policies, memoranda of understanding, or agreements.

C. INFORMATION RELATING TO CRIMINAL MATTERS

1. Coordination with Prosecutors

In an investigation relating to possible criminal activity in violation of federal law, the agent conducting the investigation shall 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 agent shall present the relevant facts to the appropriate federal prosecutor. Information on investigations that have been closed shall be available on request to a United States Attorney or his or her designee or an appropriate Department of Justice official.

2. Criminal Matters Outside FBI Jurisdiction

When credible information is received by an FBI field office concerning serious criminal activity not within the FBI's investigative jurisdiction, the field office shall 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 human source, interfere with a human source's cooperation, or reveal legally privileged information. If full disclosure is not made for the reasons indicated, then, whenever feasible, the FBI field office shall make at least limited disclosure to a law enforcement agency or agencies having jurisdiction, and full disclosure shall 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 field office shall promptly notify FBI Headquarters in writing of the facts and circumstances concerning the criminal activity. The FBI shall make periodic reports to the Deputy Attorney General on such nondisclosures and incomplete disclosures, in a form suitable to protect the identity of human sources.

~~UNCLASSIFIED – FOR OFFICIAL USE ONLY~~
Domestic Investigations and Operations Guide

3. Reporting of Criminal Activity

- a. When it appears that an FBI agent or employee has engaged in criminal activity in the course of an investigation under these Guidelines, the FBI shall notify the United States Attorney's Office or an appropriate Department of Justice Division. When it appears that a human source has engaged in criminal activity in the course of an investigation under these Guidelines, the FBI shall proceed as provided in the Attorney General's Guidelines Regarding the Use of FBI Confidential Human Sources. When information concerning possible criminal activity by any other person appears in the course of an investigation under these Guidelines, the FBI shall initiate an investigation of the criminal activity if warranted, and shall proceed as provided in paragraph 1. or 2.
- b. The reporting requirements under this paragraph relating to criminal activity by FBI agents or employees or human sources do not apply to otherwise illegal activity that is authorized in conformity with these Guidelines or other Attorney General guidelines or to minor traffic offenses.

D. INFORMATION RELATING TO NATIONAL SECURITY AND FOREIGN INTELLIGENCE MATTERS

The general principle reflected in current laws and policies 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 responsibilities in this area include carrying out the requirements of the Memorandum of Understanding Between the Intelligence Community, Federal Law Enforcement Agencies, and the Department of Homeland Security Concerning Information Sharing (March 4, 2003), or any successor memorandum of understanding or agreement. Specific requirements also exist for internal coordination and consultation with other Department of Justice components, and for provision of national security and foreign intelligence information to White House agencies, as provided in the ensuing paragraphs.

1. Department of Justice

- a. The National Security Division shall 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 shall consult concerning these activities whenever requested by either of them, and the FBI shall 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

UNCLASSIFIED – ~~FOR OFFICIAL USE ONLY~~
Domestic Investigations and Operations Guide

special request under this subparagraph, the FBI shall provide annual reports to the National Security Division concerning its foreign intelligence collection program, including information concerning the scope and nature of foreign intelligence collection activities in each FBI field office.

- b. The FBI shall keep the National Security Division apprised of all information obtained through activities under these Guidelines that is necessary to the ability of the United States to investigate or protect against threats to the national security, which shall include regular consultations between the FBI and the National Security Division to exchange advice and information relevant to addressing such threats through criminal prosecution or other means.
- c. Subject to subparagraphs d. and e., relevant United States Attorneys' Offices shall have access to and shall 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 National Security Division. The relevant United States Attorneys' Offices shall receive such access and information from the FBI field offices.
- d. In a counterintelligence investigation - i.e., an investigation relating to a matter described in Part VII.S.2 of these Guidelines - the FBI's provision of information to and consultation with a United States Attorney's Office are subject to authorization by the National Security Division. In consultation with the Executive Office for United States Attorneys and the FBI, the National Security Division shall establish policies setting forth circumstances in which the FBI will consult with the National Security Division prior to informing relevant United States Attorneys' Offices about such an investigation. The policies established by the National Security Division under this subparagraph shall (among other things) provide that:
 - i. The National Security Division will, within 30 days, authorize the FBI to share with the United States Attorneys' Offices information relating to certain espionage investigations, as defined by the policies, unless such information is withheld because of substantial national security considerations; and
 - ii. the FBI may consult freely with United States Attorneys' Offices concerning investigations within the scope of this subparagraph during an emergency, so long as the National Security Division is notified of such consultation as soon as practical after the consultation.
- e. Information shared with a United States Attorney's Office pursuant to subparagraph c. or d. shall be disclosed only to the United States Attorney or any Assistant United States Attorneys designated by the United States Attorney as points of contact to receive such information. The United

~~UNCLASSIFIED – FOR OFFICIAL USE ONLY~~
Domestic Investigations and Operations Guide

States Attorneys and designated Assistant United States Attorneys shall have appropriate security clearances and shall receive training in the handling of classified information and information derived from the Foreign Intelligence Surveillance Act, 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.

- f. The disclosure and sharing of information by the FBI under this paragraph is subject to any limitations required in orders issued by the Foreign Intelligence Surveillance Court, 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 human sources is governed by the relevant provisions of the Attorney General's Guidelines Regarding the Use of FBI Confidential Human Sources.

2. White House

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

- a. Requests to the FBI for such information from the White House shall be made through the National Security Council staff or Homeland Security Council staff including, but not limited to, the National Security Council Legal and Intelligence Directorates and Office of Combating Terrorism, or through the President's Intelligence Advisory Board or the Counsel to the President.
- b. Compromising information concerning domestic officials or political organizations, or information concerning activities of United States persons intended to affect the political process in the United States, may be disseminated to the White House only with the approval of the Attorney General, based on a determination that such dissemination is needed for foreign intelligence purposes, for the purpose of protecting against international terrorism or other threats to the national security, or for the conduct of foreign affairs. However, such approval is not required for dissemination to the White House of information concerning efforts of

~~UNCLASSIFIED – FOR OFFICIAL USE ONLY~~
Domestic Investigations and Operations Guide

foreign intelligence services to penetrate the White House, or concerning contacts by White House personnel with foreign intelligence service personnel.

- c. Examples of types of information that are suitable for dissemination to the White House on a routine basis include, but not limited to:
 - i. Information concerning international terrorism;
 - ii. information concerning activities of foreign intelligence services in the United States;
 - iii. information indicative of imminent hostilities involving any foreign power;
 - iv. information concerning potential cyber threats to the United States or its allies;
 - v. information indicative of policy positions adopted by foreign officials, governments, or powers, or their reactions to United States foreign policy initiatives;
 - vi. information relating to possible changes in leadership positions of foreign governments, parties, factions, or powers;
 - vii. information concerning foreign economic or foreign political matters that might have national security ramifications; and
 - viii. information set forth in regularly published national intelligence requirements.
- d. 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 specially limit or prescribe the White House personnel who may request information concerning such issues from the FBI.
- e. The limitations on dissemination of information by the FBI to the White House under these Guidelines do not apply to dissemination to the White House of information acquired in the course of an FBI investigation requested by the White House into the background of a potential employee or appointee, or responses to requests from the White House under Executive Order 10450.

~~UNCLASSIFIED – FOR OFFICIAL USE ONLY~~
Domestic Investigations and Operations Guide

3. Special Statutory Requirements

- a. Dissemination of information acquired under the Foreign Intelligence Surveillance Act is, to the extent provided in that Act, subject to minimization procedures and other requirements specified in that Act.
- b. Information obtained through the use of National Security Letters under 15 U.S.C. 1681v may be disseminated in conformity with the general standards of this Part. Information obtained through the use of National Security Letters under other statutes may be disseminated in conformity with the general standards of this Part, subject to any applicable limitations in their governing statutory provisions: 12 U.S.C. 3414(a)(5)(B); 15 U.S.C. 1681u(f); 18 U.S.C. 2709(d); 50 U.S.C. 436(e).

UNCLASSIFIED – ~~FOR OFFICIAL USE ONLY~~
Domestic Investigations and Operations Guide

VII. DEFINITIONS

- A. **CONSENSUAL MONITORING:** monitoring of communications for which a court order or warrant is not legally required because of the consent of a party to the communication.
- B. **EMPLOYEE:** an FBI employee or an employee of another agency working under the direction and control of the FBI.
- C. **FOR OR ON BEHALF OF A FOREIGN POWER:** the determination that activities are for or on behalf of a foreign power shall be based on consideration of the extent to which the foreign power is involved in:
 - 1. control or policy direction;
 - 2. financial or material support; or
 - 3. leadership, assignments, or discipline.
- D. **FOREIGN COMPUTER INTRUSION:** the use or attempted use of any cyber-activity or other means, by, for, or on behalf of a foreign power to scan, probe, or gain unauthorized access into one or more U.S.-based computers.
- E. **FOREIGN INTELLIGENCE:** information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations or foreign persons, or international terrorists.
- F. **FOREIGN INTELLIGENCE REQUIREMENTS:**
 - 1. national intelligence requirements issued pursuant to authorization by the Director of National Intelligence, including the National Intelligence Priorities Framework and the National HUMINT Collection Directives, or any successor directives thereto;
 - 2. requests to collect foreign intelligence by the President or by Intelligence Community officials designated by the President; and
 - 3. directions to collect foreign intelligence by the Attorney General, the Deputy Attorney General, or an official designated by the Attorney General.
- G. **FOREIGN POWER:**
 - 1. a foreign government or any component thereof, whether or not recognized by the United States;
 - 2. a faction of a foreign nation or nations, not substantially composed of United States persons;
 - 3. an entity that is openly acknowledged by a foreign government or governments to be

UNCLASSIFIED – ~~FOR OFFICIAL USE ONLY~~
Domestic Investigations and Operations Guide

directed and controlled by such a foreign government or governments;

4. a group engaged in international terrorism or activities in preparation therefor;
5. a foreign-based political organization, not substantially composed of United States persons; or
6. an entity that is directed or controlled by a foreign government or governments;

H. HUMAN SOURCE: a Confidential Human Source as defined in the Attorney General's Guidelines Regarding the Use of FBI Confidential Human Sources.

I. INTELLIGENCE ACTIVITIES: any activity conducted for intelligence purposes or to affect political or governmental processes by, for, or on behalf of a foreign power.

J. INTERNATIONAL TERRORISM:

Activities that:

1. involve violent acts or acts dangerous to human life that violate federal, state, local, or tribal criminal law or would violate such law if committed within the United States or a state, local, or tribal jurisdiction;
2. appear to be intended:
 - i. to intimidate or coerce a civilian population;
 - ii. to influence the policy of a government by intimidation or coercion; or
 - iii. to affect the conduct of a government by assassination or kidnapping; and
3. occur totally outside the United States, or transcend national boundaries in terms of the means by which they are accomplished, the persons they appear to be intended to coerce or intimidate, or the locale in which their perpetrators operate or seek asylum.

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

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

M. RECORDS: any records, databases, files, indices, information systems, or other retained information.

UNCLASSIFIED – ~~FOR OFFICIAL USE ONLY~~
Domestic Investigations and Operations Guide

- N. SENSITIVE INVESTIGATIVE MATTER: an investigative matter involving the activities of a domestic public official or political candidate (involving corruption or a threat to the national security), religious or political organization or individual prominent in such an organization, or news media, or any other matter which, in the judgment of the official authorizing an investigation, should be brought to the attention of FBI Headquarters and other Department of Justice officials.
- O. SENSITIVE MONITORING CIRCUMSTANCE:
1. investigation of a member of Congress, a federal judge, a member of the Executive Branch at Executive Level IV or above, or a person who has served in such capacity within the previous two years;
 2. investigation of the Governor, Lieutenant Governor, or Attorney General of any state or territory, or a judge or justice of the highest court of any state or territory, concerning an offense involving bribery, conflict of interest, or extortion related to the performance of official duties;
 3. a party to the communication is in the custody of the Bureau of Prisons or the United States Marshals Service or is being or has been afforded protection in the Witness Security Program; or
 4. the Attorney General, the Deputy Attorney General, or an Assistant Attorney General has requested that the FBI obtain prior approval for the use of consensual monitoring in a specific investigation.
- P. SPECIAL AGENT IN CHARGE: the Special Agent in Charge of an FBI field office (including an Acting Special Agent in Charge), except that the functions authorized for Special Agents in Charge by these Guidelines may also be exercised by the Assistant Director in Charge or by any Special Agent in Charge designated by the Assistant Director in Charge in an FBI field office headed by an Assistant Director, and by FBI Headquarters officials designated by the Director of the FBI.
- Q. SPECIAL EVENTS MANAGEMENT: planning and conduct of public events or activities whose character may make them attractive targets for terrorist attack.
- R. STATE, LOCAL, OR TRIBAL: any state or territory of the United States or political subdivision thereof, the District of Columbia, or Indian tribe.
- S. THREAT TO THE NATIONAL SECURITY:
1. international terrorism;
 2. espionage and other intelligence activities, sabotage, and assassination, conducted by, for, or on behalf of foreign powers, organizations or persons;
 3. foreign computer intrusion; and

~~UNCLASSIFIED – FOR OFFICIAL USE ONLY~~
Domestic Investigations and Operations Guide

4. other matters determined by the Attorney General, consistent with Executive Order 12333 or a successor order.

T. UNITED STATES: when used in a geographic sense, means all areas under the territorial sovereignty of the United States.

U. UNITED STATES PERSON:

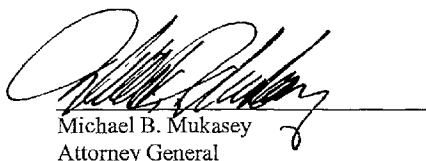
Any of the following, but not including any association or corporation that is a foreign power as defined in Subpart G.1.-3.:

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

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

V. USE: when used with respect to human sources, means obtaining information from, tasking, or otherwise operating such sources.

Date: 09/29/08


Michael B. Mukasey
Attorney General

This Page is Intentionally Blank

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

B APPENDIX B: (U) EXECUTIVE ORDER 12333

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

EXECUTIVE ORDER
12333
- - - - -

UNITED STATES INTELLIGENCE ACTIVITIES
DECEMBER 4, 1981
(AS AMENDED BY EXECUTIVE ORDERS 13284 (2003), 13355 (2004)
AND 13470 (2008))

PREAMBLE

Timely, accurate, and insightful information about the activities, capabilities, plans, and intentions of foreign powers, organizations, and persons, and their agents, is essential to the national security of the United States. All reasonable and lawful means must be used to ensure that the United States will receive the best intelligence possible. For that purpose, by virtue of the authority vested in me by the Constitution and the laws of the United States of America, including the National Security Act of 1947, as amended, (Act) and as President of the United States of America, in order to provide for the effective conduct of United States intelligence activities and the protection of constitutional rights, it is hereby ordered as follows:

PART 1 Goals, Directions, Duties, and Responsibilities with Respect to United States Intelligence Efforts

1.1 Goals. The United States intelligence effort shall provide the President, the National Security Council, and the Homeland Security Council with the necessary information on which to base decisions concerning the development and conduct of foreign, defense, and economic policies, and the protection of United States national interests from foreign security threats. All departments and agencies shall cooperate fully to fulfill this goal.

(a) All means, consistent with applicable Federal law and this order, and with full consideration of the rights of United States persons, shall be used to obtain reliable intelligence information to protect the United States and its

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

interests.

(b) The United States Government has a solemn obligation, and shall continue in the conduct of intelligence activities under this order, to protect fully the legal rights of all United States persons, including freedoms, civil liberties, and privacy rights guaranteed by Federal law.

(c) Intelligence collection under this order should be guided by the need for information to respond to intelligence priorities set by the President.

(d) Special emphasis should be given to detecting and countering:

- (1) Espionage and other threats and activities directed by foreign powers or their intelligence services against the United States and its interests;
- (2) Threats to the United States and its interests from terrorism; and
- (3) Threats to the United States and its interests from the development, possession, proliferation, or use of weapons of mass destruction.

(e) Special emphasis shall be given to the production of timely, accurate, and insightful reports, responsive to decisionmakers in the executive branch, that draw on all appropriate sources of information, including open source information, meet rigorous analytic standards, consider diverse analytic viewpoints, and accurately represent appropriate alternative views.

(f) State, local, and tribal governments are critical partners in securing and defending the United States from terrorism and other threats to the United States and its interests. Our national intelligence effort should take into account the responsibilities and requirements of State, local, and tribal governments and, as appropriate, private sector

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

entities, when undertaking the collection and dissemination of information and intelligence to protect the United States.

(g) All departments and agencies have a responsibility to prepare and to provide intelligence in a manner that allows the full and free exchange of information, consistent with applicable law and presidential guidance.

1.2 The National Security Council.

(a) *Purpose.* The National Security Council (NSC) shall act as the highest ranking executive branch entity that provides support to the President for review of, guidance for, and direction to the conduct of all foreign intelligence, counterintelligence, and covert action, and attendant policies and programs.

(b) *Covert Action and Other Sensitive Intelligence Operations.* The NSC shall consider and submit to the President a policy recommendation, including all dissents, on each proposed covert action and conduct a periodic review of ongoing covert action activities, including an evaluation of the effectiveness and consistency with current national policy of such activities and consistency with applicable legal requirements. The NSC shall perform such other functions related to covert action as the President may direct, but shall not undertake the conduct of covert actions. The NSC shall also review proposals for other sensitive intelligence operations.

1.3 Director of National Intelligence. Subject to the authority, direction, and control of the President, the Director of National Intelligence (Director) shall serve as the head of the Intelligence Community, act as the principal adviser to the President, to the NSC, and to the Homeland Security Council for intelligence matters related to national security, and shall oversee and direct the implementation of the National Intelligence Program and execution of the National Intelligence

UNCLASSIFIED - FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

Program budget. The Director will lead a unified, coordinated, and effective intelligence effort. In addition, the Director shall, in carrying out the duties and responsibilities under this section, take into account the views of the heads of departments containing an element of the Intelligence Community and of the Director of the Central Intelligence Agency.

(a) Except as otherwise directed by the President or prohibited by law, the Director shall have access to all information and intelligence described in section 1.5(a) of this order. For the purpose of access to and sharing of information and intelligence, the Director:

(1) Is hereby assigned the function under section 3(5) of the Act, to determine that intelligence, regardless of the source from which derived and including information gathered within or outside the United States, pertains to more than one United States Government agency; and

(2) Shall develop guidelines for how information or intelligence is provided to or accessed by the Intelligence Community in accordance with section 1.5(a) of this order, and for how the information or intelligence may be used and shared by the Intelligence Community. All guidelines developed in accordance with this section shall be approved by the Attorney General and, where applicable, shall be consistent with guidelines issued pursuant to section 1016 of the Intelligence Reform and Terrorism Protection Act of 2004 (Public Law 108-458) (IRTPA).

(b) In addition to fulfilling the obligations and responsibilities prescribed by the Act, the Director:

(1) Shall establish objectives, priorities, and guidance for the Intelligence Community to ensure timely and effective collection, processing, analysis, and dissemination of intelligence, of whatever nature and from whatever source

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

derived;

(2) May designate, in consultation with affected heads of departments or Intelligence Community elements, one or more Intelligence Community elements to develop and to maintain services of common concern on behalf of the Intelligence Community if the Director determines such services can be more efficiently or effectively accomplished in a consolidated manner;

(3) Shall oversee and provide advice to the President and the NSC with respect to all ongoing and proposed covert action programs;

(4) In regard to the establishment and conduct of intelligence arrangements and agreements with foreign governments and international organizations:

(A) May enter into intelligence and counterintelligence arrangements and agreements with foreign governments and international organizations;

(B) Shall formulate policies concerning intelligence and counterintelligence arrangements and agreements with foreign governments and international organizations; and

(C) Shall align and synchronize intelligence and counterintelligence foreign relationships among the elements of the Intelligence Community to further United States national security, policy, and intelligence objectives;

(E) Shall participate in the development of procedures approved by the Attorney General governing criminal drug intelligence activities abroad to ensure that these activities are consistent with foreign intelligence programs;

(6) Shall establish common security and access standards for managing and handling intelligence systems, information, and products, with special emphasis on facilitating:

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

(A) The fullest and most prompt access to and dissemination of information and intelligence practicable, assigning the highest priority to detecting, preventing, preempting, and disrupting terrorist threats and activities against the United States, its interests, and allies; and

(B) The establishment of standards for an interoperable information sharing enterprise that facilitates the sharing of intelligence information among elements of the Intelligence Community;

(7) Shall ensure that appropriate departments and agencies have access to intelligence and receive the support needed to perform independent analysis;

(8) Shall protect, and ensure that programs are developed to protect, intelligence sources, methods, and activities from unauthorized disclosure;

(9) Shall, after consultation with the heads of affected departments and agencies, establish guidelines for Intelligence Community elements for:

(A) Classification and declassification of all intelligence and intelligence-related information classified under the authority of the Director or the authority of the head of a department or Intelligence Community element; and

(B) Access to and dissemination of all intelligence and intelligence-related information, both in its final form and in the form when initially gathered, to include intelligence originally classified by the head of a department or Intelligence Community element, except that access to and dissemination of information concerning United States persons shall be governed by procedures developed in accordance with Part 2 of this order;

(10) May, only with respect to Intelligence Community elements, and after consultation with the head of the

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

originating Intelligence Community element or the head of the originating department, declassify, or direct the declassification of, information on intelligence relating to intelligence sources, methods, and activities. The Director may only delegate this authority to the Principal Deputy Director of National Intelligence;

(11) May establish, operate, and direct one or more national intelligence centers to address intelligence priorities;

(12) May establish Functional Managers and Mission Managers, and designate officers or employees of the United States to serve in these positions.

(A) Functional Managers shall report to the Director concerning the execution of their duties as Functional Managers, and may be charged with developing and implementing strategic guidance, policies, and procedures for activities related to a specific intelligence discipline or set of intelligence activities; set training and tradescraft standards; and ensure coordination within and across intelligence disciplines and Intelligence Community elements and with related non-intelligence activities. Functional Managers may also advise the Director on: the management of resources; policies and procedures; collection capabilities and gaps; processing and dissemination of intelligence; technical architectures; and other issues or activities determined by the Director.

(i) The Director of the National Security Agency is designated the Functional Manager for signals intelligence;

(ii) The Director of the Central Intelligence Agency is designated the Functional Manager for human intelligence; and

(iii) The Director of the National

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

Geospatial-Intelligence Agency is designated the Functional Manager for geospatial intelligence.

(B) Mission Managers shall serve as principal substantive advisers on all or specified aspects of intelligence related to designated countries, regions, topics, or functional issues;

(13) Shall establish uniform criteria for the determination of relative priorities for the transmission of critical foreign intelligence, and advise the Secretary of Defense concerning the communications requirements of the Intelligence Community for the transmission of such communications;

(14) Shall have ultimate responsibility for production and dissemination of intelligence produced by the Intelligence Community and authority to levy analytic tasks on intelligence production organizations within the Intelligence Community, in consultation with the heads of the Intelligence Community elements concerned;

(15) May establish advisory groups for the purpose of obtaining advice from within the Intelligence Community to carry out the Director's responsibilities, to include Intelligence Community executive management committees composed of senior Intelligence Community leaders. Advisory groups shall consist of representatives from elements of the Intelligence Community, as designated by the Director, or other executive branch departments, agencies, and offices, as appropriate;

(16) Shall ensure the timely exploitation and dissemination of data gathered by national intelligence collection means, and ensure that the resulting intelligence is disseminated immediately to appropriate government elements, including military commands;

(17) Shall determine requirements and priorities

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

for, and manage and direct the tasking, collection, analysis, production, and dissemination of, national intelligence by elements of the Intelligence Community, including approving requirements for collection and analysis and resolving conflicts in collection requirements and in the tasking of national collection assets of Intelligence Community elements (except when otherwise directed by the President or when the Secretary of Defense exercises collection tasking authority under plans and arrangements approved by the Secretary of Defense and the Director);

(18) May provide advisory tasking concerning collection and analysis of information or intelligence relevant to national intelligence or national security to departments, agencies, and establishments of the United States Government that are not elements of the Intelligence Community; and shall establish

procedures, in consultation with affected heads of departments or agencies and subject to approval by the Attorney General, to implement this authority and to monitor or evaluate the responsiveness of United States Government departments, agencies, and other establishments;

(19) Shall fulfill the responsibilities in section 1.3(b)(17) and (18) of this order, consistent with applicable law and with full consideration of the rights of United States persons, whether information is to be collected inside or outside the United States;

(20) Shall ensure, through appropriate policies and procedures, the deconfliction, coordination, and integration of all intelligence activities conducted by an Intelligence Community element or funded by the National Intelligence Program. In accordance with these policies and procedures:

(A) The Director of the Federal Bureau of

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

Investigation shall coordinate the clandestine collection of foreign intelligence collected through human sources or through human-enabled means and counterintelligence activities inside the United States;

(B) The Director of the Central Intelligence Agency shall coordinate the clandestine collection of foreign intelligence collected through human sources or through human-enabled means and counterintelligence activities outside the United States;

(C) All policies and procedures for the coordination of counterintelligence activities and the clandestine collection of foreign intelligence inside the United States shall be subject to the approval of the Attorney General; and

(D) All policies and procedures developed under this section shall be coordinated with the heads of affected departments and Intelligence Community elements;

(21) Shall, with the concurrence of the heads of affected departments and agencies, establish joint procedures to deconflict, coordinate, and synchronize intelligence activities conducted by an Intelligence Community element or funded by the National Intelligence Program, with intelligence activities, activities that involve foreign intelligence and security services, or activities that involve the use of clandestine methods, conducted by other United States Government departments, agencies, and establishments;

(22) Shall, in coordination with the heads of departments containing elements of the Intelligence Community, develop procedures to govern major system acquisitions funded in whole or in majority part by the National Intelligence Program;

(23) Shall seek advice from the Secretary of State to ensure that the foreign policy implications of proposed

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

intelligence activities are considered, and shall ensure, through appropriate policies and procedures, that intelligence activities are conducted in a manner consistent with the responsibilities pursuant to law and presidential direction of Chiefs of United States Missions; and

(24) Shall facilitate the use of Intelligence Community products by the Congress in a secure manner.

(c) The Director's exercise of authorities in the Act and this order shall not abrogate the statutory or other responsibilities of the heads of departments of the United States Government or the Director of the Central Intelligence Agency. Directives issued and actions taken by the Director in the exercise of the Director's authorities and responsibilities to integrate, coordinate, and make the Intelligence Community more effective in providing intelligence related to national security shall be implemented by the elements of the Intelligence Community, provided that any department head whose department contains an element of the Intelligence Community and who believes that a directive or action of the Director violates the requirements of section 1018 of the IRTPA or this subsection shall bring the issue to the attention of the Director, the NSC, or the President for resolution in a manner that respects and does not abrogate the statutory responsibilities of the heads of the departments.

(d) Appointments to certain positions.

(1) The relevant department or bureau head shall provide recommendations and obtain the concurrence of the Director for the selection of: the Director of the National Security Agency, the Director of the National Reconnaissance Office, the Director of the National Geospatial-Intelligence Agency, the Under Secretary of Homeland Security for Intelligence and Analysis, the Assistant Secretary of State for

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

Intelligence and Research, the Director of the Office of Intelligence and Counterintelligence of the Department of Energy, the Assistant Secretary for Intelligence and Analysis of the Department of the Treasury, and the Executive Assistant Director for the National Security Branch of the Federal Bureau of Investigation. If the Director does not concur in the recommendation, the department head may not fill the vacancy or make the recommendation to the President, as the case may be. If the department head and the Director do not reach an agreement on the selection or recommendation, the Director and the department head concerned may advise the President directly of the Director's intention to withhold concurrence.

(2) The relevant department head shall consult with the Director before appointing an individual to fill a vacancy or recommending to the President an individual be nominated to fill a vacancy in any of the following positions: the Under Secretary of Defense for Intelligence; the Director of the Defense Intelligence Agency; uniformed heads of the intelligence elements of the Army, the Navy, the Air Force, and the Marine Corps above the rank of Major General or Rear Admiral; the Assistant Commandant of the Coast Guard for Intelligence; and the Assistant Attorney General for National Security.

(c) Removal from certain positions.

(1) Except for the Director of the Central Intelligence Agency, whose removal the Director may recommend to the President, the Director and the relevant department head shall consult on the removal, or recommendation to the President for removal, as the case may be, of: the Director of the National Security Agency, the Director of the National Geospatial-Intelligence Agency, the Director of the Defense Intelligence Agency, the Under Secretary of Homeland Security for Intelligence and Analysis, the Assistant Secretary of State

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

for Intelligence and Research, and the Assistant Secretary for Intelligence and Analysis of the Department of the Treasury. If the Director and the department head do not agree on removal, or recommendation for removal, either may make a recommendation to the President for the removal of the individual.

(2) The Director and the relevant department or bureau head shall consult on the removal of: the Executive Assistant Director for the National Security Branch of the Federal Bureau of Investigation, the Director of the Office of Intelligence and Counterintelligence of the Department of Energy, the Director of the National Reconnaissance Office, the Assistant Commandant of the Coast Guard for Intelligence, and the Under Secretary of Defense for Intelligence. With respect to an individual appointed by a department head, the department head may remove the individual upon the request of the Director; if the department head chooses not to remove the individual, either the Director or the department head may advise the President of the department head's intention to retain the individual. In the case of the Under Secretary of Defense for Intelligence, the Secretary of Defense may recommend to the President either the removal or the retention of the individual. For uniformed heads of the intelligence elements of the Army, the Navy, the Air Force, and the Marine Corps, the Director may make a recommendation for removal to the Secretary of Defense.

(3) Nothing in this subsection shall be construed to limit or otherwise affect the authority of the President to nominate, appoint, assign, or terminate the appointment or assignment of any individual, with or without a consultation, recommendation, or concurrence.

1.4 *The Intelligence Community.* Consistent with applicable Federal law and with the other provisions of this order, and

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

under the leadership of the Director, as specified in each law and this order, the Intelligence Community shall:

(a) Collect and provide information needed by the President and, in the performance of executive functions, the Vice President, the NSC, the Homeland Security Council, the Chairman of the Joint Chiefs of Staff, senior military commanders, and other executive branch officials and, as appropriate, the Congress of the United States;

(b) In accordance with priorities set by the President, collect information concerning, and conduct activities to protect against, international terrorism, proliferation of weapons of mass destruction, intelligence activities directed against the United States, international criminal drug activities, and other hostile activities directed against the United States by foreign powers, organizations, persons, and their agents;

(c) Analyze, produce, and disseminate intelligence;

(d) Conduct administrative, technical, and other support activities within the United States and abroad necessary for the performance of authorized activities, to include providing services of common concern for the Intelligence Community as designated by the Director in accordance with this order;

(e) Conduct research, development, and procurement of technical systems and devices relating to authorized functions and missions or the provision of services of common concern for the Intelligence Community;

(f) Protect the security of intelligence related activities, information, installations, property, and employees by appropriate means, including such investigations of applicants, employees, contractors, and other persons with similar associations with the Intelligence Community elements as are necessary;

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

(g) Take into account State, local, and tribal governments' and, as appropriate, private sector entities' information needs relating to national and homeland security;

(h) Deconflict, coordinate, and integrate all intelligence activities and other information gathering in accordance with section 1.3(h)(20) of this order; and

(i) Perform such other functions and duties related to intelligence activities as the President may direct.

1.5 Duties and Responsibilities of the Heads of Executive Branch Departments and Agencies. The heads of all departments and agencies shall:

(a) Provide the Director access to all information and intelligence relevant to the national security or that otherwise is required for the performance of the Director's duties, to include administrative and other appropriate management information, except such information excluded by law, by the President, or by the Attorney General acting under this order at the direction of the President;

(b) Provide all programmatic and budgetary information necessary to support the Director in developing the National Intelligence Program;

(c) Coordinate development and implementation of intelligence systems and architectures and, as appropriate, operational systems and architectures of their departments, agencies, and other elements with the Director to respond to national intelligence requirements and all applicable information sharing and security guidelines, information privacy, and other legal requirements;

(d) Provide, to the maximum extent permitted by law, subject to the availability of appropriations and not inconsistent with the mission of the department or agency, such further support to the Director as the Director may request.

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

after consultation with the head of the department or agency, for the performance of the Director's functions;

(e) Respond to advisory tasking from the Director under section 1.3(b)(18) of this order to the greatest extent possible, in accordance with applicable policies established by the head of the responding department or agency;

(f) Ensure that all elements within the department or agency comply with the provisions of Part 2 of this order, regardless of Intelligence Community affiliation, when performing foreign intelligence and counterintelligence functions;

(g) Deconflict, coordinate, and integrate all intelligence activities in accordance with section 1.3(b)(20), and intelligence and other activities in accordance with section 1.3(b)(21) of this order;

(h) Inform the Attorney General, either directly or through the Federal Bureau of Investigation, and the Director of clandestine collection of foreign intelligence and counterintelligence activities inside the United States not coordinated with the Federal Bureau of Investigation;

(i) Pursuant to arrangements developed by the head of the department or agency and the Director of the Central Intelligence Agency and approved by the Director, inform the Director and the Director of the Central Intelligence Agency, either directly or through his designee serving outside the United States, as appropriate, of clandestine collection of foreign intelligence collected through human sources or through human-enabled means outside the United States that has not been coordinated with the Central Intelligence Agency; and

(j) Inform the Secretary of Defense, either directly or through his designee, as appropriate, of clandestine collection of foreign intelligence outside the United States in a region of

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

combat or contingency military operations designated by the Secretary of Defense, for purposes of this paragraph, after consultation with the Director of National Intelligence.

1.6 *Heads of Elements of the Intelligence Community.* The heads of elements of the Intelligence Community shall:

(a) Provide the Director access to all information and intelligence relevant to the national security or that otherwise is required for the performance of the Director's duties, to include administrative and other appropriate management information, except such information excluded by law, by the President, or by the Attorney General acting under this order at the direction of the President;

(b) Report to the Attorney General possible violations of Federal criminal laws by employees and of specified Federal criminal laws by any other person as provided in procedures agreed upon by the Attorney General and the head of the department, agency, or establishment concerned, in a manner consistent with the protection of intelligence sources and methods, as specified in those procedures;

(c) Report to the Intelligence Oversight Board, consistent with Executive Order 13462 of February 28, 2008, and provide copies of all such reports to the Director, concerning any intelligence activities of their elements that they have reason to believe may be unlawful or contrary to executive order or presidential directives;

(d) Protect intelligence and intelligence sources, methods, and activities from unauthorized disclosure in accordance with guidance from the Director;

(e) Facilitate, as appropriate, the sharing of information or intelligence, as directed by law or the President, to State, local, tribal, and private sector entities;

(f) Disseminate information or intelligence to foreign

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

governments and international organizations under intelligence or counterintelligence arrangements or agreements established in accordance with section 1.3(b)(4) of this order;

(g) Participate in the development of procedures approved by the Attorney General governing production and dissemination of information or intelligence resulting from criminal drug intelligence activities abroad if they have intelligence responsibilities for foreign or domestic criminal drug production and trafficking; and

(h) Ensure that the inspectors general, general counsels, and agency officials responsible for privacy or civil liberties protection for their respective organizations have access to any information or intelligence necessary to perform their official duties.

1.7 *Intelligence Community Elements.* Each element of the Intelligence Community shall have the duties and responsibilities specified below, in addition to those specified by law or elsewhere in this order. Intelligence Community elements within executive departments shall serve the information and intelligence needs of their respective heads of departments and also shall operate as part of an integrated Intelligence Community, as provided in law or this order.

(a) *THE CENTRAL INTELLIGENCE AGENCY.* The Director of the Central Intelligence Agency shall:

(1) Collect (including through clandestine means), analyze, produce, and disseminate foreign intelligence and counterintelligence;

(2) Conduct counterintelligence activities without assuming or performing any internal security functions within the United States;

(3) Conduct administrative and technical support activities within and outside the United States as necessary for

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

cover and proprietary arrangements;

(4) Conduct covert action activities approved by the President. No agency except the Central Intelligence Agency (or the Armed Forces of the United States in time of war declared by the Congress or during any period covered by a report from the President to the Congress consistent with the War Powers Resolution, Public Law 93-148) may conduct any covert action activity unless the President determines that another agency is more likely to achieve a particular objective;

(5) Conduct foreign intelligence liaison relationships with intelligence or security services of foreign governments or international organizations consistent with section 1.3(b)(4) of this order;

(6) Under the direction and guidance of the Director, and in accordance with section 1.3(b)(4) of this order, coordinate the implementation of intelligence and counterintelligence relationships between elements of the Intelligence Community and the intelligence or security services of foreign governments or international organizations; and

(7) Perform such other functions and duties related to intelligence as the Director may direct.

(b) THE DEFENSE INTELLIGENCE AGENCY. The Director of the Defense Intelligence Agency shall:

(1) Collect (including through clandestine means), analyze, produce, and disseminate foreign intelligence and counterintelligence to support national and departmental missions;

(2) Collect, analyze, produce, or, through tasking and coordination, provide defense and defense-related intelligence for the Secretary of Defense, the Chairman of the Joint Chiefs of Staff, combatant commanders, other Defense components, and non-Defense agencies;

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

- (3) Conduct counterintelligence activities;
 - (4) Conduct administrative and technical support activities within and outside the United States as necessary for cover and proprietary arrangements;
 - (5) Conduct foreign defense intelligence liaison relationships and defense intelligence exchange programs with foreign defense establishments, intelligence or security services of foreign governments, and international organizations in accordance with sections 1.3(b)(4), 1.7(a)(6), and 1.10(1) of this order;
 - (6) Manage and coordinate all matters related to the Defense Attaché system; and
 - (7) Provide foreign intelligence and counterintelligence staff support as directed by the Secretary of Defense.
- (c) THE NATIONAL SECURITY AGENCY. The Director of the National Security Agency shall:
- (1) Collect (including through clandestine means), process, analyze, produce, and disseminate signals intelligence information and data for foreign intelligence and counterintelligence purposes to support national and departmental missions;
 - (2) Establish and operate an effective unified organization for signals intelligence activities, except for the delegation of operational control over certain operations that are conducted through other elements of the Intelligence Community. No other department or agency may engage in signals intelligence activities except pursuant to a delegation by the Secretary of Defense, after coordination with the Director;
 - (3) Control signals intelligence collection and processing activities, including assignment of resources to an appropriate agent for such periods and tasks as required for the

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

direct support of military commanders;

(4) Conduct administrative and technical support activities within and outside the United States as necessary for cover arrangements;

(5) Provide signals intelligence support for national and departmental requirements and for the conduct of military operations;

(6) Act as the National Manager for National Security Systems as established in law and policy, and in this capacity be responsible to the Secretary of Defense and to the Director;

(7) Prescribe, consistent with section 102A(g) of the Act, within its field of authorized operations, security regulations covering operating practices, including the transmission, handling, and distribution of signals intelligence and communications security material within and among the elements under control of the Director of the National Security Agency, and exercise the necessary supervisory control to ensure compliance with the regulations; and

(8) Conduct foreign cryptologic liaison relationships in accordance with sections 1.3(b)(4), 1.7(a)(6), and 1.10(i) of this order.

(d) THE NATIONAL RECONNAISSANCE OFFICE. The Director of the National Reconnaissance Office shall:

(1) Be responsible for research and development, acquisition, launch, deployment, and operation of overhead systems and related data processing facilities to collect intelligence and information to support national and departmental missions and other United States Government needs; and

(2) Conduct foreign liaison relationships relating to the above missions, in accordance with sections 1.3(b)(4), 1.7(a)(6), and 1.10(i) of this order.

UNCLASSIFIED - FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

(e) **THE NATIONAL GEOSPATIAL-INTELLIGENCE AGENCY.** The Director of the National Geospatial-Intelligence Agency shall:

(1) Collect, process, analyze, produce, and disseminate geospatial intelligence information and data for foreign intelligence and counterintelligence purposes to support national and departmental missions;

(2) Provide geospatial intelligence support for national and departmental requirements and for the conduct of military operations;

(3) Conduct administrative and technical support activities within and outside the United States as necessary for cover arrangements; and

(4) Conduct foreign geospatial intelligence liaison relationships, in accordance with sections 1.3(b)(4), 1.7(a)(9), and 1.16(i) of this order.

(f) **THE INTELLIGENCE AND COUNTERINTELLIGENCE ELEMENTS OF THE ARMY, NAVY, AIR FORCE, AND MARINE CORPS.** The Commanders and heads of the intelligence and counterintelligence elements of the Army, Navy, Air Force, and Marine Corps shall:

(1) Collect (including through clandestine means), produce, analyze, and disseminate defense and defense-related intelligence and counterintelligence to support departmental requirements, and, as appropriate, national requirements;

(2) Conduct counterintelligence activities;

(3) Monitor the development, procurement, and management of tactical intelligence systems and equipment and conduct related research, development, and test and evaluation activities; and

(4) Conduct military intelligence liaison relationships and military intelligence exchange programs with selected cooperative foreign defense establishments and international organizations in accordance with

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

sections 1.3(b)(3), 1.7(a)(6), and 1.10(1) of this order.

(g) INTELLIGENCE ELEMENTS OF THE FEDERAL BUREAU OF INVESTIGATION. Under the supervision of the Attorney General and pursuant to such regulations as the Attorney General may establish, the intelligence elements of the Federal Bureau of Investigation shall:

(1) Collect (including through clandestine means), analyze, produce, and disseminate foreign intelligence and counterintelligence to support national and departmental missions, in accordance with procedural guidelines approved by the Attorney General, after consultation with the Director;

(2) Conduct counterintelligence activities; and

(3) Conduct foreign intelligence and counterintelligence liaison relationships with intelligence, security, and law enforcement services of foreign governments or international organizations in accordance with sections 1.3(b)(4) and 1.7(a)(6) of this order.

(h) THE INTELLIGENCE AND COUNTERINTELLIGENCE ELEMENTS OF THE COAST GUARD. The Commandant of the Coast Guard shall:

(1) Collect (including through clandestine means), analyze, produce, and disseminate foreign intelligence and counterintelligence including defense and defense-related information and intelligence to support national and departmental missions;

(2) Conduct counterintelligence activities;

(3) Monitor the development, procurement, and management of tactical intelligence systems and equipment and conduct related research, development, and test and evaluation activities; and

(4) Conduct foreign intelligence liaison relationships and intelligence exchange programs with foreign intelligence services, security services or international

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

organizations in accordance with sections 1.3(b)(4), 1.7(a)(6), and, when operating as part of the Department of Defense, 1.10(i) of this order.

(1) THE BUREAU OF INTELLIGENCE AND RESEARCH, DEPARTMENT OF STATE; THE OFFICE OF INTELLIGENCE AND ANALYSIS, DEPARTMENT OF THE TREASURY; THE OFFICE OF NATIONAL SECURITY INTELLIGENCE, DRUG ENFORCEMENT ADMINISTRATION; THE OFFICE OF INTELLIGENCE AND ANALYSIS, DEPARTMENT OF HOMELAND SECURITY; AND THE OFFICE OF INTELLIGENCE AND COUNTERINTELLIGENCE, DEPARTMENT OF ENERGY. The heads of the Bureau of Intelligence and Research, Department of State; the Office of Intelligence and Analysis, Department of the Treasury; the Office of National Security Intelligence, Drug Enforcement Administration; the Office of Intelligence and Analysis, Department of Homeland Security; and the Office of Intelligence and Counterintelligence, Department of Energy shall:

(1) Collect (overtly or through publicly available sources), analyze, produce, and disseminate information, intelligence, and counterintelligence to support national and departmental missions; and

(2) Conduct and participate in analytic or information exchanges with foreign partners and international organizations in accordance with sections 1.3(b)(4) and 1.7(a)(6) of this order.

(3) THE OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE. The Director shall collect (overtly or through publicly available sources), analyze, produce, and disseminate information, intelligence, and counterintelligence to support the missions of the Office of the Director of National Intelligence, including the National Counterterrorism Center, and to support other national missions.

1.9 The Department of State. In addition to the authorities

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

exercised by the Bureau of Intelligence and Research under sections 1.4 and 1.7(1) of this order, the Secretary of State shall:

- (a) Collect (overtly or through publicly available sources) information relevant to United States foreign policy and national security concerns;
- (b) Disseminate, to the maximum extent possible, reports received from United States diplomatic and consular posts;
- (c) Transmit reporting requirements and advisory taskings of the Intelligence Community to the Chiefs of United States Missions abroad; and
- (d) Support Chiefs of United States Missions in discharging their responsibilities pursuant to law and presidential direction.

1.9 The Department of the Treasury. In addition to the authorities exercised by the Office of Intelligence and Analysis of the Department of the Treasury under sections 1.4 and 1.7(1) of this order the Secretary of the Treasury shall collect (overtly or through publicly available sources) foreign financial information and, in consultation with the Department of State, foreign economic information.

1.10 The Department of Defense. The Secretary of Defense shall:

- (a) Collect (including through clandestine means), analyze, produce, and disseminate information and intelligence and be responsive to collection tasking and advisory tasking by the Director;
- (b) Collect (including through clandestine means), analyze, produce, and disseminate defense and defense-related intelligence and counterintelligence, as required for execution of the Secretary's responsibilities;
- (c) Conduct programs and missions necessary to fulfill

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

national, departmental, and tactical intelligence requirements;

(d) Conduct counterintelligence activities in support of Department of Defense components and coordinate counterintelligence activities in accordance with section 1.3(b)(20) and (23) of this order;

(e) Act, in coordination with the Director, as the executive agent of the United States Government for signals intelligence activities;

(f) Provide for the timely transmission of critical intelligence, as defined by the Director, within the United States Government;

(g) Carry out or contract for research, development, and procurement of technical systems and devices relating to authorized intelligence functions;

(h) Protect the security of Department of Defense installations, activities, information, property, and employees by appropriate means, including such investigations of applicants, employees, contractors, and other persons with similar associations with the Department of Defense as are necessary;

(i) Establish and maintain defense intelligence relationships and defense intelligence exchange programs with selected cooperative foreign defense establishments, intelligence or security services of foreign governments, and international organizations, and ensure that such relationships and programs are in accordance with sections 1.3(b)(4), 1.3(b)(21) and 1.7(a)(6) of this order;

(j) Conduct such administrative and technical support activities within and outside the United States as are necessary to provide for cover and proprietary arrangements, to perform the functions described in sections (a) through (i) above, and to support the Intelligence Community elements of the Department of

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

Defense; and

(k) Use the Intelligence Community elements within the Department of Defense identified in section 1.7(b) through (f) and, when the Coast Guard is operating as part of the Department of Defense,

(h) above to carry out the Secretary of Defense's responsibilities assigned in this section or other departments, agencies, or offices within the Department of Defense, as appropriate, to conduct the intelligence missions and responsibilities assigned to the Secretary of Defense.

1.11 *The Department of Homeland Security.* In addition to the authorities exercised by the Office of Intelligence and Analysis of the Department of Homeland Security under sections 1.4 and 1.7(i) of this order, the Secretary of Homeland Security shall conduct, through the United States Secret Service, activities to determine the existence and capability of surveillance equipment being used against the President or the Vice President of the United States, the Executive Office of the President, and, as authorized by the Secretary of Homeland Security or the President, other Secret Service protectees and United States officials. No information shall be acquired intentionally through such activities except to protect against use of such surveillance equipment, and these activities shall be conducted pursuant to procedures agreed upon by the Secretary of Homeland Security and the Attorney General.

1.12 *The Department of Energy.* In addition to the authorities exercised by the Office of Intelligence and Counterintelligence of the Department of Energy under sections 1.4 and 1.7(i) of this order, the Secretary of Energy shall:

(a) Provide expert scientific, technical, analytic, and research capabilities to other agencies within the Intelligence Community, as appropriate:

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

(b) Participate in formulating intelligence collection and analysis requirements where the special expert capability of the Department can contribute; and

(c) Participate with the Department of State in overtly collecting information with respect to foreign energy matters.

1.13 *The Federal Bureau of Investigation.* In addition to the authorities exercised by the intelligence elements of the Federal Bureau of Investigation of the Department of Justice under sections 1.4 and 1.7(g) of this order and under the supervision of the Attorney General and pursuant to such regulations as the Attorney General may establish, the Director of the Federal Bureau of Investigation shall provide technical assistance, within or outside the United States, to foreign intelligence and law enforcement services, consistent with section 1.3(b)(20) and (21) of this order, as may be necessary to support national or departmental missions.

PART 2 *Conduct of Intelligence Activities*

2.1 *Need.* Timely, accurate, and insightful information about the activities, capabilities, plans, and intentions of foreign powers, organizations, and persons, and their agents, is essential to informed decisionmaking in the areas of national security, national defense, and foreign relations. Collection of such information is a priority objective and will be pursued in a vigorous, innovative, and responsible manner that is consistent with the Constitution and applicable law and respectful of the principles upon which the United States was founded.

2.2 *Purpose.* This Order is intended to enhance human and technical collection techniques, especially those undertaken abroad, and the acquisition of significant foreign intelligence, as well as the detection and countering of international terrorist activities, the spread of weapons of mass destruction,

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

and espionage conducted by foreign powers. Set forth below are certain general principles that, in addition to and consistent with applicable laws, are intended to achieve the proper balance between the acquisition of essential information and protection of individual interests. Nothing in this Order shall be construed to apply to or interfere with any authorized civil or criminal law enforcement responsibility of any department or agency.

2.3 Collection of information. Elements of the Intelligence Community are authorized to collect, retain, or disseminate information concerning United States persons only in accordance with procedures established by the head of the Intelligence Community element concerned or by the head of a department containing such element and approved by the Attorney General, consistent with the authorities provided by Part 1 of this Order, after consultation with the Director. Those procedures shall permit collection, retention, and dissemination of the following types of information:

- (a) Information that is publicly available or collected with the consent of the person concerned;
- (b) Information constituting foreign intelligence or counterintelligence, including such information concerning corporations or other commercial organizations. Collection within the United States of foreign intelligence not otherwise obtainable shall be undertaken by the Federal Bureau of Investigation (FBI) or, when significant foreign intelligence is sought, by other authorized elements of the Intelligence Community, provided that no foreign intelligence collection by such elements may be undertaken for the purpose of acquiring information concerning the domestic activities of United States persons;
- (c) Information obtained in the course of a lawful foreign

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

intelligence, counterintelligence, international drug or international terrorism investigation;

(d) Information needed to protect the safety of any persons or organizations, including those who are targets, victims, or hostages of international terrorist organizations;

(e) Information needed to protect foreign intelligence or counterintelligence sources, methods, and activities from unauthorized disclosure. Collection within the United States shall be undertaken by the FBI except that other elements of the Intelligence Community may also collect such information concerning present or former employees, present or former intelligence element contractors or their present or former employees, or applicants for such employment or contracting;

(f) Information concerning persons who are reasonably believed to be potential sources or contacts for the purpose of determining their suitability or credibility;

(g) Information arising out of a lawful personnel, physical, or communications security investigation;

(h) Information acquired by overhead reconnaissance not directed at specific United States persons;

(i) Incidentally obtained information that may indicate involvement in activities that may violate Federal, state, local, or foreign laws; and

(j) Information necessary for administrative purposes.

In addition, elements of the Intelligence Community may disseminate information to each appropriate element within the Intelligence Community for purposes of allowing the recipient element to determine whether the information is relevant to its responsibilities and can be retained by it, except that information derived from signals intelligence may only be disseminated or made available to Intelligence Community elements in accordance with procedures established by the

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

Director in coordination with the Secretary of Defense and approved by the Attorney General.

2.4 Collection Techniques. Elements of the Intelligence Community shall use the least intrusive collection techniques feasible within the United States or directed against United States persons abroad. Elements of the Intelligence Community are not authorized to use such techniques as electronic surveillance, unconsented physical searches, mail surveillance, physical surveillance, or monitoring devices unless they are in accordance with procedures established by the head of the Intelligence Community element concerned or the head of a department containing such element and approved by the Attorney General, after consultation with the Director. Such procedures shall protect constitutional and other legal rights and limit use of such information to lawful governmental purposes. These procedures shall not authorize:

(a) The Central Intelligence Agency (CIA) to engage in electronic surveillance within the United States except for the purpose of training, testing, or conducting countermeasures to hostile electronic surveillance;

(b) Unconsented physical searches in the United States by elements of the Intelligence Community other than the FBI, except for:

(1) Searches by counterintelligence elements of the military services directed against military personnel within the United States or abroad for intelligence purposes, when authorized by a military commander empowered to approve physical searches for law enforcement purposes, based upon a finding of probable cause to believe that such persons are acting as agents of foreign powers; and

(2) Searches by CIA of personal property of non-United States persons lawfully in its possession;

UNCLASSIFIED - FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

(c) Physical surveillance of a United States person in the United States by elements of the Intelligence Community other than the FBI, except for:

(1) Physical surveillance of present or former employees, present or former intelligence element contractors or their present or former employees, or applicants for any such employment or contracting; and

(2) Physical surveillance of a military person employed by a non-intelligence element of a military service; and

(d) Physical surveillance of a United States person abroad to collect foreign intelligence, except to obtain significant information that cannot reasonably be acquired by other means.

2.5 Attorney General Approval. The Attorney General hereby is delegated the power to approve the use for intelligence purposes, within the United States or against a United States person abroad, of any technique for which a warrant would be required if undertaken for law enforcement purposes, provided that such techniques shall not be undertaken unless the Attorney General has determined in each case that there is probable cause to believe that the technique is directed against a foreign power or an agent of a foreign power. The authority delegated pursuant to this paragraph, including the authority to approve the use of electronic surveillance as defined in the Foreign Intelligence Surveillance Act of 1978, as amended, shall be exercised in accordance with that Act.

2.6 Assistance to Law Enforcement and other Civil Authorities.

Elements of the Intelligence Community are authorized to:

(a) Cooperate with appropriate law enforcement agencies for the purpose of protecting the employees, information, property, and facilities of any element of the Intelligence Community;

(b) Unless otherwise precluded by law or this Order,

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

participate in law enforcement activities to investigate or prevent clandestine intelligence activities by foreign powers, or international terrorist or narcotics activities;

(c) Provide specialized equipment, technical knowledge, or assistance of expert personnel for use by any department or agency, or when lives are endangered, to support local law enforcement agencies. Provision of assistance by expert personnel shall be approved in each case by the general counsel of the providing element or department; and

(d) Render any other assistance and cooperation to law enforcement or other civil authorities not precluded by applicable law.

2.7 Contracting. Elements of the Intelligence Community are authorized to enter into contracts or arrangements for the provision of goods or services with private companies or institutions in the United States and need not reveal the sponsorship of such contracts or arrangements for authorized intelligence purposes. Contracts or arrangements with academic institutions may be undertaken only with the consent of appropriate officials of the institution.

2.8 Consistency With Other Laws. Nothing in this Order shall be construed to authorize any activity in violation of the Constitution or statutes of the United States.

2.9 Undisclosed Participation in Organizations Within the United States. No one acting on behalf of elements of the Intelligence Community may join or otherwise participate in any organization in the United States on behalf of any element of the Intelligence Community without 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 or the head of a department containing such element and approved by

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

the Attorney General, after consultation with the Director. Such participation shall be authorized only if it is essential to achieving lawful purposes as determined by the Intelligence Community element head or designee. No such participation may be undertaken for the purpose of influencing the activity of the organization or its members except in cases where:

(a) The participation is undertaken on behalf of the FBI in the course of a lawful investigation; or

(b) The organization concerned is composed primarily of individuals who are not United States persons and is reasonably believed to be acting on behalf of a foreign power.

2.10 *Human Experimentation.* No element of the Intelligence Community shall sponsor, contract for, or conduct research on human subjects except in accordance with guidelines issued by the Department of Health and Human Services. The subject's informed consent shall be documented as required by those guidelines.

2.11 *Prohibition on Assassination.* No person employed by or acting on behalf of the United States Government shall engage in or conspire to engage in assassination.

2.12 *Indirect Participation.* No element of the Intelligence Community shall participate in or request any person to undertake activities forbidden by this Order.

2.13 *Limitation on Covert Action.* No covert action may be conducted which is intended to influence United States political processes, public opinion, policies, or media.

PART 3 *General Provisions*

3.1 *Congressional Oversight.* The duties and responsibilities of the Director and the heads of other departments, agencies, elements, and entities engaged in intelligence activities to cooperate with the Congress in the conduct of its responsibilities for oversight of intelligence activities shall

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

be implemented in accordance with applicable law, including title V of the Act. The requirements of applicable law, including title V of the Act, shall apply to all covert action activities as defined in this Order.

3.2 *Implementation.* The President, supported by the NSC, and the Director shall issue such appropriate directives, procedures, and guidance as are necessary to implement this order. Heads of elements within the Intelligence Community shall issue appropriate procedures and supplementary directives consistent with this order. No procedures to implement Part 2 of this order shall be issued without the Attorney General's approval, after consultation with the Director. The Attorney General shall provide a statement of reasons for not approving any procedures established by the head of an element in the Intelligence Community (or the head of the department containing such element) other than the FBI. In instances where the element head or department head and the Attorney General are unable to reach agreements on other than constitutional or other legal grounds, the Attorney General, the head of department concerned, or the Director shall refer the matter to the NSC.

3.3 *Procedures.* The activities herein authorized that require procedures shall be conducted in accordance with existing procedures or requirements established under Executive Order 12333. New procedures, as required by Executive Order 12333, as further amended, shall be established as expeditiously as possible. All new procedures promulgated pursuant to Executive Order 12333, as amended, shall be made available to the Select Committee on Intelligence of the Senate and the Permanent Select Committee on Intelligence of the House of Representatives.

3.4 *References and Transition.* References to "Senior Officials of the Intelligence Community" or "SOICs" in executive orders or

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

other Presidential guidance, shall be deemed references to the heads of elements in the Intelligence Community, unless the President otherwise directs; references in Intelligence Community or Intelligence Community element policies or guidance, shall be deemed to be references to the heads of elements of the Intelligence Community, unless the President or the Director otherwise directs.

3.5 Definitions. For the purposes of this Order, the following terms shall have these meanings:

(a) Counterintelligence means information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations, or persons, or their agents, or international terrorist organizations or activities.

(b) Covert action means an activity or activities of the United States Government to influence political, economic, or military conditions abroad, where it is intended that the role of the United States Government will not be apparent or acknowledged publicly, but does not include:

(1) Activities the primary purpose of which is to acquire intelligence, traditional counterintelligence activities, traditional activities to improve or maintain the operational security of United States Government programs, or administrative activities;

(2) Traditional diplomatic or military activities or routine support to such activities;

(3) Traditional law enforcement activities conducted by United States Government law enforcement agencies or routine support to such activities; or

(4) Activities to provide routine support to the overt activities (other than activities described in

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

paragraph (1), (2), or (3) of other United States Government agencies abroad.

(c) *Electronic surveillance* means acquisition of a nonpublic communication by electronic means without the consent of a person who is a party to an electronic communication or, in the case of a non-electronic communication, without the consent of a person who is visibly present at the place of communication, but not including the use of radio direction-finding equipment solely to determine the location of a transmitter.

(d) *Employee* means a person employed by, assigned or detailed to, or acting for an element within the Intelligence Community.

(e) *Foreign intelligence* means information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, foreign persons, or international terrorists.

(f) *Intelligence* includes foreign intelligence and counterintelligence.

(g) *Intelligence activities* means all activities that elements of the Intelligence Community are authorized to conduct pursuant to this order.

(h) *Intelligence Community* and elements of the Intelligence Community refers to:

- (1) The Office of the Director of National Intelligence;
- (2) The Central Intelligence Agency;
- (3) The National Security Agency;
- (4) The Defense Intelligence Agency;
- (5) The National Geospatial-Intelligence Agency;
- (6) The National Reconnaissance Office;
- (7) The other offices within the Department

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

of Defense for the collection of specialized national foreign intelligence through reconnaissance programs;

(8) The intelligence and counterintelligence elements of the Army, the Navy, the Air Force, and the Marine Corps;

(9) The intelligence elements of the Federal Bureau of Investigation;

(10) The Office of National Security Intelligence of the Drug Enforcement Administration;

(11) The Office of Intelligence and Counterintelligence of the Department of Energy;

(12) The Bureau of Intelligence and Research of the Department of State;

(13) The Office of Intelligence and Analysis of the Department of the Treasury;

(14) The Office of Intelligence and Analysis of the Department of Homeland Security;

(15) The intelligence and counterintelligence elements of the Coast Guard; and

(16) Such other elements of any department or agency as may be designated by the President, or designated jointly by the Director and the head of the department or agency concerned, as an element of the Intelligence Community.

(i) *National Intelligence and Intelligence Related to National Security* means all intelligence, regardless of the source from which derived and including information gathered within or outside the United States, that pertains, as determined consistent with any guidance issued by the President, or that is determined for the purpose of access to information by the Director in accordance with section 1.3(a)(1) of this order, to pertain to more than one United States Government agency; and that involves threats to the United States, its

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

people, property, or interests; the development, proliferation, or use of weapons of mass destruction; or any other matter bearing on United States national or homeland security.

(j) *The National Intelligence Program* means all programs, projects, and activities of the Intelligence Community, as well as any other programs of the Intelligence Community designated jointly by the Director and the head of a United States department or agency or by the President. Such term does not include programs, projects, or activities of the military departments to acquire intelligence solely for the planning and conduct of tactical military operations by United States Armed Forces.

(k) *United States person* means a United States citizen, an alien known by the intelligence element concerned to be a permanent resident alien, an unincorporated association substantially composed of United States citizens or permanent resident aliens, or a corporation incorporated in the United States, except for a corporation directed and controlled by a foreign government or governments.

3.6 Revocation. Executive Orders 13354 and 13355 of August 27, 2004, are revoked; and paragraphs 1.3(b)(9) and (10) of Part 1 supersede provisions within Executive Order 12958, as amended, to the extent such provisions in Executive Order 12958, as amended, are inconsistent with this Order.

3.7 General Provisions.

(a) Consistent with section 1.3(c) of this order, nothing in this order shall be construed to impair or otherwise affect:

- (1) Authority granted by law to a department or agency, or the head thereof; or
- (2) Functions of the Director of the Office of Management and Budget relating to budget, administrative, or legislative proposals.

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

(b) This order shall be implemented consistent with applicable law and subject to the availability of appropriations.

(c) This order is intended only to improve the internal management of the executive branch and is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity, by any party against the United States, its departments, agencies or entities, its officers, employees, or agents, or any other person.

/s/ Ronald Reagan

THE WHITE HOUSE

December 4, 1981

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

This Page is Intentionally Blank

UNCLASSIFIED - ~~FOR OFFICIAL USE ONLY~~

UNCLASSIFIED – ~~FOR OFFICIAL USE ONLY~~
Domestic Investigations and Operations Guide

C APPENDIX C: (U//FOUO) USE AND TARGETING OF A FEDERAL PRISONER HELD IN THE CUSTODY OF THE BOP OR USMS DURING AN FBI PREDICATED INVESTIGATION; INTERVIEW OF A FEDERAL PRISONER HELD IN THE CUSTODY OF THE BOP OR USMS DURING AN FBI ASSESSMENT OR PREDICATED INVESTIGATION

C.1 (U) OVERVIEW/SUMMARY

(U//~~FOUO~~) **Use and Targeting a Federal Prisoner:** During an FBI Predicated Investigation, it may be necessary and appropriate to: 1) use a cooperating federal prisoner to gather and obtain evidence and intelligence; or 2) target a federal prisoner. This policy sets forth the approval process for the use of and targeting of a federal prisoner held in the custody of the Bureau of Prisons (BOP) or the United States Marshals Service (USMS).

(U//~~FOUO~~) **Interview a Federal Prisoner:** During an FBI Assessment or Predicated Investigation, it may be necessary and appropriate to interview a federal prisoner in the custody of the BOP or USMS. This policy sets forth the approval process for the interview of a federal prisoner held in the custody of the BOP or the USMS during an FBI Assessment or Predicated Investigation.

(U//~~FOUO~~) **Exclusions from this Policy:** This policy does not apply to:

- A) (U//FOUO) [REDACTED]

b7E

C.2 (U) LEGAL AUTHORITY

(U) The FBI is authorized by the Department of Justice (DOJ) to use and target a federal prisoner for investigative purposes and interview a Federal Prisoner (DOJ Memorandum “Use and Targeting of Federal Prisoners in Investigations,” January 22, 2009).

C.3 (U) DEFINITIONS

(U) **Federal Prisoner:** For purposes within this section, a federal prisoner is one who is held in the custody of either the BOP or the USMS pursuant to an order of a court in connection with a criminal matter, regardless of where the person is housed.

(U) **Use of a Federal Prisoner:** Use of a federal prisoner means to employ a federal prisoner during an investigation in such a manner that the prisoner will interact with others who are not members of law enforcement (e.g., the prisoner will engage in a consensually monitored telephone call with a target) or the prisoner will be taken out of the custody of BOP or USMS (e.g., the prisoner is removed from the prison to assist the FBI in locating a hide-out) or law enforcement will interact covertly with the prisoner (e.g., an undercover agent engages with the prisoner in the visiting room of the prison).

(U) **Targeting a Federal Prisoner:** “Targeting” a federal prisoner means that the federal prisoner is the target of the investigation and that investigative activity will directly interact with either the prisoner or the federal facility (e.g., as part of a money laundering investigation targeting a prisoner, the FBI wishes to engage in a consensually monitored conversation with the prisoner).

(U) **Interview of a Federal Prisoner:** Interview of a federal prisoner means to interact with a federal prisoner, overtly representing oneself as an FBI employee, in order to gather information.

C.3.1 (U) *USE AND TARGETING A FEDERAL PRISONER*

(U//~~FOUO~~) An FBI employee may request the use of or the targeting of a federal prisoner in an FBI Predicated Investigation [REDACTED]

b7E

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

b7E

C.3.2 (U) *INTERVIEW A FEDERAL PRISONER*

(U//~~FOUO~~) An FBI employee may request to interview a federal prisoner in an FBI Assessment or Predicated Investigation [REDACTED]

b7E

C.4 (U) *APPROVAL REQUIREMENTS*

C.4.1 (U) *APPROVAL - USE AND TARGETING OF A FEDERAL PRISONER*

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

b7E

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

b7E

[REDACTED] The process is as follows:

A) (U//~~FOUO~~) The FBI field office employee must:

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

b7E

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

b7E

3) (U//~~FOUO~~) [REDACTED]

b7E

4) (U//~~FOUO~~) [REDACTED]

b7E

UNCLASSIFIED – ~~FOR OFFICIAL USE ONLY~~
Domestic Investigations and Operations Guide

5) (U//~~FOUO~~) [REDACTED] b7E

6) (U//~~FOUO~~) [REDACTED] b7E

B) (U//~~FOUO~~) [REDACTED] b7E

1) (U//~~FOUO~~) [REDACTED] b7E

2) (U//~~FOUO~~) [REDACTED] b7E

3) (U//~~FOUO~~) [REDACTED] b7E

4) (U//~~FOUO~~) [REDACTED] b7E

(U//~~FOUO~~) Note: [REDACTED] b7E

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

[REDACTED] b7E

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

[REDACTED]

(U//~~FOUO~~) Note: The DOJ Memorandum governing the Use and Targeting of Federal Prisoners is labeled “Sensitive Investigative Matter.” This is not a SIM as defined in DIOG Section 10. [REDACTED] b7E

C.4.2 (U) APPROVAL - INTERVIEW A FEDERAL PRISONER

(U//~~FOUO~~) The FBI employee must:

A) (U//~~FOUO~~) [REDACTED] b7E

B) (U//~~FOUO~~) [REDACTED] b7E

C) (U//~~FOUO~~) [REDACTED] b7E

C.5 (U) EXEMPTIONS TO DOJ APPROVAL REQUIREMENT

(U//~~FOUO~~)

b7E

A)

(U//~~FOUO~~)

b7E

B)

(U//~~FOUO~~)

b7E

1) (U//~~FOUO~~)

b7E

2) (U//~~FOUO~~)

b7E

3) (U//~~FOUO~~)

b7E

4) (U//~~FOUO~~)

b7E

C)

(U//~~FOUO~~)

b7E

D)

(U//~~FOUO~~)

b7E

(U)

b7E

(U//~~FOUO~~)

b7E

A)

(U//~~FOUO~~)

b7E

B)

(U//~~FOUO~~)

b7E

C)

(U//~~FOUO~~)

b7E

D)

(U//~~FOUO~~)

b7E

C.6 (U) EXTENSION REQUESTS

(U//~~FOUO~~) Agents may request extensions of the authority to use or target a prisoner in an FBI investigation

b7E

A)

(U//~~FOUO~~)

b7E

B)

(U//~~FOUO~~)

b7E

UNCLASSIFIED – ~~FOR OFFICIAL USE ONLY~~
Domestic Investigations and Operations Guide

- C) (U//~~FOUO~~) [REDACTED] b7E
- D) (U//~~FOUO~~) [REDACTED] b7E
- E) (U//~~FOUO~~) [REDACTED] b7E

C.7 (U) TRANSPORTATION OF FEDERAL PRISONER

(U//~~FOUO~~) If it is necessary to remove the federal prisoner from the detention facility in which he/she is housed as a part of the investigation [REDACTED] b7E

[REDACTED]

- A) (U//~~FOUO~~) [REDACTED] b7E
- [REDACTED]
- B) (U//~~FOUO~~) [REDACTED] b7E
- C) (U//~~FOUO~~) [REDACTED] b7E
- D) (U//~~FOUO~~) [REDACTED] b7E
- [REDACTED]
- E) (U//~~FOUO~~) [REDACTED] b7E
- F) (U//~~FOUO~~) [REDACTED] b7E
- [REDACTED]
- G) (U//~~FOUO~~) [REDACTED] b7E
- [REDACTED]
- H) (U//~~FOUO~~) [REDACTED] b7E

This Page is Intentionally Blank

UNCLASSIFIED – ~~FOR OFFICIAL USE ONLY~~
Domestic Investigations and Operations Guide

**D APPENDIX D: (U) DEPARTMENT OF JUSTICE
MEMORANDUM ON COMMUNICATIONS WITH THE
WHITE HOUSE AND CONGRESS, DATED MAY 11, 2009**

UNCLASSIFIED ~~—FOR OFFICIAL USE ONLY—~~
Domestic Investigations and Operations Guide

ALL FBI INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 05-08-2018 BY NSICG

b6
b7C



Office of the Attorney General
Washington, D. C. 20530

May 11, 2009

MEMORANDUM FOR HEADS OF DEPARTMENT COMPONENTS
ALL UNITED STATES ATTORNEYS

FROM:

A handwritten signature in dark ink, appearing to be "E. J. [unclear]", written over the printed name of the Attorney General.

THE ATTORNEY GENERAL

SUBJECT:

Communications with the White House and Congress

The rule of law depends upon the evenhanded administration of justice. The legal judgments of the Department of Justice must be impartial and insulated from political influence. It is imperative that the Department's investigatory and prosecutorial powers be exercised free from partisan consideration. It is a fundamental duty of every employee of the Department to ensure that these principles are upheld in all of the Department's legal endeavors.

In order to promote the rule of law, therefore, this memorandum sets out guidelines to govern all communications between representatives of the Department, on the one hand, and representatives of the White House and Congress, on the other, and procedures intended to implement those guidelines. (The "White House," for the purposes of this Memorandum, means all components within the Executive Office of the President.) These guidelines have been developed in consultation with, and have the full support of, the Counsel to the President.

1. Pending or Contemplated Criminal or Civil Investigations and Cases

The Assistant Attorneys General, the United States Attorneys, and the heads of the investigative agencies in the Department have the primary responsibility to initiate and supervise investigations and cases. These officials, like their superiors and their subordinates, must be insulated from influences that should not affect decisions in particular criminal or civil cases. As the Supreme Court said long ago with respect to United States Attorneys, so it is true of all those who exercise the Department's investigatory and prosecutorial powers: they are representatives "not of an ordinary party to a controversy, but of a sovereignty whose obligation to govern impartially is as compelling as its obligation to govern at all; and whose interest, therefore, in a criminal prosecution is not that it shall win a case, but that justice shall be done." *Berger v. United States*, 295 U.S. 78, 88 (1935).

a. In order to ensure the President's ability to perform his constitutional obligation to "take care that the laws be faithfully executed," the Justice Department will advise the White House concerning pending or contemplated criminal or civil investigations or cases when—but only when—it is important for the performance of the President's duties and appropriate from a law enforcement perspective.

UNCLASSIFIED – ~~FOR OFFICIAL USE ONLY~~
Domestic Investigations and Operations Guide

Memorandum for Head of Department Components
All United States Attorneys
Subject: Communications with the White House and Congress

Page 2

b. Initial communications between the Department and the White House concerning pending or contemplated criminal investigations or cases will involve only the Attorney General or the Deputy Attorney General, from the side of the Department, and the Counsel to the President, the Principal Deputy Counsel to the President, the President or the Vice President, from the side of the White House. If the communications concern a pending or contemplated civil investigation or case, the Associate Attorney General may also be involved. If continuing contact between the Department and the White House on a particular matter is required, the officials who participated in the initial communication may designate subordinates from each side to carry on such contact. The designating officials must monitor subsequent contacts, and the designated subordinates must keep their superiors regularly informed of any such contacts. Communications about Justice Department personnel in reference to their handling of specific criminal or civil investigations or cases are expressly included within the requirements of this paragraph. This policy does not, however, prevent officials in the communications, public affairs, or press offices of the White House and the Department of Justice from communicating with each other to coordinate efforts.

c. In order to ensure that Congress may carry out its legitimate investigatory and oversight functions, the Department will respond as appropriate to inquiries from Congressional Committees consistent with policies, laws, regulations, or professional ethical obligations that may require confidentiality and consistent with the need to avoid publicity that may undermine a particular investigation or litigation. Outside the context of Congressional hearings or investigations, all inquiries from individual Senators and Members of Congress or their staffs concerning particular contemplated or pending criminal investigations or cases should be directed to the Attorney General or the Deputy Attorney General. In the case of particular civil investigations or cases, inquiries may also be directed to the Associate Attorney General.

d. These procedures are not intended to interfere with the normal communications between the Department and its client departments and agencies (including agencies within the Executive Office of the President when they are the Department's clients) and any meetings or communications necessary to the proper conduct of an investigation or litigation.

2. National Security Matters

It is critically important to have frequent and expeditious communications relating to national security matters, including counter-terrorism and counter-espionage issues. Therefore communications from (or to) the Deputy Counsel to the President for National Security Affairs, the staff of the National Security Council and the staff of the Homeland Security Council that relate to a national security matter are not subject to the limitations set out above. However, this exception for national security matters does not extend to pending adversary cases in litigation that may have national security implications. Communications related to such cases are subject to the guidelines for pending cases described above.

UNCLASSIFIED – ~~FOR OFFICIAL USE ONLY~~
Domestic Investigations and Operations Guide

Memorandum for Head of Department Components
All United States Attorneys
Subject: Communications with the White House and Congress

Page 3

3. White House Requests for Legal Advice

All requests from the White House for formal legal opinions shall come from the President, the Counsel to the President, or one of the Deputy Counsels to the President, and shall be directed to the Attorney General and the Assistant Attorney General for the Office of Legal Counsel. The Assistant Attorney General for the Office of Legal Counsel shall report to the Attorney General and the Deputy Attorney General any communications that, in his or her view, constitute improper attempts to influence the Office of Legal Counsel's legal judgment.

4. Communications Involving the Solicitor General's Office.

Matters in which the Solicitor General's Office is involved often raise questions about which contact with the Office of the Counsel to the President is appropriate. Accordingly, the Attorney General and Deputy Attorney General may establish distinctive arrangements with the Office of the Counsel to govern such contacts.

5. Presidential Pardon Matters

The Office of the Pardon Attorney may communicate directly with the Counsel to the President and the Deputy Counsels to the President, concerning pardon matters. The Counsel to the President and the Deputy Counsels to the President may designate subordinates to carry on contact with the Office of the Pardon Attorney after the initial contact is made.

6. Personnel Decisions Concerning Positions in the Civil Service

All personnel decisions regarding career positions in the Department must be made without regard to the applicant's or occupant's partisan affiliation. Thus, while the Department regularly receives communications from the White House and from Senators, Members of Congress, and their staffs concerning political appointments, such communications regarding positions in the career service are not proper when they concern a job applicant's or a job holder's partisan affiliation. Efforts to influence personnel decisions concerning career positions on partisan grounds should be reported to the Deputy Attorney General.

7. Other Communications Not Relating to Pending Investigations or Criminal or Civil Cases

All communications between the Department and the White House or Congress that are limited to policy, legislation, budgeting, political appointments, public affairs, intergovernmental relations, or administrative matters that do not relate to a particular contemplated or pending investigation or case may be handled directly by the parties concerned. Such communications should take place with the knowledge of the Department's lead contact regarding the subject

UNCLASSIFIED – ~~FOR OFFICIAL USE ONLY~~
Domestic Investigations and Operations Guide

Memorandum for Head of Department Components
All United States Attorneys
Subject: Communications with the White House and Congress

Page 4

under discussion. In the case of communications with Congress, the Office of the Deputy Attorney General and Office of the Assistant Attorney General for Legislative Affairs should be kept informed of all communications concerning legislation and the Office of the Associate Attorney General should be kept informed about important policy communications in its areas of responsibility.

As Attorney General Benjamin Civiletti noted in issuing a similar memorandum during the Carter Administration, these guidelines and procedures are not intended to wall off the Department from legitimate communication. We welcome criticism and advice. What these procedures are intended to do is route communications to the proper officials so they can be adequately reviewed and considered, free from either the reality or the appearance of improper influence.

Decisions to initiate investigations and enforcement actions are frequently discretionary. That discretion must be exercised to the extent humanly possible without regard to partisanship or the social, political, or interest group position of either the individuals involved in the particular cases or those who may seek to intervene against them or on their behalf.

This memorandum supersedes the memorandum issued by Attorney General Mukasey on December 19, 2007, titled *Communications with the White House*.

This Page is Intentionally Blank

**E APPENDIX E: (U//~~FOUO~~) ATTORNEY GENERAL
MEMORANDUM – REVISED POLICY ON THE USE OR
DISCLOSURE OF FISA INFORMATION, DATED
JANUARY 10, 2008**

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 05-08-2018 BY NSICG

b6
b7C

UNCLASSIFIED – ~~FOR OFFICIAL USE ONLY~~

Domestic Investigations and Operations Guide

ALL FBI INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 05-08-2018 BY [redacted] NSICG

b6
b7C

~~FOR OFFICIAL USE ONLY~~



U.S. Department of Justice

National Security Division

Office of the Assistant Attorney General

Washington, D.C. 20530

January 10, 2008

TO: All United States Attorneys
All National Security Division Attorneys
All Anti-Terrorism Coordinators

CC: Assistant Attorney General, Criminal Division
Assistant Attorney General, Civil Division
Director, Federal Bureau of Investigation

FROM: Kenneth L. Wainstein *KLW*
Assistant Attorney General for National Security

SUBJECT: Revised FISA Use Policy as Approved by the Attorney General

We are pleased to provide the Department of Justice's revised policy on the use or disclosure of information obtained or derived from collections under the Foreign Intelligence Surveillance Act of 1978 (FISA), as approved by the Attorney General today. Also attached is a form for use with respect to notifications that are required under Section I of the revised policy.

This revised policy includes significant changes from current practice that will streamline the process for using FISA information in certain basic investigative processes, while still ensuring that important intelligence and law enforcement interests are protected.

You will note that the revised policy authorizes the use or disclosure of FISA information, under the specific circumstances described in the policy, with notification to NSD and after consultation with the FBI (or other Intelligence Community agencies) for the following investigative processes:

•



b7E

~~FOR OFFICIAL USE ONLY~~

UNCLASSIFIED – ~~FOR OFFICIAL USE ONLY~~
Domestic Investigations and Operations Guide

~~FOR OFFICIAL USE ONLY~~

-
-
-

b7E

b7E

b7E

As described in the revised policy, the Department continues to require prior authorization from the Assistant Attorney General for National Security (AAG/NSD) for the use or disclosure of FISA information in order to file criminal charges or in post-charge criminal proceedings, as well as in connection with certain investigative processes (*e.g.*, criminal search warrants under Rule 41 of the Federal Rules of Criminal Procedure). The revised policy also requires the prior authorization of the AAG/NSD or his designee for the use or disclosure of FISA information in non-criminal proceedings.

The revised policy was drafted by a Justice Department working group that included representatives from the Attorney General's Advisory Committee of United States Attorneys (AGAC), National Security Division (NSD), Federal Bureau of Investigation (FBI), and Office of Legal Policy (OLP). The working group also consulted with the Office of the Director of National Intelligence (ODNI) in the course of the development of this policy.

The revised policy requires that it be reviewed one year from its effective date and requires NSD to issue guidance on what constitutes information "derived from" FISA collections by March 31, 2008.

As noted in the policy, prosecutors are encouraged to contact the National Security Division at any time in order to obtain guidance regarding this policy and to expedite resolution of any issues.

~~FOR OFFICIAL USE ONLY~~

~~UNCLASSIFIED – FOR OFFICIAL USE ONLY~~
Domestic Investigations and Operations Guide

ALL FBI INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 05-08-2018 BY NSICG

~~FOR OFFICIAL USE ONLY~~

b6
b7C



U.S. Department of Justice

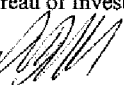
Office of the Attorney General

Washington, D.C. 20530

January 10, 2008

TO: All Federal Prosecutors

CC: Assistant Attorney General, National Security Division
Assistant Attorney General, Criminal Division
Assistant Attorney General, Civil Division
Director, Federal Bureau of Investigation

FROM: Michael B. Mukasey 
Attorney General

SUBJECT: Revised Policy on the Use or Disclosure of FISA Information

As a general matter, it is the policy of the Department of Justice to use all lawful processes in the investigation and prosecution of cases involving terrorism, intelligence, and national security, and to undertake all efforts necessary to protect the American people from the threat posed by foreign powers and their agents, while also exercising due regard for the protection of intelligence sources, methods, and collections, and the privacy and civil liberties of United States persons.

There are important purposes to be served by consultation and coordination with respect to the use or disclosure of FISA information¹ in investigations, criminal prosecutions, and other proceedings. First, because FISA information is almost always classified, the use or disclosure of such information will normally require declassification by the originating agency in accordance with the originating agency's policies and procedures. Second, the use of such information could directly or indirectly compromise intelligence sources, methods, or collections, or disclose the existence or nature of or otherwise compromise an investigation. Third, FISA requires the Government to notify the court and an "aggrieved person" of its intent

¹ The term "FISA information," as used in this policy, means any information acquired, obtained, or derived from collection authorized pursuant to FISA. Whether specific information qualifies as "derived from" FISA collection may be a fact-bound question that depends, at least in part, on the attenuation of the information to be used from the original FISA acquired or obtained information and whether the information was also obtained from an independent source, as well as other factors. Where such a question arises, the application of this policy should be discussed among the USAO, FBI, and NSD, and if consensus is not reached, a determination will be made by the Assistant Attorney General for National Security. Separate guidance regarding what constitutes information "derived from" FISA collection will be issued by the National Security Division no later than March 31, 2008.

~~FOR OFFICIAL USE ONLY~~

~~UNCLASSIFIED – FOR OFFICIAL USE ONLY~~
Domestic Investigations and Operations Guide

~~FOR OFFICIAL USE ONLY~~

to use or disclose any FISA information before it is used against such person in a broad range of proceedings. Fourth, the Government is required to ensure that complete and accurate filings are made with the Foreign Intelligence Surveillance Court (FISC), and that the Government complies with all of FISA's statutory requirements. Fifth, it is important to ensure that litigation risks, if any, are properly assessed. Finally, in certain cases, it may be appropriate to make disclosures to a United States District Court regarding classified facts before legal process is obtained.

Given these purposes, it is essential that coordination take place in connection with the use or disclosure of FISA information. Such coordination should be streamlined in order to promote efficient, nimble, and useful investigative activities. The risk of compromising the purposes described above varies depending on the stage of the investigation, criminal prosecution, or other proceeding. As a general matter, [REDACTED]

b7E

[REDACTED] federal prosecutors should consider alternative approaches for taking action.

Prosecutors are encouraged to contact the National Security Division at any time in order to obtain guidance regarding this policy and to expedite resolution of any issues.

The following policy is therefore adopted and supersedes any existing Attorney General policies with respect to the use and disclosure of FISA information to the extent that they are inconsistent with this policy:

- (a) the Assistant Attorney General for National Security may act as the Attorney General, as provided for under FISA, *see* 50 U.S.C. § 1801(g), for the purpose of authorizing the use or disclosure of FISA information pursuant to this policy;² and
- (b) federal prosecutors and all others who may seek to use or disclose FISA information in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States, in coordination with NSD and FBI, are authorized to do so pursuant to the terms of this policy, shall coordinate with NSD [REDACTED] and shall comply with the following procedures in matters that involve the use or disclosure of FISA information:³

b7E

² Such authorization may also be provided by the Attorney General, Acting Attorney General, and the Deputy Attorney General. *See* 50 U.S.C. § 1801(g).

³ Nothing in this policy is intended to supersede or replace existing policies for prosecutors regarding notification, consultation, and approval for certain investigative and prosecutive steps, including consultation with other districts where related matters may be under investigation. For example, the United States Attorneys' Manual sets forth when a prosecutor must obtain prior approval for various court actions in national security prosecutions. *See, e.g.,* United States Attorneys' Manual (USAM) §§ 9-2.131 ("Matters Assumed by Criminal Division or Higher

~~FOR OFFICIAL USE ONLY~~

UNCLASSIFIED ~~FOR OFFICIAL USE ONLY~~
Domestic Investigations and Operations Guide

~~FOR OFFICIAL USE ONLY~~

I. Use or Disclosure of FISA Information Requiring Consultation with FBI or other Intelligence Community Agencies and Notification to NSD

- A. Certain investigative processes present only moderate risks. As a result, where FISA information is used or disclosed in connection with the processes described below, consultation with FBI (or other Intelligence Community agencies, as appropriate)⁴ and notice to NSD is required:

1.

[Redacted]

b7E

2.

[Redacted]

b7E

3.

[Redacted]

b7E

4.

[Redacted]

b7E

- B. Where FISA information is used or disclosed in connection with the processes described above, the following notification process shall be followed:

1.

[Redacted]

b7E

Authority"); 9-2.136 ("Investigative and Prosecutive Policy for International Terrorism Matters"); 9-2.155 ("Sensitive Matters"); 9-2.400 ("Prior Approvals Chart").

⁴ For the purposes of this document, the term "Intelligence Community agencies" refers to the appropriate agencies within the Intelligence Community, including the Office of the Director of National Intelligence. Consultation with Intelligence Community agencies other than the FBI is typically appropriate when the sources, methods, or collections involve Intelligence Community agencies other than the FBI. Prosecutors are encouraged to contact the National Security Division, as needed, to assist with the consultation process with the FBI or other Intelligence Community agencies.

⁵ Some courts require a significant measure of information with respect to [Redacted] to the extent that applications in such districts require the disclosure of additional FISA information beyond the disclosure of [Redacted] advance authorization as provided for in Section II of this policy is required prior to such applications being made to the court.

b7E

~~FOR OFFICIAL USE ONLY~~

UNCLASSIFIED – ~~FOR OFFICIAL USE ONLY~~
Domestic Investigations and Operations Guide

~~FOR OFFICIAL USE ONLY~~

2. As provided on the attached draft [redacted] the federal prosecutor must indicate that he or she has [redacted]

b7E

3. [redacted]
above—to ensure that NSD complies with potential obligations to notify the Foreign Intelligence Surveillance Court.

b7E

- C. Where consultations with the FBI (or other Intelligence Community agencies, as appropriate) demonstrate that [redacted]

b7E

[redacted]
further consultation that includes NSD (working with Intelligence Community agencies, as appropriate) shall take place prior to the use of such processes.

1. [redacted]

b7E

- D. This section does not permit the use or disclosure of FISA information obtained [redacted]

b7E

[redacted] Federal prosecutors must seek specific, separate use authority from the Assistant Attorney General for National Security prior to initiating any criminal proceedings.

II. Use or Disclosure of FISA Information Requiring the Advance Authorization of the Assistant Attorney General for National Security

- A. The advance authorization of the Assistant Attorney General for National Security is required where FISA information is [redacted]

b7E

[redacted]

b7E

~~FOR OFFICIAL USE ONLY~~

UNCLASSIFIED – ~~FOR OFFICIAL USE ONLY~~
Domestic Investigations and Operations Guide

~~FOR OFFICIAL USE ONLY~~

1. *Investigative Processes Requiring Advance Authorization*

- a. [REDACTED] As a result, authorization of the Assistant Attorney General for National Security is required before FISA information is used or disclosed in connection with the processes described below:

b7E

i. [REDACTED]

b7E

ii. [REDACTED] Title 18, Chapter 119, United States Code;

b7E

iii. [REDACTED] Title 18, Chapter 121, United States Code;

b7E

iv. [REDACTED] Rule 41 of the Federal Rules of Criminal Procedure;

b7E

v. [REDACTED] 18 U.S.C. § 3144;

b7E

vi. [REDACTED]

b7E

vii. [REDACTED]

b7E

2. *Criminal Indictments and Post-Indictment Proceedings*

- a. The use or disclosure of FISA information [REDACTED] As a result, the advance authorization of the Assistant Attorney General for National Security is required before such use or disclosure.

b7E

- b. This advance authorization requirement applies to [REDACTED]

b7E

[REDACTED]

~~FOR OFFICIAL USE ONLY~~

UNCLASSIFIED – ~~FOR OFFICIAL USE ONLY~~
Domestic Investigations and Operations Guide

~~FOR OFFICIAL USE ONLY~~

3. Among the factors that will be considered with respect to granting use authority are: [REDACTED]

b7E

4. Because the process of obtaining advance authorization will require NSD to coordinate with Intelligence Community agencies, federal prosecutors should seek such advance authorization at the earliest juncture possible. In addition, because the use of such information will normally require

b7E

- a. Prosecutors are encouraged to contact NSD at any time in order to obtain guidance regarding this policy and to expedite resolution of any issues.
- b. Where advance authorization involving [REDACTED] [REDACTED] NSD shall provide notice of such request to ODNI.

b7E

III. Use or Disclosure of FISA Information In Non-Criminal Proceedings

- A. [REDACTED] Therefore, authorization of the Assistant Attorney General for National Security or his designee is required before such use or disclosure.

b7E

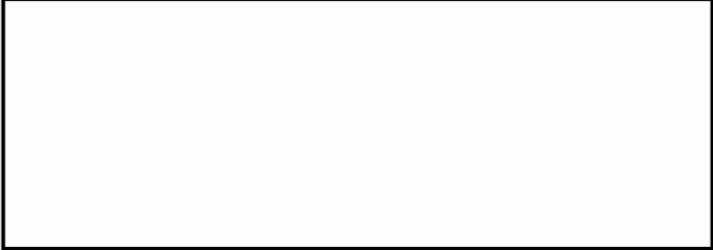
1. [REDACTED]

b7E

~~FOR OFFICIAL USE ONLY~~

UNCLASSIFIED – ~~FOR OFFICIAL USE ONLY~~
Domestic Investigations and Operations Guide

~~FOR OFFICIAL USE ONLY~~

2. Among the factors that will be considered with respect to granting use authority are: 

 3. Because the process of obtaining advance authorization will require NSD to coordinate with Intelligence Community agencies, the attorney for the government should seek such advance authorization at the earliest juncture possible. In addition, because the use of such information will normally require 

 - a. Prosecutors are encouraged to contact NSD at any time in order to obtain guidance regarding this policy and to expedite resolution of any issues.
 - b. Where advance authorization involving particularly sensitive sources, methods, or collections is requested, NSD shall provide notice of such request to ODNI.
- This policy shall be reviewed one year from its effective date to evaluate its effectiveness.

b7E

b7E

~~FOR OFFICIAL USE ONLY~~

UNCLASSIFIED – ~~FOR OFFICIAL USE ONLY~~
Domestic Investigations and Operations Guide

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 05-08-2018 BY NSICG

b6
b7C

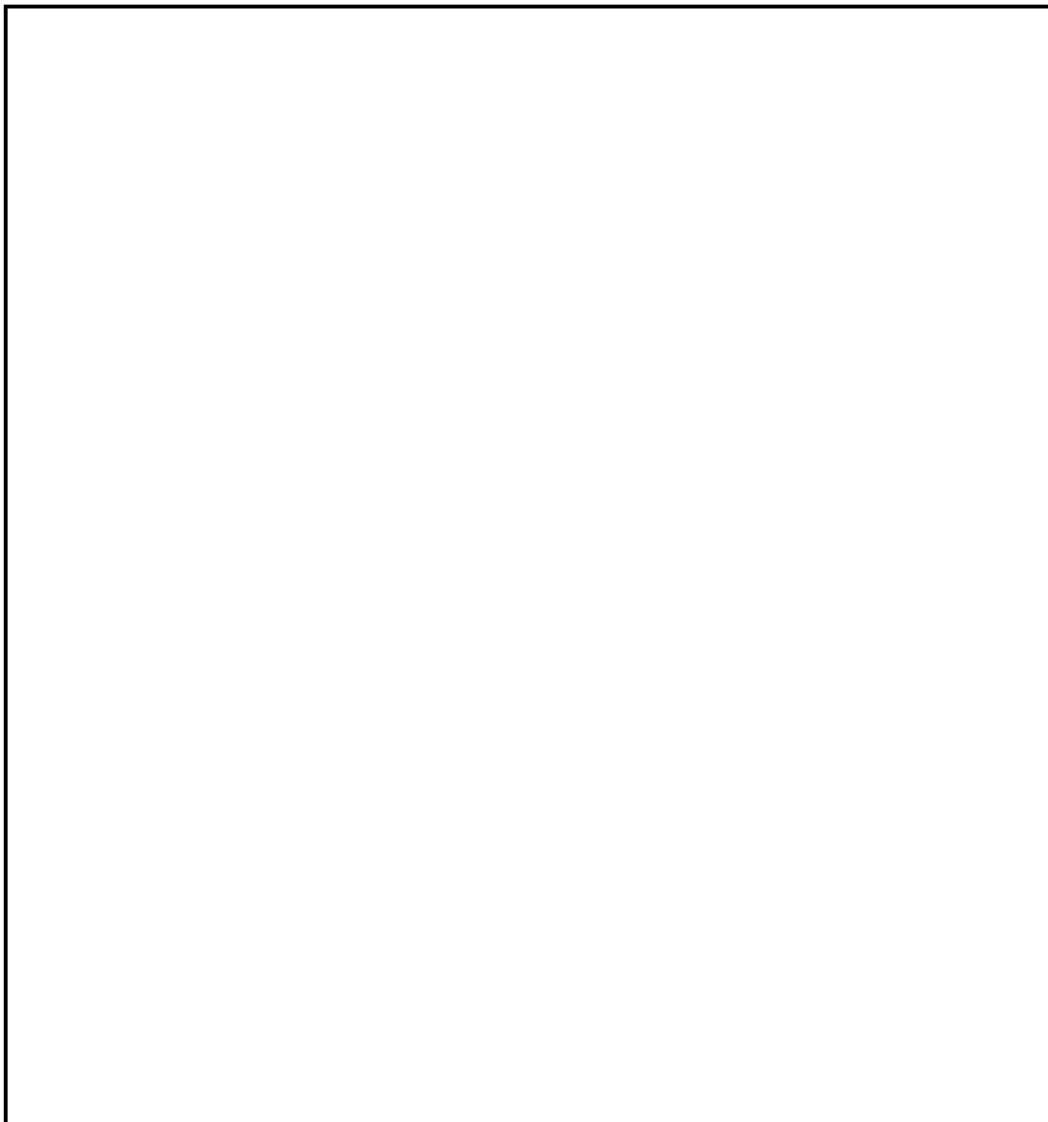
Classification:

NOTIFICATION OF USE OR DISCLOSURE OF FISA INFORMATION FORM

b7E

Classification:

Classification:



b7E

Classification:

This Page is Intentionally Blank

UNCLASSIFIED – ~~FOR OFFICIAL USE ONLY~~
Domestic Investigations and Operations Guide

F APPENDIX F: (U) DOJ POLICY ON USE OF FORCE

F.1 (U) USE OF LESS-THAN-LETHAL DEVICES

(U) Deputy Attorney General's Memorandum on Use of Less-than-Lethal Devices dated 4/21/2011.

F.2 (U) USE OF DEADLY FORCE

(U) Deadly Force Policy, dated 7/1/2004.

F.3 (U) TRAINING

A) (U) Deadly Force Policy Training Material, dated 7/29/2004.

B) (U) Instructional Outline and Use of Force Scenarios

F.1 (U) USE OF LESS-THAN-LETHAL DEVICES

(U) Deputy Attorney General's Memorandum on Use of Less-than-Lethal Devices dated 4/21/2011.

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

ALL FBI INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 05-08-2018 BY [REDACTED] NSICG



U.S. Department of Justice
Office of the Deputy Attorney General

b6
b7C

The Deputy Attorney General

Memorandum, DOJ, 2011

May 16, 2011

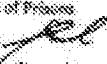
MEMORANDUM FOR: Robert S. Mueller III
Director
Federal Bureau of Investigation

Michele M. Leonhart
Administrator
Drug Enforcement Administration

Kenneth E. Melson
Acting Director
Bureau of Alcohol, Tobacco, Firearms and Explosives

Stacia A. Hyton
Director
United States Marshals Service

Thomas R. Kane
Acting Director
Federal Bureau of Prisons

FROM: James M. Cole 
Deputy Attorney General

SUBJECT: Policy on the Use of Less-Than-Lethal Devices

Attached is the Department's Policy on the Use of Less-Than-Lethal Devices, approved by the Attorney General on April 21, 2011. Please ensure that the policy is distributed to every affected employee within your component.

Attachment

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

ALL INFORMATION CONTAINED

HEREIN IS UNCLASSIFIED

DATE 05-08-2018 BY NSICG

b6
b7C

DEPARTMENT OF JUSTICE POLICY STATEMENT
ON THE USE OF LESS-THAN-LETHAL DEVICES

- I. Department of Justice (DOJ) law enforcement officers (officers) are authorized to use less-than-lethal devices only as consistent with this policy statement.
- II. Pursuant to this policy statement, less-than-lethal devices:
 - A. Are synonymous with "less lethal," "non-lethal," "non-lethally," and other terms referring to devices used in situations covered by this policy statement; and
 - B. Include, but are not limited to:
 1. Impact Devices (e.g., batons, bean bag projectiles, baton launcher, rubber projectiles, stingballs);
 2. Chemical Agents (e.g., tear gas, pepper spray, pepperballs); and
 3. Conducted Energy Devices (e.g., electronic immobilization, control, and restraint devices).
- III. DOJ officers are authorized to use less-than-lethal devices only in those situations where reasonable force, based on the totality of the circumstances at the time of the incident, is necessary to effectuate an arrest, obtain lawful compliance from a subject, or protect any person from physical harm. Use of less-than-lethal devices must cease when it is no longer necessary to achieve the law enforcement objective.
- IV. DOJ officers are authorized to use only those less-than-lethal devices authorized by their component and that they are trained to use, absent exigent circumstances.
- V. DOJ officers are not authorized to use less-than-lethal devices if voice commands or physical control achieve the law enforcement objective. DOJ officers are prohibited from using less-than-lethal devices to punish, harass, or abuse any person.
- VI. Less-than-lethal devices are used with a reasonable expectation that death or serious bodily injury will not

-3-

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

result. They are, however, recognized as having the potential to cause death or serious bodily injury, and DOJ officers may use less-than-lethal devices as deadly weapons only when authorized under the DOJ Policy Statement on the Use of Deadly Force.

- VII. DOJ officers must make necessary medical assistance available to subjects of less-than-lethal device use as soon as practicable.
- VIII. DOJ components must establish rules and procedures implementing this policy statement. Each component will ensure that state/local officers participating in joint task force operations are aware of and adhere to the policy and its limits on DOJ officers.
- IX. DOJ components must establish training programs and procedures for using less-than-lethal devices that are consistent with this policy statement and Federal law.
- X. DOJ components must individually establish procedures for documenting, reporting, reviewing, and investigating (as warranted). All incidents involving the use of less-than-lethal devices.
- XI. This policy statement is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity, against the United States, its departments, agencies, or other entities, its officers or employees, or any other person.

F.2 (U) USE OF DEADLY FORCE

(U) Deadly Force Policy, dated 7/1/2004.

Domestic Investigations and Operations Guide

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 05-08-2018 BY NSICC

b6
b7C

POLICY STATEMENT USE OF DEADLY FORCE
Approved by the Attorney General July 1, 2004

GENERAL PRINCIPLES

- I. Law enforcement officers and correctional officers of the Department of Justice may use deadly force only when necessary, that is, when the officer has a reasonable belief that the subject of such force poses an imminent danger of death or serious physical injury to the officer or to another person.
 - A. Deadly force may not be used solely to prevent the escape of a fleeing suspect.
 - B. Firearms may not be fired solely to disable moving vehicles.
 - C. If feasible and if to do so would not increase the danger to the officer or others, a verbal warning to submit to the authority of the officer shall be given prior to the use of deadly force.
 - D. Warning shots are not permitted outside of the prison context.
 - E. Officers will be trained in alternative methods and tactics for handling resisting subjects, which must be used when the use of deadly force is not authorized by this policy.

CUSTODIAL SITUATIONS

- II. Unless force other than deadly force appears to be sufficient, deadly force may be used to prevent the escape of a prisoner committed to the custody of the Attorney General or the Bureau of Prisons
 - A. if the prisoner is effecting his or her escape in a manner that poses an imminent danger to the safety of the officer or another person; or
 - B. if the prisoner is escaping from a secure facility or is escaping while in transit to or from a secure facility.
- III. If the subject is in a non-secure facility, deadly force may be used only when the subject poses an imminent danger of death or serious physical injury to the officer or another person.
- IV. If the subject is in transit to or from a non-secure facility and is not accompanied by a person who is in transit to or from a secure facility, deadly force may be used only when the subject poses an imminent danger of death or serious physical injury to the officer or to another person.

UNCLASSIFIED – ~~FOR OFFICIAL USE ONLY~~
Domestic Investigations and Operations Guide

- V. After an escape from a facility or vehicle and its immediate environs has been effected, officers attempting to apprehend the escaped prisoner may use deadly force only when the escaped prisoner poses an imminent danger of death or serious physical injury to the officer or another person.
- VI. Deadly force may be used to maintain or restore control of a prison or correctional facility when the officer reasonably believes that the intended subject of the deadly force is participating in a disturbance in a manner that threatens the safety of the officer or another person.
- VII. In the prison context, warning shots may be fired within or in the immediate environs of a secure facility if there is no apparent danger to innocent persons: (A) If reasonably necessary to deter or prevent the subject from escaping from a secure facility; or (B) if reasonably necessary to deter or prevent the subject's use of deadly force or force likely to cause serious physical injury.

APPLICATION OF THE POLICY

- VIII. This policy is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or equity, against the United States, its departments, agencies, or other entities, its officer or employees, or any other person.

F.3 (U) TRAINING

A) (U) Deadly Force Policy Training Material, dated 7/29/2004.

UNCLASSIFIED - ~~FOR OFFICIAL USE ONLY~~

Domestic Investigations and Operations Guide

(Rev. 01-31-2003)

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 05-08-2018 BY [REDACTED] NSICG

b6
b7C

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 07/29/2004

To: All Divisions

Attn: AD
ADIC
SAC
CDC
PFI
FBIHQ, Manuals Desk
FBIHQ, Manuals Desk

From: General Counsel
Legal Instruction Unit
Contact: [REDACTED]

b6
b7C

Approved By: Caproni, Valerie E.
[REDACTED]

Drafted By: [REDACTED]

Case ID #: 66F-HQ-1312253
66F-HQ-C1384970
66F-HQ-C1384970

Title: REVISIONS TO THE DEPARTMENT OF
JUSTICE DEADLY FORCE POLICY -
DISSEMINATION OF TRAINING MATERIALS

Synopsis: This Electronic Communication (EC) provides recipients with training materials incorporating the revisions approved on July 1, 2004 to the Department of Justice (DOJ) Deadly Force Policy.

Reference: 66F-HQ-1312253 Serial 8

Enclosure(s): One copy of an instructional outline and one copy of use of force scenarios provided to all recipients for training purposes.

Details: As discussed in the referenced EC, dated 7/7/2004, on July 1, 2004, the Attorney General approved a revised Policy Statement on the use of Deadly Force. In order to assist Field Offices in providing training and guidance on the practical application of the Deadly Force Policy in light of the revised language, the Legal Instruction Unit (LIU), Office of the General Counsel, revised training materials used with the prior Policy Statement to reflect the changes approved by the Attorney General.

UNCLASSIFIED – ~~FOR OFFICIAL USE ONLY~~
Domestic Investigations and Operations Guide

To: All Divisions From: General Counsel
Re: 66F-HQ-1312253, 07/29/2004

The training materials consist of an Instructional Outline and a set of 13 factual scenarios with a discussion of the use of force within the scenario and whether its use violates the policy. This material is similar to what was used for instructional purposes since 12/1/1995. The revised material reflects what was noted in the EC, that the revised policy does not expand or contract the current justification for the use of deadly force. Nonetheless, revisions to the training materials were necessary in order to describe the application of deadly force consistent with the new more succinct policy statement.

The revisions to the training materials primarily relate to the elimination of the "safe alternative" language as a function of the "necessity" for use of deadly force and elimination of language addressing [REDACTED]

b7E

[REDACTED] For a more detailed discussion of the nature of the revised Policy Statement and the basis for these revisions, refer to the referenced EC.

UNCLASSIFIED – ~~FOR OFFICIAL USE ONLY~~
Domestic Investigations and Operations Guide

To: All Divisions From: General Counsel
Re: 66F-HQ-1312253, 07/29/2004

LEAD(s):

Set Lead 1: (Action)

ALL RECEIVING OFFICES

It is requested that this communication be distributed
to all appropriate personnel.

♦♦

UNCLASSIFIED – ~~FOR OFFICIAL USE ONLY~~
Domestic Investigations and Operations Guide

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 05-08-2018 BY NSICG

b6
b7C

DEADLY FORCE POLICY
TRAINING MATERIAL - 7/29/2004

DEPARTMENT OF JUSTICE DEADLY FORCE POLICY¹

Law enforcement officers of the Department of Justice may use deadly force only when necessary, that is, when the officer has a reasonable belief that the subject of such force poses an imminent danger of death or serious physical injury to the officer or to another person.

- A. **Deadly force may not be used solely to prevent the escape of a fleeing suspect.**
- B. **Firearms may not be fired solely to disable moving vehicles.**
- C. **If feasible and to do so would not increase the danger to the officer or others, a verbal warning to submit to the authority of the officer shall be given prior to the use of deadly force.**
- D. **Warning shots are not permitted²**
- E. **Officers will be trained in alternative methods and tactics for handling resisting subjects which must be used when the use of deadly force is not authorized by this policy.**

This policy is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity, against the United States, its departments, agencies, or other entities, its officers or employees, or any other person.

¹Department of Justice Policy Statement Use of Deadly Force (07/01/2004) in pertinent part (Language relating to Custodial Situations has been intentionally omitted pursuant to FBI policy. See, 66F-HQ-1312253, EC from the Director's Office to All Divisions, titled "REVISIONS TO THE DEPARTMENT OF JUSTICE DEADLY FORCE POLICY", dated 07/07/2004).

²Not included in the above description is the policy relating to the use of deadly force to prevent the escape of a prisoner committed to the custody of the Attorney General or the Bureau of Prisons. Because Agents will seldom find themselves in a position to apply the custodial aspect of the policy, the FBI will adhere to the policy decision set forth in the Airtel from the Director to All Field Offices, titled "Deadly Force Policy Matters," dated 1/5/95, which states "A policy decision has been made that except in cases of prison unrest which would principally involve HRT and/or SWAT, FBI Agents should adhere to the policy and training principles governing the use of deadly force in non-custodial situations.

F.4 (U) TRAINING

B) (U) Instructional Outline and Use of Force Scenarios.

UNCLASSIFIED – ~~FOR OFFICIAL USE ONLY~~
Domestic Investigations and Operations Guide

07/29/2004

INSTRUCTIONAL OUTLINE

I. INTRODUCTION

The following general principles shall guide the interpretation and application of this policy:

- A. This policy shall not be construed to require Agents to assume unreasonable risks to themselves.
- B. The reasonableness of an Agent's decision to use deadly force must be viewed from the perspective of the Agent on the scene without the benefit of 20/20 hindsight.
- C. Allowance must be made for the fact that Agents are often forced to make split-second decisions in circumstances that are tense, uncertain, and rapidly evolving.

II. DEFINITIONS

- A. "DEADLY FORCE": Is force that is reasonably likely to cause death or serious physical injury.
- B. "REASONABLE BELIEF": Is synonymous with "Probable Cause". It is determined by a totality of the facts and circumstances known to Agents at the time, and the logical inferences that may be drawn from them.
- C. "NECESSARY": The necessity to use deadly force based on the existence of a reasonable belief that the person against whom such force is used poses an imminent danger of death or serious physical injury to the Agent or other persons.
- D. "IMMINENT DANGER": "Imminent" does not mean "immediate" or "instantaneous", but that an action is pending. Thus, a subject may pose an imminent danger even if he is not at that very moment pointing a weapon at the Agent. For example, imminent danger may exist if Agents have probable cause to believe any of the following:

UNCLASSIFIED – ~~FOR OFFICIAL USE ONLY~~
Domestic Investigations and Operations Guide

1. The subject possess a weapon, or is attempting to gain access to a weapon, under circumstances indicating an intention to use it against the Agents or others; or,
2. The subject is armed and running to gain the tactical advantage of cover; or,
3. A subject with the capability of inflicting death or serious physical injury--or otherwise incapacitating agents--without a deadly weapon, is demonstrating an intention to do so; or,
4. The subject is attempting to escape from the vicinity of a violent confrontation in which the suspect inflicted or attempted the infliction of death or serious physical injury.

III APPLICATION OF DEADLY FORCE

In assessing the necessity to use deadly force, the following practical considerations are relevant to its proper application:

A. Inherent Limitation on Abilities to Assess the Threat and Respond.

1. Limited Time (Action v. Reaction) - there will always be an interval of time between a subject's action and an Agent's ability to perceive that action, to assess its nature, and to formulate and initiate an appropriate response. The inherent disadvantage posed by the action/reaction factor places a significant constraint on the time frame within which Agents must perceive, assess and react to a threat.
2. Limited Means (Wound Ballistics) - When the decision is made to use deadly force, Agents have *no guaranteed means of instantaneously stopping the threat*. The human body can sustain grievous - even ultimately fatal - injury and continue to function for a period of time (from several seconds to several minutes) depending on the location, number, and severity of the wounds. The lack of a reliable means of instantaneously stopping the threat, may extend the time that imminent danger can persist. This factor further constrains the time frame within which Agents must respond to a perceived threat.

B. Achieving Intended Purpose.

1

b7E

Domestic Investigations and Operations Guide

If the subject does not surrender, the only reliable means of achieving that goal is to cause physiological incapacitation of the subject(s) as quickly as possible. Attempts to do anything else - such as shooting to cause minor injury - are unrealistic and can risk exposing Agents or others to continued danger of death or serious physical injury.

2.



b7E

C. Consideration of Risk to Other Parties.

Even when deadly force is permissible, Agents should assess whether its use creates a danger to third parties that outweighs the likely benefits of its use.

UNCLASSIFIED – ~~FOR OFFICIAL USE ONLY~~
Domestic Investigations and Operations Guide

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 05-08-2018 BY [REDACTED] NSICG

b6
b7C

SCENARIO #1: [REDACTED]

b5
b7E

[REDACTED]

DISCUSSION:

[REDACTED]

b7E

[REDACTED]

UNCLASSIFIED – ~~FOR OFFICIAL USE ONLY~~
Domestic Investigations and Operations Guide

SCENARIO #2:

b5
b7E

DISCUSSION:

b7E

UNCLASSIFIED – ~~FOR OFFICIAL USE ONLY~~
Domestic Investigations and Operations Guide

SCENARIO #3:

b5
b7E

DISCUSSION:

b7E

UNCLASSIFIED – ~~FOR OFFICIAL USE ONLY~~
Domestic Investigations and Operations Guide

SCENARIO #4:

b5
b7E

DISCUSSION:

b7E

UNCLASSIFIED – ~~FOR OFFICIAL USE ONLY~~
Domestic Investigations and Operations Guide

SCENARIO #5:

b5
b7E

DISCUSSION:

b7E

UNCLASSIFIED – ~~FOR OFFICIAL USE ONLY~~
Domestic Investigations and Operations Guide

SCENARIO #6:

b5
b7E

DISCUSSION:

b7E

UNCLASSIFIED – ~~FOR OFFICIAL USE ONLY~~
Domestic Investigations and Operations Guide

SCENARIO #7:

b5
b7E

DISCUSSION:

b7E

UNCLASSIFIED – ~~FOR OFFICIAL USE ONLY~~
Domestic Investigations and Operations Guide

SCENARIO #8:

b5
b7E

DISCUSSION:

b7E

UNCLASSIFIED – ~~FOR OFFICIAL USE ONLY~~
Domestic Investigations and Operations Guide

SCENARIO #9:

b5
b7E

DISCUSSION:

b7E

SCENARIO #10:

b5
b7E

DISCUSSION:

b7E

UNCLASSIFIED – ~~FOR OFFICIAL USE ONLY~~
Domestic Investigations and Operations Guide

SCENARIO #11:

b5
b7E

DISCUSSION:

b7E

UNCLASSIFIED – ~~FOR OFFICIAL USE ONLY~~
Domestic Investigations and Operations Guide

SCENARIO #12:

b5
b7E

DISCUSSION:

b7E

UNCLASSIFIED – ~~FOR OFFICIAL USE ONLY~~
Domestic Investigations and Operations Guide

SCENARIO #13:

b5
b7E

DISCUSSION:

b7E

UNCLASSIFIED – ~~FOR OFFICIAL USE ONLY~~
Domestic Investigations and Operations Guide

SCENARIO #14:

b5
b7E

DISCUSSION:

b7E

This Page is Intentionally Blank

~~SECRET//NOFORN~~

Domestic Investigations and Operations Guide

§G



ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

(U) DOMESTIC INVESTIGATIONS AND OPERATIONS GUIDE

(U) Appendix G

(U) Classified Provisions

(U) Version Dated: September 28, 2016

APPENDIX G: (U) CLASSIFIED PROVISIONS

(U) This Part supplements the unclassified provisions of the AGG-Dom and DIOG.

(U) Table of Contents

G.1	(U) Limitation on Certain Searches	3
G.2	(U) Circumstances Warranting a Preliminary or Full Investigation	4
G.3	(U) Determination of United States Person (USPER) Status	5
(U) G.4	(S//NF) Attorney General Threat Country List	6
G.5	(U) Assistance to and/or from Foreign Agencies in the United States	7
G.6	(U) Consensual Monitoring	8
G.7	(U) Sensitive Investigative Matters (SIM)	9
G.8	(U) Data Analysis	11
G.9	(U) Notice Requirements for the DOJ National Security Division (NSD)	12
G.10	(U) [REDACTED]	13
G.11	(U) [REDACTED]	16
G.12	(U) National Security Letters for Telephone Toll Records of Members of the News Media or News Organizations	17
G.13	(U) Other Investigative Resources	20
G.14	(U) Recruitment-In-Place Type 5 Assessments (“RIP Type 5”) on Subjects of Approved Counterintelligence (CD) Full Investigations	21

b7E

~~Derived from: Multiple Sources~~

~~Declassify on: December 1, 2033~~

G.1 (U) LIMITATION ON CERTAIN SEARCHES

G.1.1 (U) *CLASSIFIED AGG-DOM PROVISION*

(S)

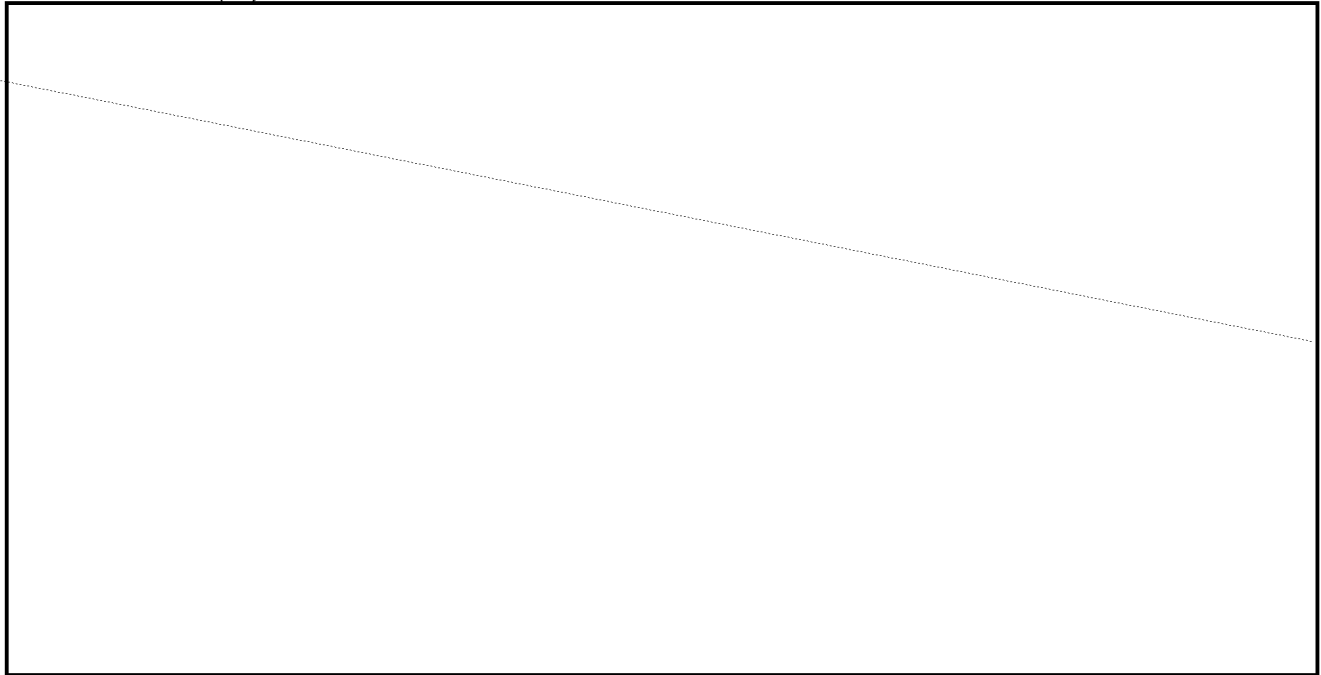
b1
b3

G.1.2 (U) *DIOG CLASSIFIED PROVISION*

(U) Refer to the Domestic Investigations and Operations Guide (DIOG) Section 18.7.1 for procedures to obtain a FISA search warrant.

G.2 (U) CIRCUMSTANCES WARRANTING A PRELIMINARY OR FULL INVESTIGATION

G.2.1 (U) *CLASSIFIED AGG-DOM PROVISION*



(S)

b1
b3

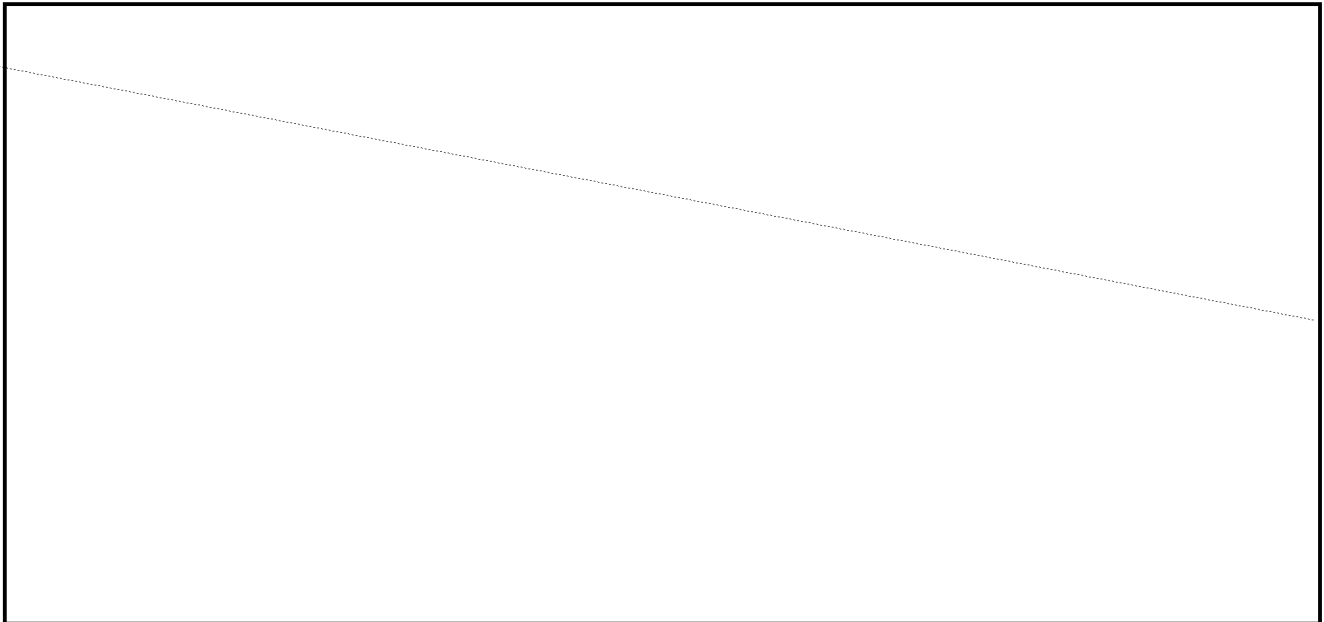
G.2.2 (U) *DIOG CLASSIFIED PROVISION*

(U) The provisions of DIOG Sections 6 (Preliminary Investigations) or 7 (Full Investigations) with regard to the purpose, approval and notification requirements apply fully to investigations predicated under this provision.

G.3 (U) DETERMINATION OF UNITED STATES PERSON (USPER) STATUS

G.3.1 (U) CLASSIFIED AGG-DOM PROVISION

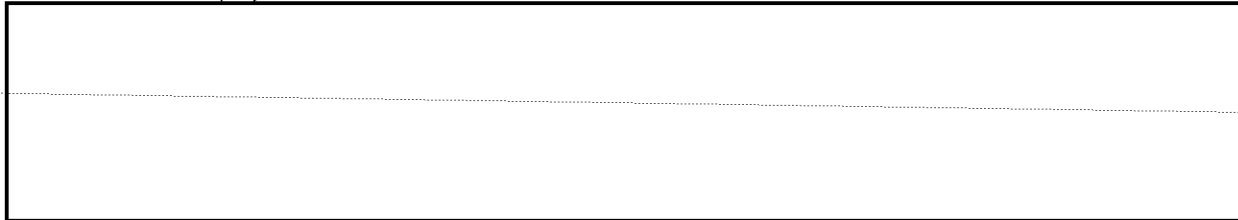
(S)



b1
b3

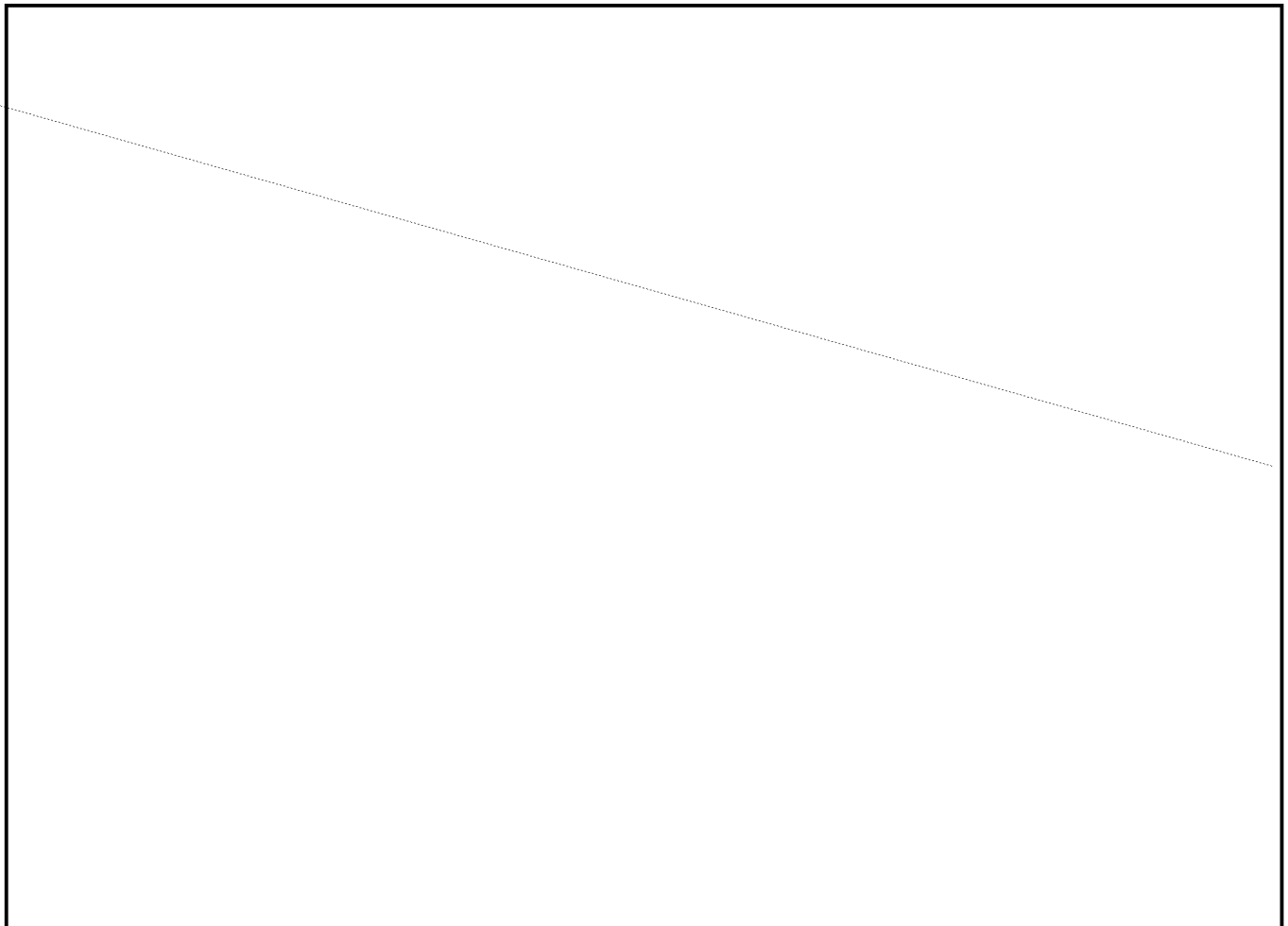
(U) G.4 ~~(S//NF)~~ ATTORNEY GENERAL THREAT COUNTRY LIST

G.4.1 (U) *CLASSIFIED AGG-DOM PROVISION*



b1
b3

G.4.2 (U) *DIOG CLASSIFIED PROVISION*



b1
b3

G.5 (U) ASSISTANCE TO AND/OR FROM FOREIGN AGENCIES IN THE UNITED STATES

G.5.1 (U) *DIOG CLASSIFIED PROVISION*

(S)

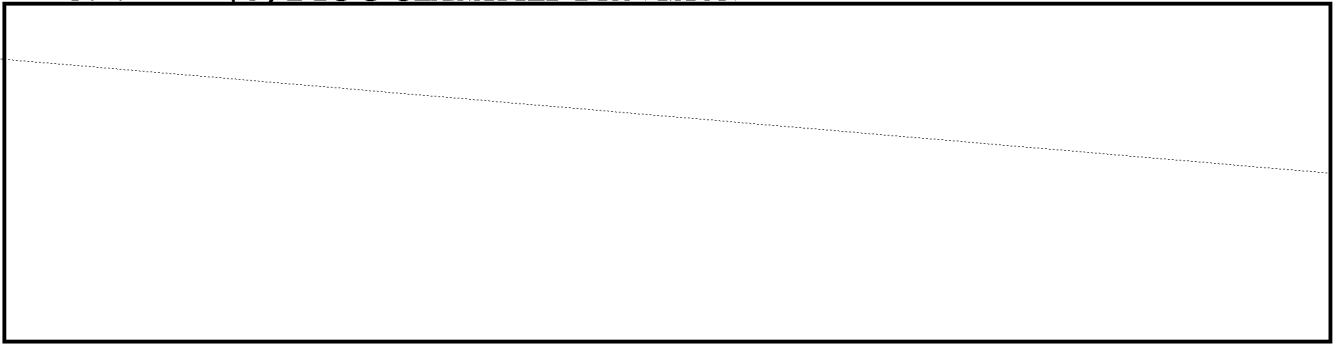
b1

b3

G.6 (U) CONSENSUAL MONITORING

G.6.1 (U) *DIOG CLASSIFIED PROVISION*

(S)



b1
b3

G.7 (U) SENSITIVE INVESTIGATIVE MATTERS (SIM)**G.7.1 (U) DIOG CLASSIFIED PROVISION**

(S)

b1
b3**G.7.1.1 (U//~~FOUO~~) MEMBER OF THE NEWS MEDIA OR A NEWS ORGANIZATION**

(U//~~FOUO~~) DIOG Section 10.1.2.2.5 defines a member of the news media or a news organization as a SIM. It further defines a member of the news media or a news organization as:

(U//~~FOUO~~) “News media” includes persons and organizations that gather, report or publish news, whether through traditional means (e.g., newspapers, radio, magazines, news service) or the on-line or wireless equivalent. A “member of the media” is a person who gathers, reports, or publishes news through the news media.

(U//~~FOUO~~) The term “News Media” also includes an entity organized and operated for the purpose of gathering, reporting or publishing news. The definition does not, however, include a person or entity who posts information or opinion on the Internet in blogs, chat rooms or social networking sites, such as YouTube, Facebook, or MySpace, unless that person or entity falls within the definition of a member of the media or a news organization under the other provisions within this section (e.g., a national news reporter who posts on his/her personal blog).

(U//~~FOUO~~) Examples of news media entities include television or radio stations broadcasting to the public at large and publishers of newspapers or periodicals that make their products available to the public at large in print form or through an Internet distribution. A freelance journalist may be considered to work for a news organization if the journalist has a contract with the news entity or has a history of publishing content. Publishing a newsletter or operating a website does not by itself qualify an individual as a member of the news media. Businesses, law firms, and trade associations offer newsletters or have websites; these are not considered news media. As the term is used in the DIOG, “news media” is not intended to include persons and entities that simply make information available. Instead, it is intended to apply to a person or entity that gathers information of potential interest to a segment of the general public, uses editorial skills to turn raw materials into a distinct work, and distributes that work to an audience, as journalism professional. If there is doubt about whether a particular person or entity should be considered part of the “news media,” the doubt should be resolved in favor of considering the person or entity to be the “news media.”

G.7.1.1.1

(S)

b1
b3



G.7.1.2 (U) ACADEMIC NEXUS

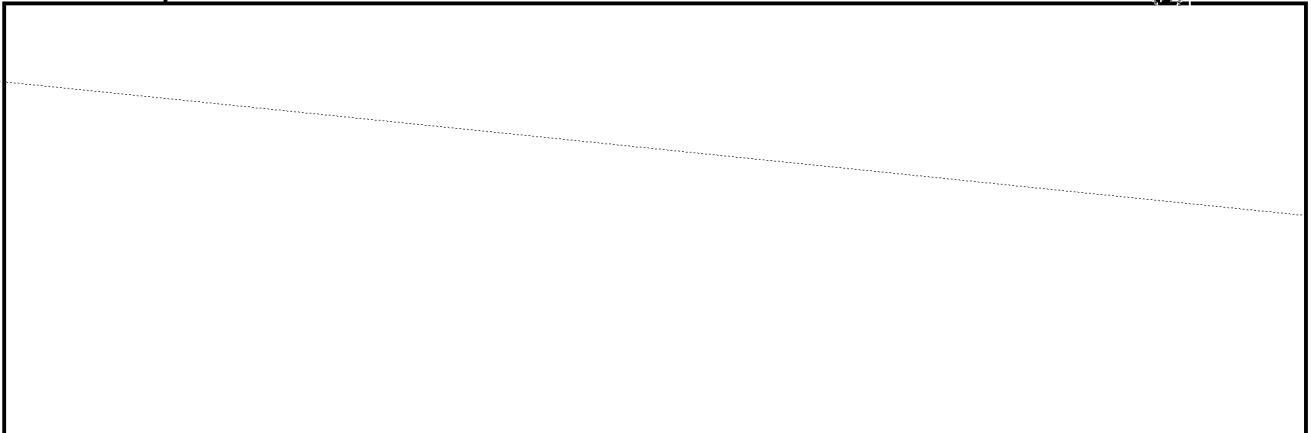
(U//~~FOUO~~) DIOG Section 10.1.2.2.6 states:

(U//~~FOUO~~) *Academic Nexus*—As a matter of FBI policy, an investigative activity having an “academic nexus” is a SIM if:

- (i) (U//~~FOUO~~) the investigative activity involves matters related to the responsibilities of an administrator or faculty member employed by any college or university that is located inside the United States, provided the matter under Assessment/investigation is related to the individual’s position at the institution; or
- (ii) (U//~~FOUO~~) the matter involves any student association recognized and approved by a college or university at which the student association at issue is located, and the college or university is located inside the United States.

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

G.7.1.2.1



G.8 (U) DATA ANALYSIS

G.8.1 (U) *DIOG CLASSIFIED PROVISION*

~~(S//X)~~ Data analysis conducted by the FBIHQ Counterintelligence Division, [REDACTED]

(S) [REDACTED] must be coordinated with the FBIHQ Office of the General Counsel, Privacy and Civil Liberties Unit and the National Security Law Branch regarding the proper documentation and disposition of such analysis.

b1
b3

G.9 (U) NOTICE REQUIREMENTS FOR THE DOJ NATIONAL SECURITY DIVISION (NSD)

G.9.1 (U) *DIOG CLASSIFIED PROVISION*

- (U) A) ~~(S)~~ **Sensitive Investigative Matter:** For a national security investigation or “assistance to other agencies” involving a sensitive investigative matter that is classified “Secret,” the appropriate FBIHQ section must send electronic notice to DOJ NSD at [REDACTED]. For a national security investigation or “assistance to other agencies” involving a sensitive investigative matter that is classified “Top Secret,” the appropriate FBIHQ section must send electronic notice to DOJ NSD at [REDACTED]. Notices to DOJ NSD must contain only the Letterhead Memorandum (LHM); the electronic communication (EC) should not be sent to DOJ NSD. b7E
- (U) B) ~~(S)~~ **National Security Full Investigation of a United States Person (USPER):** For a Full Investigation of a USPER relating to a threat to the national security (this reporting requirement does not apply to full positive foreign intelligence investigations) that is classified “Secret,” the appropriate FBIHQ section must send electronic notice to DOJ NSD at [REDACTED]. For a Full Investigation of a USPER relating to a threat to the national security that is classified “Top Secret,” the appropriate FBIHQ section must send electronic notice to DOJ NSD at [REDACTED]. Notices to DOJ NSD must only contain the LHM; the EC should not be sent to DOJ NSD.
- (U) C) ~~(S)~~ **Assistance to a Foreign Agency:** When FBIHQ approval is required to provide assistance to a foreign agency in a matter involving a threat to the national security, notice must be provided to DOJ NSD. For a foreign assistance matter that is classified “Secret,” the appropriate FBIHQ division approving the investigative method must send electronic notice to DOJ NSD at [REDACTED]. For a foreign assistance matter that is classified “Top Secret,” the appropriate FBIHQ division approving the investigative method must send electronic notice to DOJ NSD at [REDACTED]. Notices to DOJ NSD must only contain the LHM; the EC should not be sent to DOJ NSD.

G.10 (U) [REDACTED]

b1

G.10.1 **(U) *DIOG CLASSIFIED PROVISION***

(U) *Note:* The [REDACTED]
[REDACTED] - see Appendix G.10.1.3.A below) conducted under DIOG Section 5.

G.10.1.1 **(U) DEFINITION**

[REDACTED]

b1
b3

(S)

(S)

G.10.1.2 [REDACTED]

b1
b3

(S)

[REDACTED]

(S)

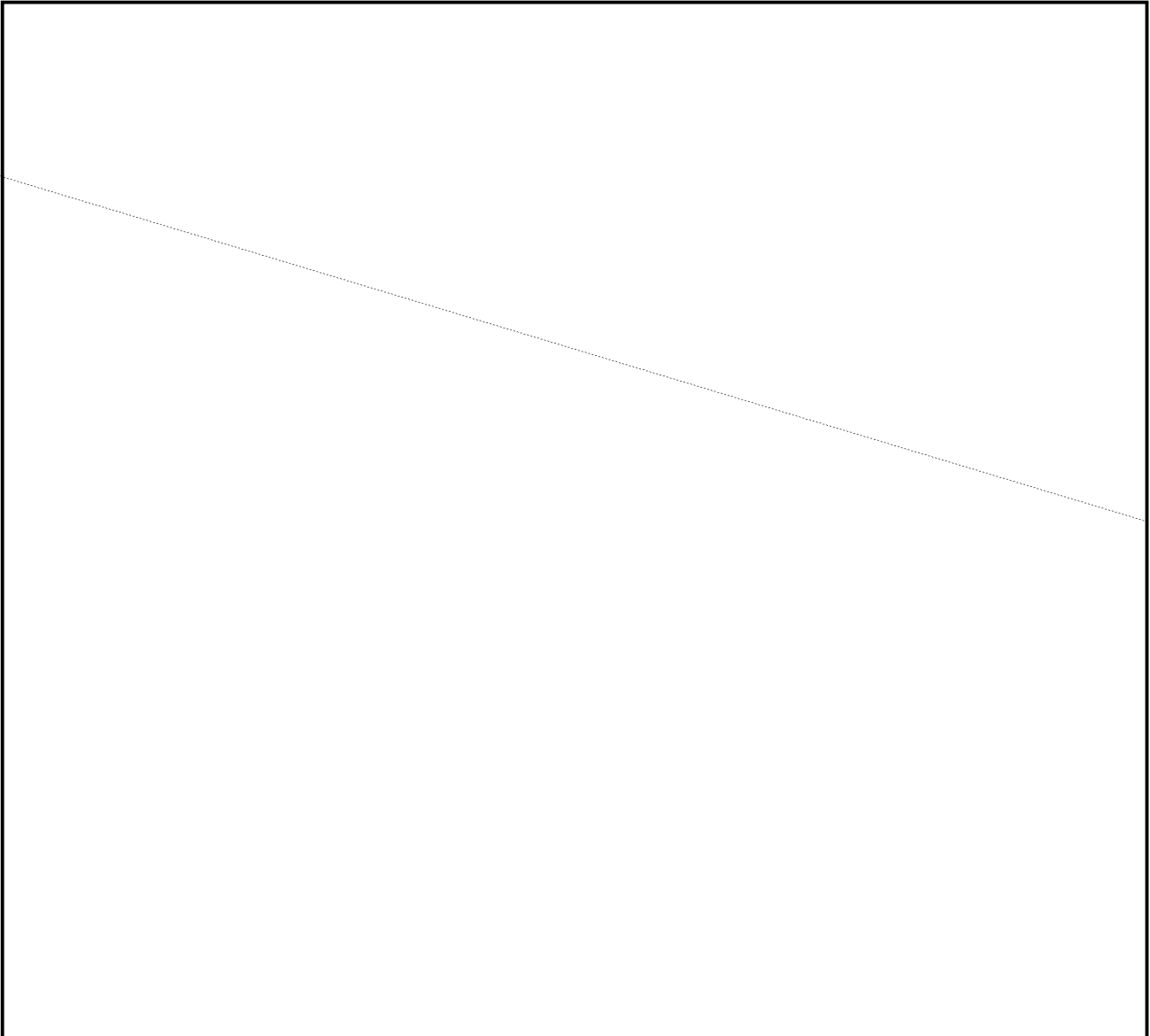


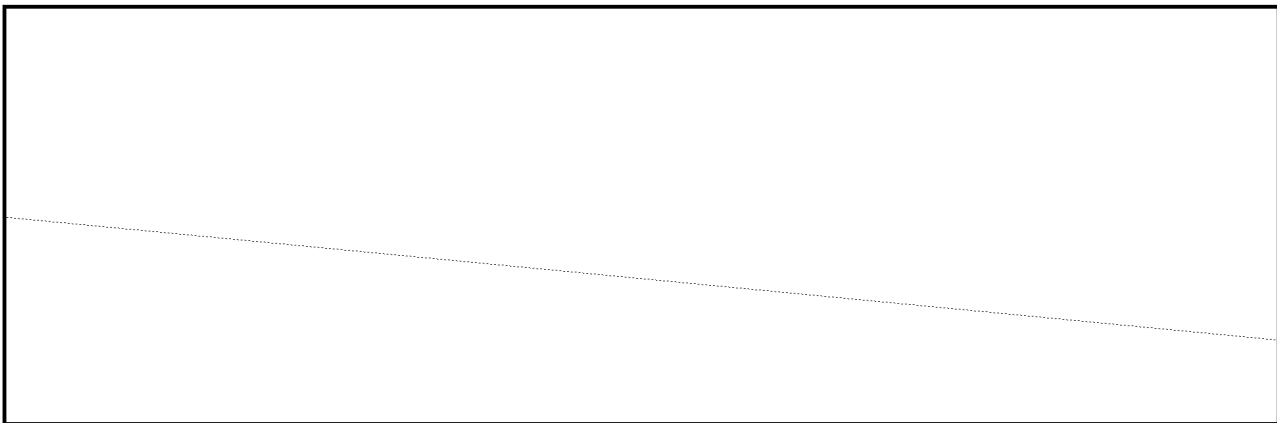
(S)

G.10.1.3



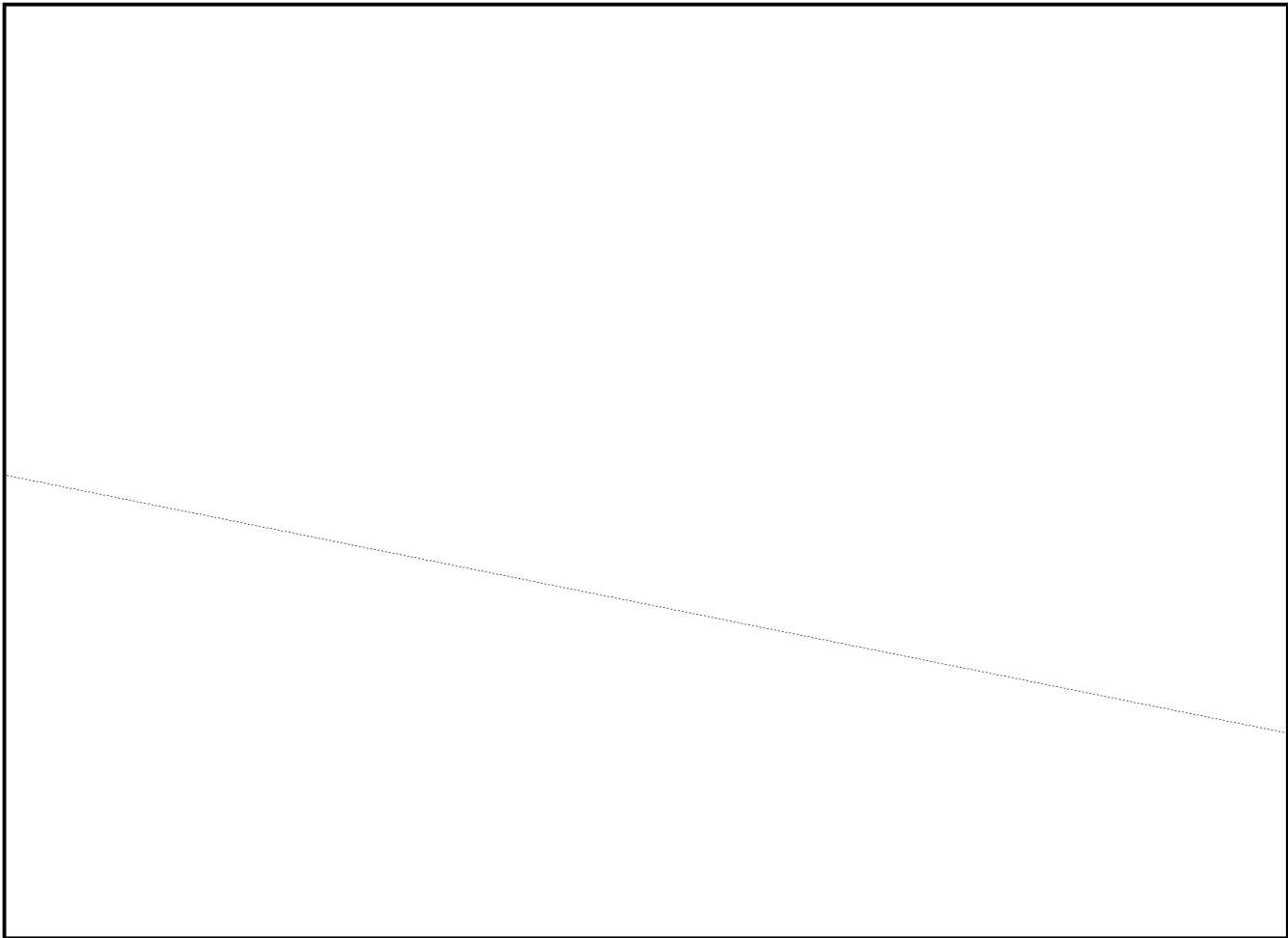
(S)





(S)

G.10.1.5 (U) DISPUTE RESOLUTION



(S)

G.10.1.4



Domestic Investigations and Operations Guide

G.11 (U) [REDACTED]

b7E

G.11.1 (U) ***DIOG CLASSIFIED PROVISION***

(U) ~~(S)~~ Procedures for conducting a [REDACTED]
[REDACTED]

(U) G.11.1.1 ~~(S)~~ **CENTRAL INTELLIGENCE AGENCY HEADQUARTERS (CIAHQ)**

(S)

[REDACTED]

b1
b3

(U) G.11.1.2 ~~(S)~~ **NATIONAL SECURITY AGENCY HEADQUARTERS (NSAHQ)**

(S)

[REDACTED]

b1
b3

G.12 (U) NATIONAL SECURITY LETTERS FOR TELEPHONE TOLL RECORDS OF MEMBERS OF THE NEWS MEDIA OR NEWS ORGANIZATIONS

(U) G.12.1 ~~(S//NF)~~ MEMBERS OF THE NEWS MEDIA OR NEWS ORGANIZATIONS

~~(S//NF)~~ An investigation of members of the news media or news organizations is a sensitive investigative matter (SIM). A member of the news media or a news organization is defined in DIOG Section 10.1.2.2.5 and Appendix G.7.1.1 [REDACTED]

b1
b3

(S)

[REDACTED]

G.12.2 (U) LAW ENFORCEMENT TOOLS OTHER THAN NATIONAL SECURITY LETTERS

b7E

(U) [REDACTED]
[REDACTED]

G.12.3 (U) APPROVAL REQUIREMENTS FOR AN NSL SEEKING RECORDS OF A MEMBER OF THE NEWS MEDIA

[REDACTED]

(U//~~FOUO~~) In addition to the approval requirements for NSLs set out in DIOG Section 18.6.6.3.3., [REDACTED]

b7E

[REDACTED]

(U//~~FOUO~~) Example 1: [REDACTED]
[REDACTED]

b7E

(U//~~FOUO~~) Example 2: [REDACTED]
[REDACTED]

G.12.4 ~~(U//FOUO)~~ **APPROVAL REQUIREMENTS FOR AN NSL SEEKING
RECORDS RELATED TO THE NEWS MEDIA OR NEWS ORGANIZATION**

(U//~~FOUO~~)

b7E

(U//~~FOUO~~) *Example 1:*

(U//~~FOUO~~) *Example 2:*

G.12.5 (U) ~~(S//NF)~~ **APPROVAL REQUIREMENTS FOR AN NSL SEEKING RECORDS
OF A MEMBER OF THE NEWS MEDIA**

b1
(S) b3

~~(S//NF)~~

(S)

b1
b3
b7E

(S)

G.12.1 *(U)SPECIFIC PROCEDURES FOR REQUESTING AN NSL*

(U) The procedures for creating an NSL [REDACTED]

b7E

[REDACTED]

[REDACTED] are the

same as set out in DIOG Section 18.6.6.3.7. [REDACTED]

[REDACTED]

G.13 (U) OTHER INVESTIGATIVE RESOURCES

G.13.1 (U) *DIOG CLASSIFIED PROVISION*

G.13.1.1 (U//~~FOUO~~) SENSITIVE TECHNICAL EQUIPMENT

(S) ~~(S)~~ **Definition:** The term “Sensitive Technical Equipment” (STE) includes [redacted] STE is a) any technology [redacted]

b1
b3
b7E

(S) [redacted] c) technology that has been jointly developed with or developed by another U.S. Government (USG) agency such that the FBI is not the sole owner and on which originator controls have been placed. The Assistant Director of the OTD after consultation with the relevant operational division is authorized to determine whether particular equipment is (or is not) STE.

(S) ~~(S//NF)~~ **Authorized Investigative Activity:** Any use of [redacted]

(S) [redacted] For additional guidance, refer to the Extraterritorial Guidelines (see DIOG Section 13) [redacted]

G.14 (U) **RECRUITMENT-IN-PLACE TYPE 5 ASSESSMENTS (“RIP TYPE 5”)** ☐

b7E

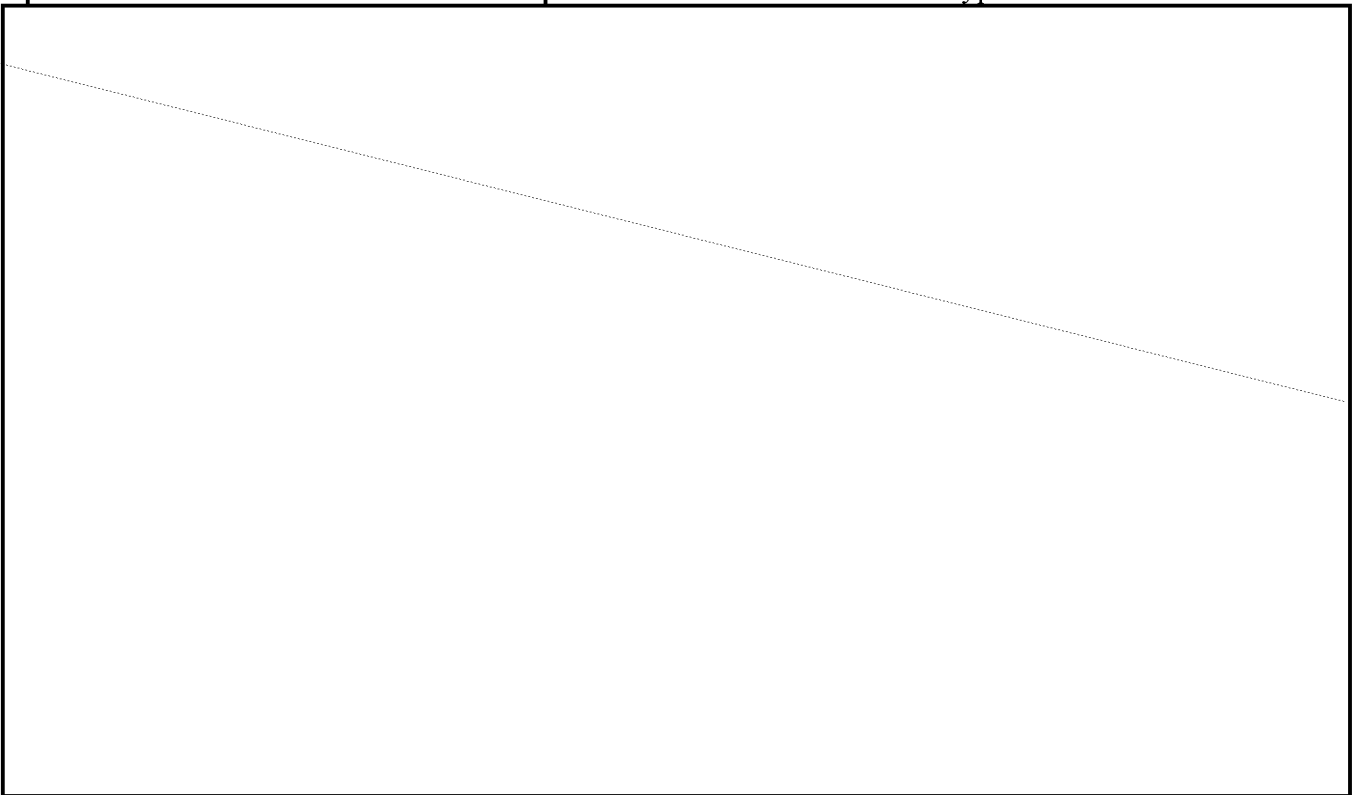


(U) See Quick Reference Guide for RIP Type 5 Assessments (links to a ~~SECRET~~ document).

(U/~~FOUO~~) **Summary:** A Type 5 Assessment provides the authority and process for identifying, evaluating, and recruiting a potential confidential human source (CHS). The following provisions integrate guidance from relevant subsections of the DIOG, the Counterintelligence Division Policy Guide (CDPG), 0717PG, and the Confidential Human Source Policy Guide (CHSPG), 0836PG. ☐ Where noted, requirements remain the same as those in the DIOG, the CDPG, and the CHSPG, but the process has been tailored for specific use of Type 5 Assessments ☐

☐ hereinafter referred to as “RIP Type 5s.”

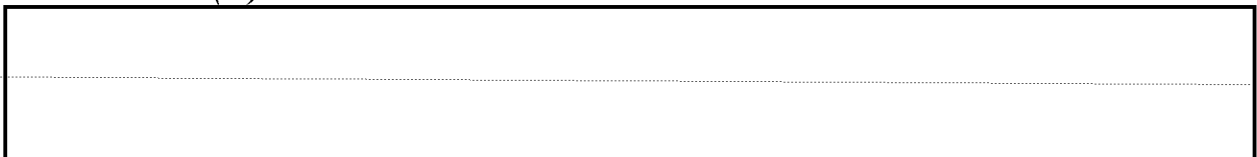
(S)



b1
b3

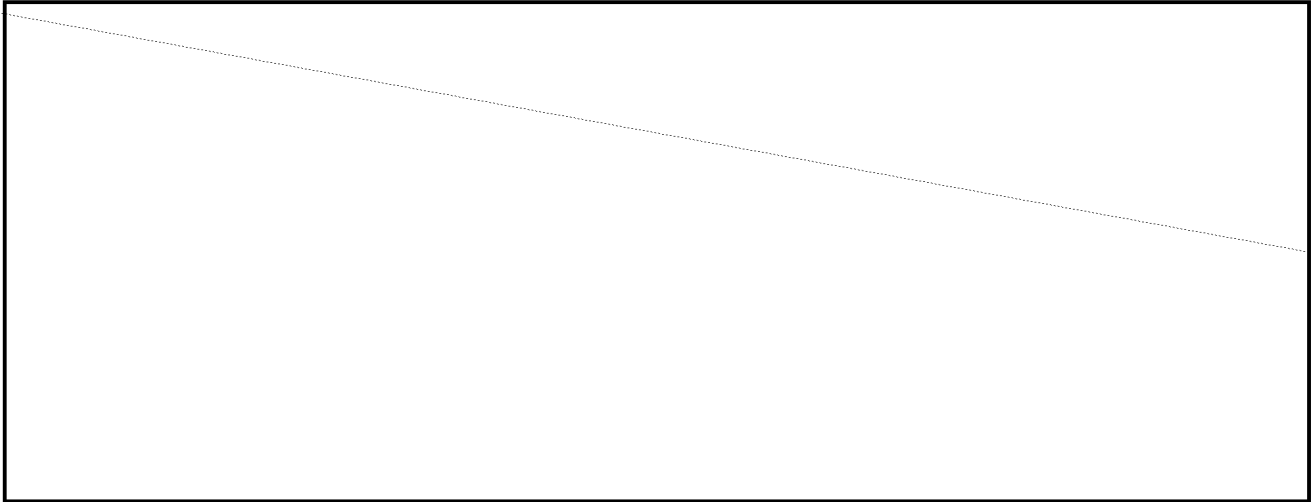
G.14.1 (U) **RIP TYPE 5 ASSESSMENTS**

(S)

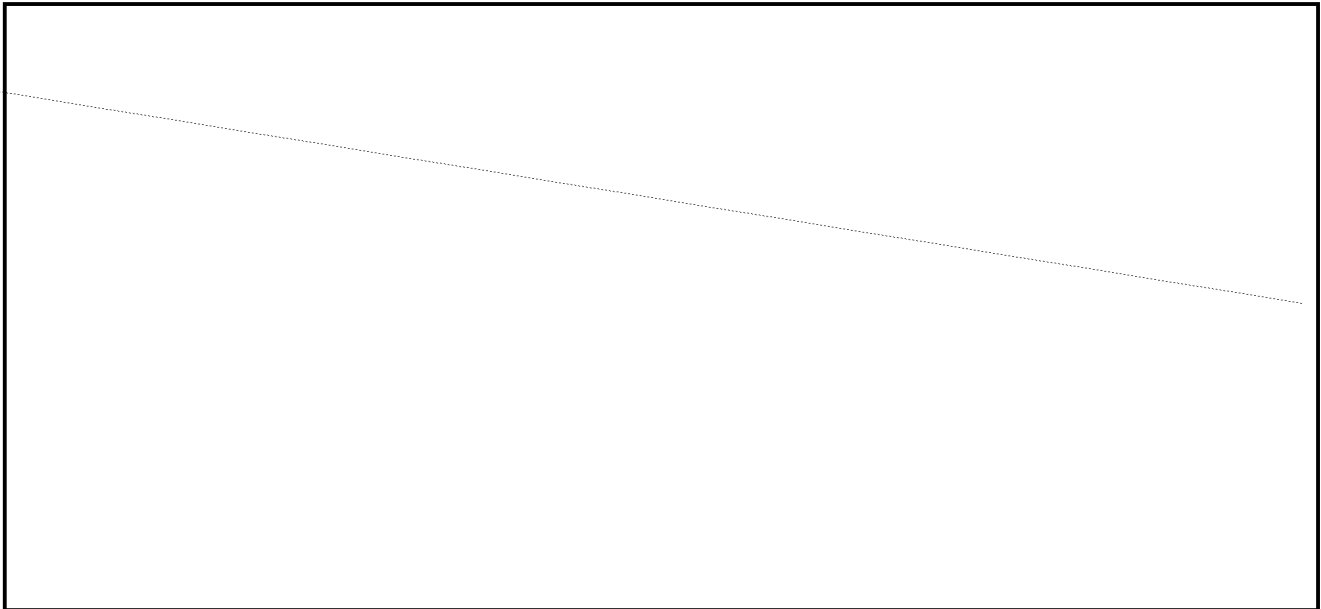


G.14.2 ***(U) STANDARDS FOR OPENING OR APPROVING A RIP TYPE 5 ASSESSMENT***

(S)

b1
b3

(S)



G.14.3 ***(U) FILE REVIEW***

(U) The frequency of the supervisory file review must be in accordance with DIOG 3.4.4.3. Additionally, the RIP Type 5 Assessment review standards (ARS) are as follows and must be documented in an EC

b7E

- (U//~~FOUO~~) Whether authorized investigative methods have been used properly.
- (U//~~FOUO~~) Whether reimbursable expenses incurred by an SA, if any, were reasonable and properly authorized.
- (U//~~FOUO~~) Whether the potential RIP can or should be recruited.

¹ (U//~~FOUO~~)



- (U//~~FOUO~~) Whether the RIP Type 5 Assessment should continue for an additional 90 days (60 days for probationary employees). If continuation is deemed justified, the supervisory special agent (SSA) must document the rationale for keeping the RIP Type 5 Assessment open.

(U//~~FOUO~~) Because the ARS EC must be made part of the case file and documented

b7E

The EC must only document that the RIP Type 5 has met the ARS listed above.

G.14.4 ***(U) AUTHORIZED INVESTIGATIVE METHODS PERMITTED
IN RIP TYPE 5 ASSESSMENTS***

(S)

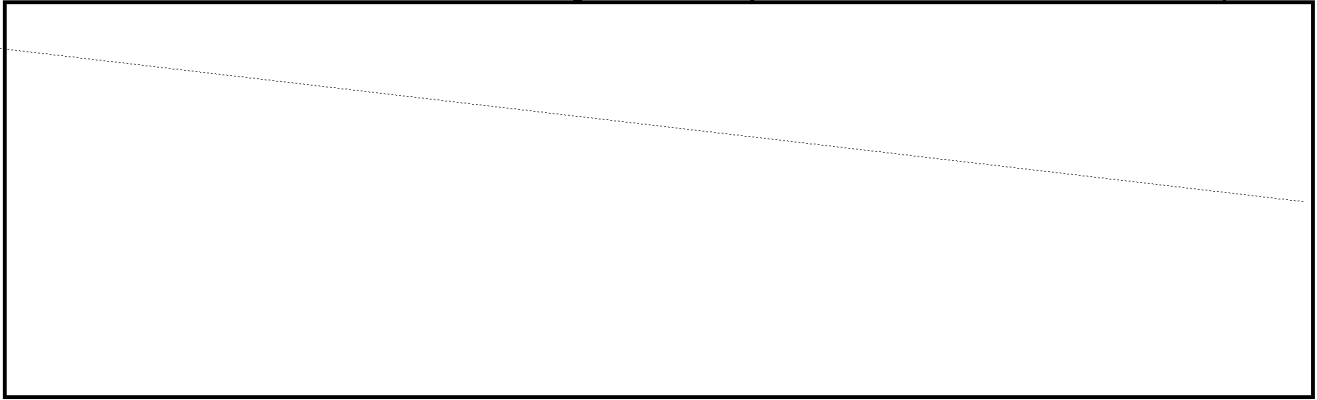
b1
b3

(S)

G.14.5

(S)

(S)

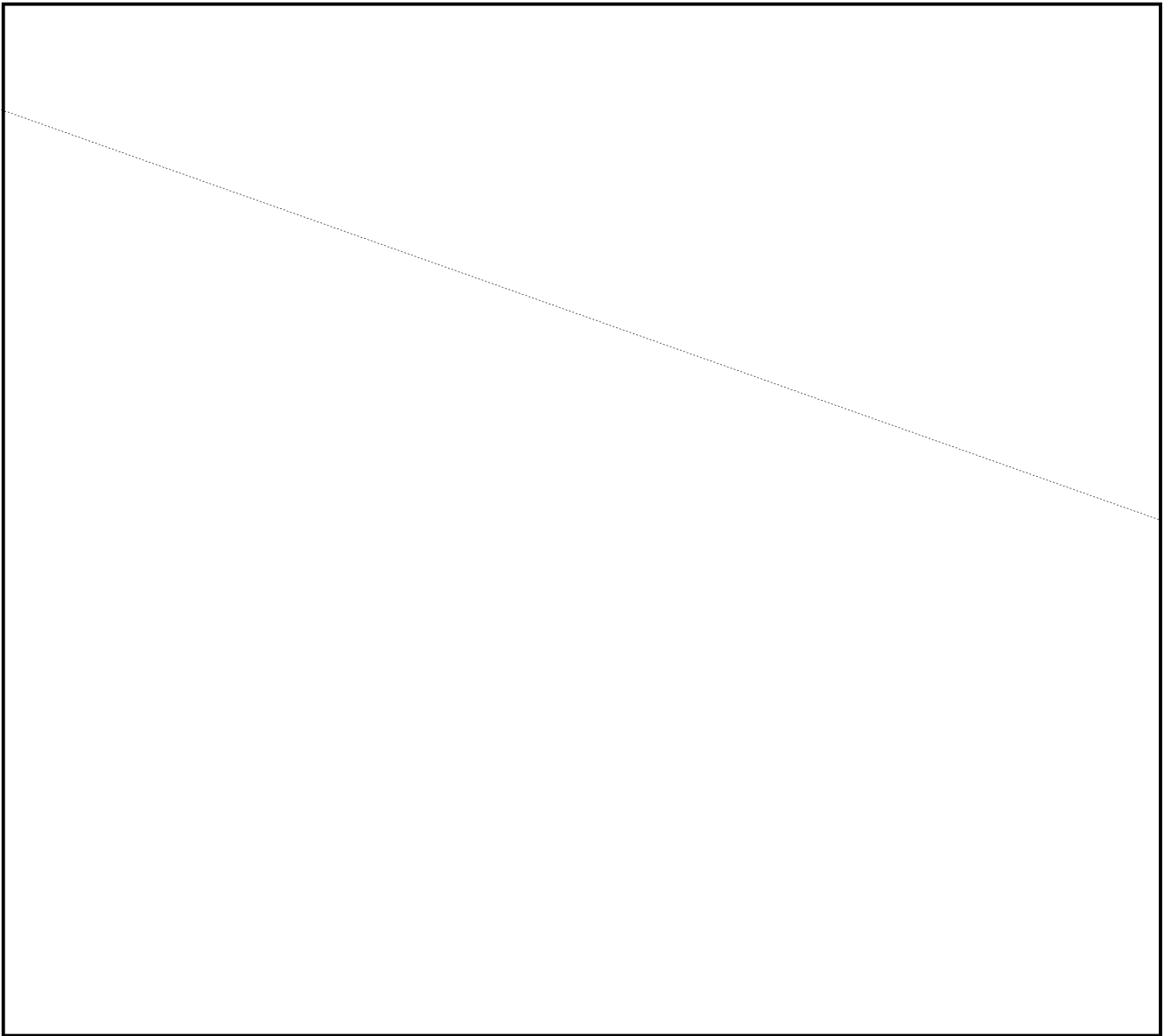


(S)

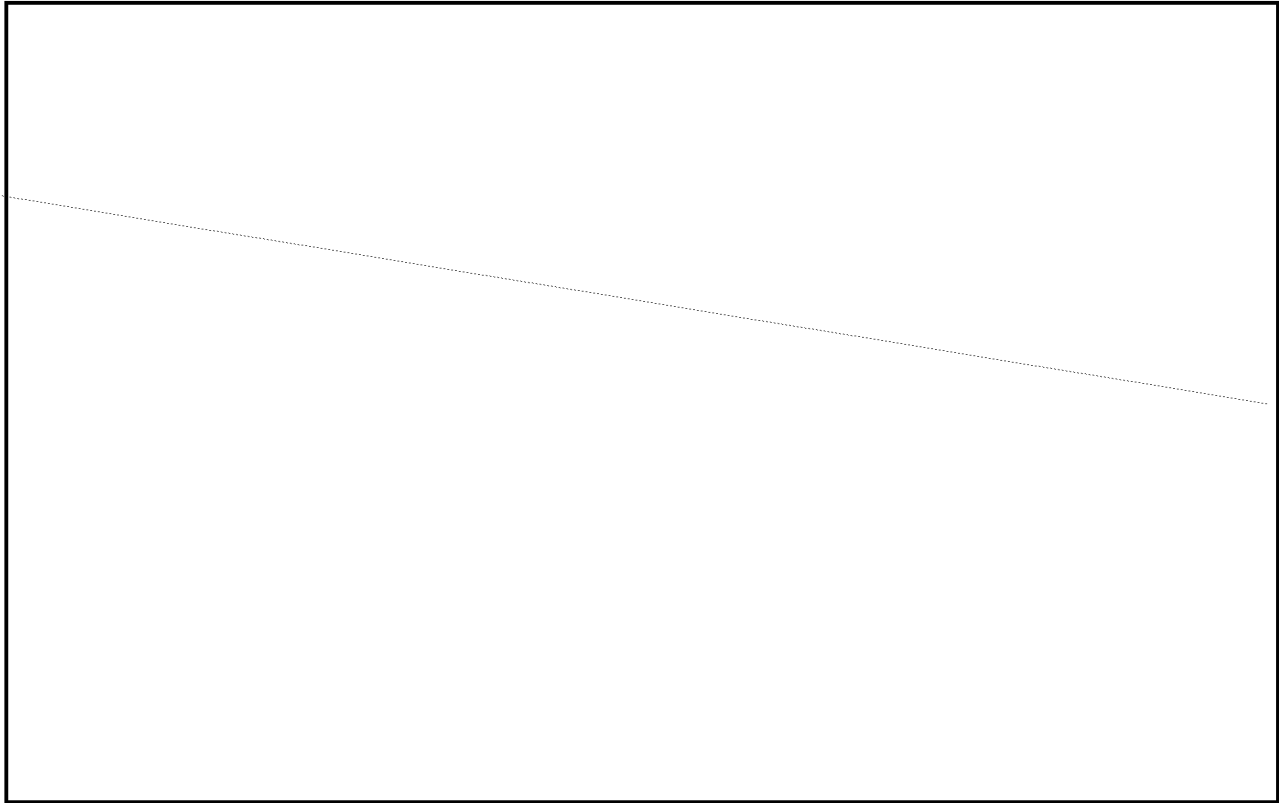
G.14.5.1



(S)

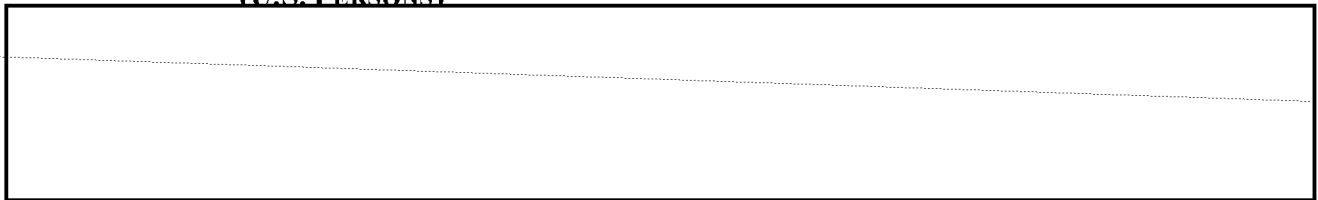


(S)



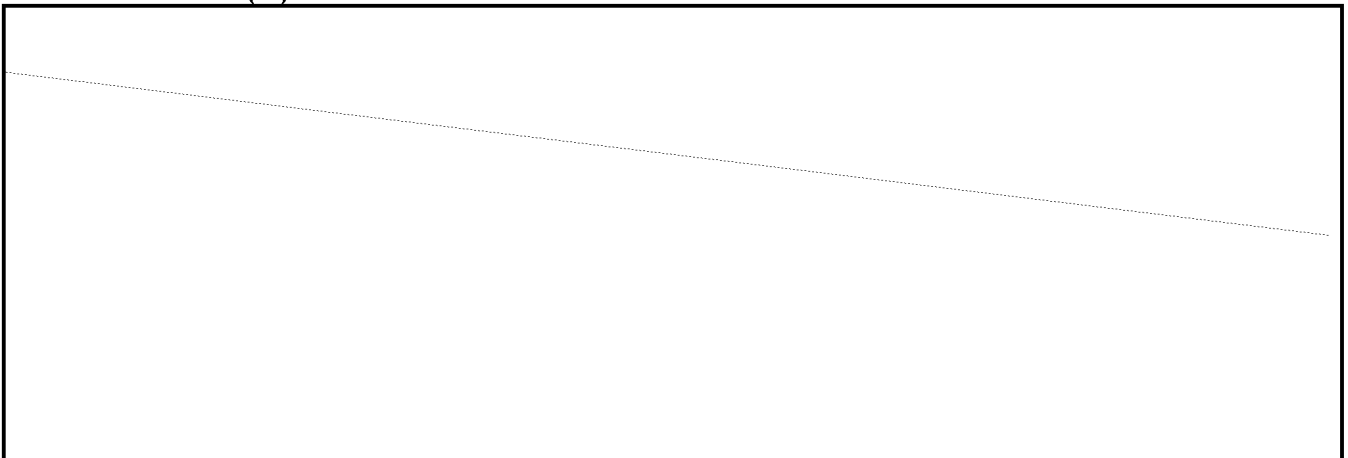
**G.14.5.2 (U) ADDITIONAL APPROVAL REQUIREMENT FOR UNITED STATES PERSONS
(U.S. PERSONS)**

(S)



G.14.5.3 (U) RECRUITMENT FROM THE COVERT APPROACH

(S)



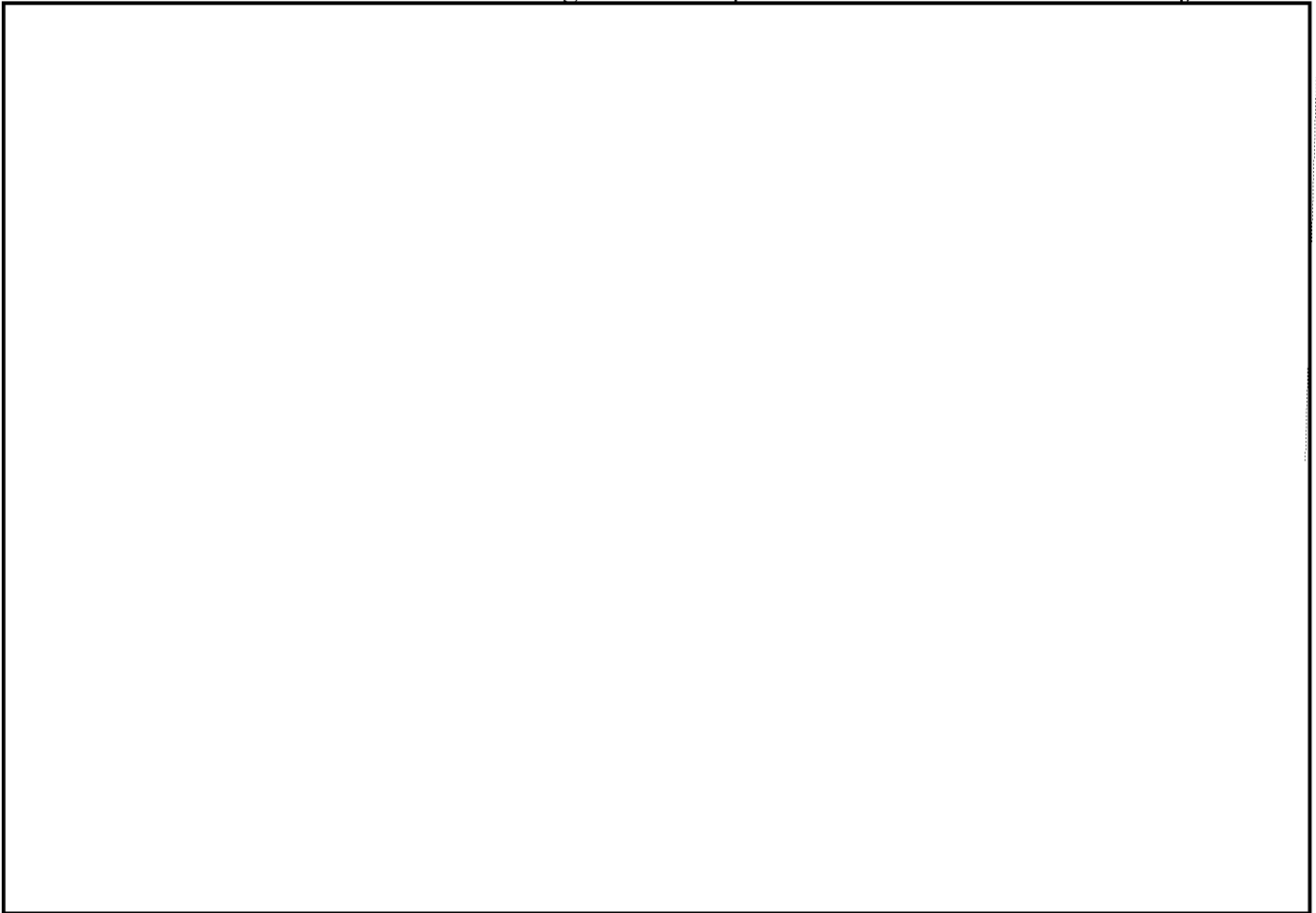
G.14.5.3.1 *(U) RECRUITMENT HAND-OFF TO ANOTHER AGENT*

b1
(S) b3

G.14.5.3.2 *(U) RECRUITMENT FROM THE COVERT APPROACH (No HAND-OFF)*

(S)

b1
(S) b3



G.14.6 (U) [redacted] *IN RIP TYPE 5*

b7E



(S) b1
b3

G.14.7 (U) *CLOSING A RIP TYPE 5*

(U//~~FOUO~~) A RIP Type 5 must be closed, via EC to the subfile, with SSA approval.

G.14.8 ***(U) DECONFLICTION GUIDANCE***

(S) [Redacted]

b1
b3

G.14.9 ***(U) STATUS AS A POLICY EXCEPTION***

(S) [Redacted]

UNCLASSIFIED – ~~FOR OFFICIAL USE ONLY~~
Domestic Investigations and Operations Guide

H APPENDIX H: (U) PRE-TITLE III ELECTRONIC SURVEILLANCE (ELSUR) SEARCH POLICY

H.1 (U) SCOPE

(U) 18 U.S.C. § 2518(1) (e) requires that each application for an order to intercept wire, oral, or electronic communications (hereinafter “Title III”) contain a statement describing all previous applications for Title III surveillance of the same persons, facilities, or places named in the current application. The below policy is designed to conform with this statutory requirement, clarify any past confusion, and address the effects on the previous search policy resulting from the recent elimination of the requirement for an agency Action Memorandum by the Office of Enforcement Operations (OEO).

H.1.1 (U) COMPLIANCE WITH THE PREVIOUS APPLICATION PROVISION

(U) 18 U.S.C. § 2518(1) (e) requires that each application for an order to intercept wire, oral, or electronic communications (hereinafter “Title III”) contain a statement describing all previous applications for Title III surveillance of the same persons, facilities, or places named in the current application. Although a failure to comply with § 2518(1) (e) will not always result in suppression of evidence, deliberate noncompliance likely will.

(U) To comply with this requirement, FBI search policy requires that a “search,” i.e., an automated indices search, of the FBI’s [REDACTED] system be conducted prior to filing a Title III affidavit and application with the court. To assist field offices in conducting appropriate searches, the following guidelines are provided.

b7E

H.1.1.1 (U) WHEN TO SEARCH

- A) (U) ELSUR SEARCHES: ELSUR searches for both sensitive and nonsensitive Title IIIs, including all original, extension, and renewal applications⁵³, must be conducted not more than 45 calendar days prior to the date the application and affidavit are filed with the court.
- B) (U) Any of the persons, facilities, and/or places named in an extension or renewal application and affidavit which have been the subject of a previous search conducted not more than 45 calendar days prior to the date the application and affidavit are filed with the court need not be searched again.

(U) If an individual named by a partial name, nickname, street name, and/or code name in a previous application is subsequently identified by at least a first initial and a last name, a search must be conducted for the now-identified individual prior to seeking any new application naming that person.

H.1.1.2 (U) HOW TO SEARCH

(U) The [REDACTED] must be searched for previously submitted Title III applications to intercept communications involving any of the persons, facilities, and/or places specified in the current Title III application.

⁵³ This requirement also applies to what is sometimes referred to as a “spin-off” Title III which is actually a new application to begin surveillance at or of additional facilities arising from an existing investigation in which one or more Title IIIs have already been authorized. As such “spin-off” Title IIIs are considered to be an “original” request, even though some or all of the named persons are also named in the prior Title III(s).

UNCLASSIFIED – ~~FOR OFFICIAL USE ONLY~~
Domestic Investigations and Operations Guide

- A) (U) **PRIOR APPLICATIONS**: Searches are required only for previously submitted applications. There is no obligation to search for prior interceptions. The ELSUR search will provide records of the persons, facilities, and/or places named in prior applications filed by the FBI and other federal law enforcement agencies named in the request. Any prior applications identified must be set forth in the affidavit in support of the new application._

H.1.1.2.1 (U) **PERSONS**

(U) In submitting a Pre-Title III ELSUR Search Request, FD-940 , list the true names or best known names of individuals for whom there is probable cause to believe that: (1) they are involved in the specified criminal activity, or (2) their criminal communications are expected to be intercepted over the target facility or within the target premises.⁵⁴ These individuals are often identified in the application and affidavit as the “Target Subjects,” “Target Violators,” and/or “Target Interceptees.”

- A) (U) A minimum of a first initial and last name is required for an search. Biographical data such as date of birth, FBI Number, and/or Social Security Account Number, if known, must be included in the search request, even if not listed in the affidavit. Aliases, partial names, nicknames, street names, and/or code names may also be included as further identifying information on the FD-940. However, they will only be searched if they otherwise meet minimum ELSUR search requirements. For example, if an alias is a full name alias, it must be included and will be searched (i.e., John Smith a/k/a “William Johnson” or William Smith a/k/a “Liam Smith”). However, if the subject is identified as John Smith a/k/a “Big Buddy,” “Big Buddy” may be included as further identifying information, but will not be the subject of a separate ELSUR search.
- B) (U) Persons not fully identified by at least a first initial and a last name who are identified in the application and affidavit as “John Doe,” “Jane Doe,” or “FNU LNU” need not be the subject of a pre-Title III ELSUR search. For example, FNU LNU a/k/a “El Jefe” need not be included in an ELSUR search, or listed in the FD-940 search request.
- C) (U) A search of the must be conducted for the subscriber or service provider of the target facility only if the subscriber or service provider is believed to be involved in the specified criminal offense(s).
- D) (U) Any additional persons, facilities, and/or places mentioned in the affidavit, **but not also specified in the application as a person, facility, and/or place for which authorization to intercept is being sought**, need not be searched or listed in the FD-940 (Pre-Title III ELSUR Search Request).

b7E

H.1.1.2.2 (U) **FACILITY**

(U) List available numeric and/or alphanumeric values directly associated with the targeted device, equipment, or instrument over or from which the subjects are communicating (e.g., a telephone, pager, computer, etc.), and over or from which interceptions are being sought. Such values may include, but are not limited to, the telephone number of a land line phone, cell phone, or pager, Personal Identification Number (PIN), Cap Code, Electronic Serial Number (ESN), International Mobile Subscriber Identity (IMSI) Number, International Mobile Equipment Identifier (IMEI) Number, and/or Internet account information (including but not limited to screen name, online identity, ICQ number, and/or IP address).

⁵⁴ (U) All individuals listed in the application and affidavit as being involved in the specified criminal activity should be searched in

Domestic Investigations and Operations Guide

- A) (U) Names of businesses, organizations, or agencies must be searched only if there is probable cause to believe the business, organization, or agency is culpable in the specified criminal offense(s).
- B) (U) Searches need not be conducted for telephone numbers or other facilities subscribed to, leased, or owned by the FBI for use in the investigation for which the ELSUR is being sought.
- C) (U) Any additional facilities mentioned in the affidavit, but not also specified in the application as a person, facility, and/or place for which authorization to intercept is being sought, need not be searched or listed in the FD-940 (Pre-Title III ELSUR Search Request). For example, telephone numbers identified as calling or being called by the Target Telephone, and set out in the pen register section of a Title III affidavit need not be the subject of a pre-Title III ELSUR search.

H.1.1.2.3 (U) *PLACES*

(U) List: (1) each address of a targeted landline phone or computer terminal which will be subject to the Title III order, and/or (2) [REDACTED]

b7E

[REDACTED]
[REDACTED] Do not include addresses of subscribers or proprietors of mobile installations such as cell phones, pagers, vehicles, boats or planes, etc.

H.1.1.2.4 (U) *ADDITIONS*

(U) Persons, facilities, and/or places added to an application and affidavit during the course of the review process and after the initial pre-Title III search request must be searched prior to submitting the affidavit to the court.⁵⁵

H.1.1.3 (U) *WHERE TO SEARCH*

(U) A search of the FBI's [REDACTED] must be conducted for each item named in the search request. DOJ policy requires a search of the Drug Enforcement Administration (DEA) and Immigration and Customs Enforcement (ICE) [REDACTED] for all Title 21 predicate offenses. As a matter of FBI policy, a DEA and ICE ELSUR search is automatically conducted by FBIHQ for all [REDACTED] and [REDACTED] investigative classifications, and any other application involving a Title 21 offense.

b7E

- A) (U) The [REDACTED] of any other federal, state, or local law enforcement agency that is actively participating in a joint investigation (as opposed to mere task force participation) or as to which there is reason to believe may have previously sought to intercept wire, oral, or electronic communications involving any of the persons, facilities, and/or places specified in the instant application, should be searched. Where a search of state and/or local law enforcement ELSUR records is requested, the request should include a point of contact from the outside agency, if known.

⁵⁵ Occasionally, during the course of their review, DOJ's Office of Enforcement Operations, will suggest that an additional name be added as a "Target Subject" (or similar) in a Title III application and affidavit prior to the grant of DOJ approval. If that name is added, it must be searched through [REDACTED] prior to submitting the affidavit to the court.

Domestic Investigations and Operations Guide

- B) (U) If there is reason to believe that any of the persons, facilities, and/or places specified in the current application have been the target of Title III electronic surveillance by another federal agency, that agency must be requested to conduct an ELSUR search of its records.

H.1.1.4 (U) HOW TO INITIATE A SEARCH REQUEST

(U) The FD-940 (Pre-Title III ELSUR Search Request) is used for requesting pre-Title III ELSUR searches of the of the FBI and any other federal, state, or local law enforcement agency. The form is designed to assist personnel requesting a search by guiding them through the process. Use of the form will ensure search requirements are met.

b7E

(U) If an emergency situation exists, as defined by 18 U.S.C. § 2518(7), an ELSUR search may be requested telephonically to the field office EOT.

H.1.1.4.1 (U) SEARCH PROCEDURE

(U) The EOT will conduct a search of the for records of “previous applications only” or “all records” as specified in the FD-940. Records retrieved as a result of the search will be furnished to the requesting Agent. If intercept records are requested for any or all of the persons, facilities, and/or places named in the FD-940, intercept records which relate to unclassified criminal matters will be provided in their entirety to the requesting Agent and documented in the appropriate case file location(s).

(U) It is the responsibility of the requesting Agent to use reasonable efforts to determine whether the persons, facilities, and/or places identified in the search are the same persons, facilities, and/or places specified in the current application. If there is reason to believe they are, offices identified as having filed previous applications must be contacted and the EOT in that office must be asked to review the pertinent investigative file(s) to determine whether the persons, facilities, and/or places identified in the search are, in fact, the same as those specified in the current application.

(U) It is not necessary to contact other offices regarding common names for which no special identifying data is available unless there is reason to believe there is a nexus between the current investigation and the investigation conducted by the other field offices.

(U) Documentation confirming the conduct of all pre-Title III ELSUR searches must be electronically placed in the appropriate investigative file.

H.1.1.5 (U) WHAT TO SAY

- A) (U) NO PREVIOUS APPLICATIONS: Sample proposed affidavit language when no previous applications have been filed:
- 1) (U) “Based upon a search of the records of the Federal Bureau of Investigation (and any other agency requested), no previous applications have been filed for an order authorizing the interception of wire, oral, or electronic communications involving any of the persons, facilities, and/or places specified herein for which authorization to intercept is being sought.”
- B) (U) PREVIOUS APPLICATIONS:
- 1) (U) If there was a previous application, include all relevant information concerning such application in the affidavit in support of the current application. Identify the persons, facilities, and/or places named, the method(s) of interception sought, the date the order was granted or denied, the court that issued or denied the order, the name of the authorizing or

Domestic Investigations and Operations Guide

denying judge (if known), and the relevance, if any, of the previous application to the current investigation.

- 2) (U) Sample proposed affidavit language when previous applications have been filed: “John Doe was named in a previous application for an order authorizing the interception of wire and electronic communications. The order was signed on (date), by U.S. District Judge (name), of the District of (State), authorizing the interceptions for a period of thirty (30) days. An extension of the order was signed by Judge (name) on (date), authorizing the continued interception for an additional 30-day period.” (Include relevance, if any, of the previous applications to the current investigation).

H.1.1.6 (U) DOCUMENTATION

- A) (U) Agents must provide a copy of the following to the field office’s ELSUR Operations Technician (EOT):
- 1) (U) executed affidavit, application, and order;
 - 2) (U) completed CDC Checklist (FD-926);
 - 3) (U) EC signed by the appropriate approving official (SAC or designee or appropriate HQ official) documenting approval to seek court authorization for the Title III application; and
 - 4) (U) DOJ Memorandum directed to the AUSA entitled “Authorization for Interception Order Application.”
- B) (U) The EOT and the ELSUR supervisor are responsible for confirming that ELSUR searches were properly conducted as set forth in the final applications submitted to the court. Because this review is not conducted until after the application and order have been submitted to the court, the SA and SSA are responsible for verifying that all required ELSUR searches have been conducted prior to submission of the application and affidavit to the court. Within 10 calendar days of obtaining court authority for the original and all extensions/renewals of the Title III intercept, the case agent must also submit to the EOT a signed copy of the: (i) affidavit, (ii) application, (iii) order, (iv) copy of the CDC Title III Checklist (FD-926); (v) SAC approval EC; and (vi) a copy of the DOJ Authorizing Memo. The EOT will be responsible for transmitting a copy of these documents to the Order Management Group in OTD. The Order Management Group will be responsible for indexing and uploading these documents into the [REDACTED] These requirements also apply to the joint Title III operations discussed in section 18.7.2.13.
- C) (U) Form FD-940 (Pre Title III ELSUR Search Request) must be used when requesting a search of any federal, state, or local law enforcement agency’s [REDACTED], including the FBI’s.
- D) (U) All requests for ELSUR searches must be electronically placed in the corresponding investigative file and submitted with adequate time for the EOT to conduct the search and document the results. It is the responsibility of the affiant and the affiant’s supervisor to ensure that all ELSUR checks have been properly completed prior to submission of the application and affidavit to the court.

b7E

H.1.1.7 ROLE OF SPECIAL OPERATIONS DIVISION AND [REDACTED]

b7E

[REDACTED] SEARCHES

(U//FOUO) [REDACTED]



(U//~~FOUO~~)



H.1.1.8 (U) **ADDITIONAL GUIDANCE AND EXAMPLES**

(U) Additional guidance regarding the conduct of pre-Title III ELSUR searches, including examples applying the policy set forth above, can be found at the [DIOG Resources site](#).

This Page is Intentionally Blank

UNCLASSIFIED – ~~FOR OFFICIAL USE ONLY~~
Domestic Investigations and Operations Guide

I APPENDIX I: (U) ACCESSING STUDENT RECORDS MAINTAINED BY AN EDUCATIONAL INSTITUTION ("BUCKLEY AMENDMENT")

I.1 (U) SUMMARY

(U) The Family Educational Rights and Privacy Act (FERPA) of 1974 (20 U.S.C. § 1232g, as amended by Public Law 107-56 (USA Patriot Act)), commonly referred to as the "Buckley Amendment," restricts the ability of educational agencies or institutions (collectively "schools") to release educational records or personally identifiable information contained in such records without the consent of the student or the student's parent.

(U) FERPA defines "education records" as those records, files, documents and other materials which:

- A) (U) contain information directly related to a student; and
- B) (U) are maintained by an educational agency or institution or by a person acting for such agency or institution. (20 U.S.C. § 1232g(a)(4)(A)(i)).

(U//~~FOUO~~) If operationally feasible, FBI employees should request the consent of the student or parent, as appropriate, in order to obtain covered records. During an Assessment, the FBI may ask school officials to provide certain information without the consent of the student or parent (see Section 18.5.6); during a Predicated Investigation, the FBI may compel production of education records, as set forth below.

I.2 (U//~~FOUO~~) ACCESSING STUDENT INFORMATION OR RECORDS DURING AN ASSESSMENT

(U//~~FOUO~~) During an Assessment, FBI employees may seek **voluntary disclosure** of certain student records and information about students from schools without the consent of the student or parent.

I.2.1 (U) *DIRECTORY INFORMATION*

(U//~~FOUO~~) "Directory information" is information contained in an education record of a student "that would not generally be considered harmful or an invasion of privacy." (34 C.F.R. § 99.3) Specifically, "directory information" includes, but is not limited to: the student's name, address, telephone listing, electronic mail address, photograph, date and place of birth, major field of study, dates of attendance, grade level, enrollment status (e.g., undergraduate or graduate, full-time or part-time), participation in officially recognized activities or sports, weight and height of members of athletic teams, degrees, honors and awards received, and the most recent educational agency or institution attended. A school may disclose "directory information" from its records without prior consent if: (1) it has a directory information policy to disclose such information and (2) it has provided its students notice of the policy and the opportunity to opt out of having "directory information" disclosed. (See 34 C.F.R. § 99.37)

(U//~~FOUO~~) The scope of information that can be released as directory information may be narrowed by the school. For instance, if a college chooses not to categorize students' names and addresses as directory information, it must not voluntarily disclose such information to the FBI

(*Krauss v. Nassau Community College*, 469 N.Y.S. 2d 553 (N.Y. Sup. 1983)). Schools are also required to afford students (or parents, if the student is under 18) the opportunity to prohibit the release of directory information without their prior consent (or a court order). *Note*: the Buckley Amendment *permits* schools to release directory information (absent an objection from the student); it does *not require* them to do so. Directory information may be sought orally or in writing.

I.2.2 (U) *OBSERVATIONS*

(U//~~FOUO~~) FERPA governs the release of educational records. It does not govern the release of information gathered by a school official, based on his or her own observations. Accordingly, notwithstanding Buckley, a school official may disclose activity or behavior observed by the official.

I.2.3 (U) *LAW ENFORCEMENT UNIT RECORDS*

(U//~~FOUO~~) Under FERPA, schools may disclose information from “law enforcement unit records” without the consent of the parent or student. This exemption is limited to records that a law enforcement unit of a school creates and maintains for a law enforcement purpose. “Law enforcement record” is narrowly defined as a record that is: (i) created by the law enforcement unit; (ii) created for a law enforcement purpose; and (iii) maintained by the law enforcement unit. (34 C.F.R. § 99.8(b)) If another component of the school discloses a student education record to the school’s law enforcement unit, that record is not a “law enforcement unit record” because it was not *created* by the law enforcement unit. Thus, a law enforcement unit cannot disclose, without student consent, information obtained from education records created by other component of the school, even if the record has been shared with the law enforcement unit.

I.2.4 (U) *HEALTH OR SAFETY EMERGENCY*

(U//~~FOUO~~) FERPA does not restrict the disclosure of educational records in connection with a health or safety emergency. The regulations provide that schools may disclose information from an education record “to appropriate parties in connection with an emergency if knowledge of the information is necessary to protect the health or safety of the student or other individuals” and that the exception is to be “strictly construed.” As is the case with other emergency disclosure provisions (see 18 U.S.C. § 2702), it is up to the school to determine in the first instance whether disclosure is necessary to protect the health or safety of the student or another individual. If it makes that determination, it is permitted to disclose educational records voluntarily and without the consent of the student or parent.

I.2.5 (U) *NON-STUDENTS*

(U//~~FOUO~~) FERPA governs records of “students.” A “student” is defined as a person on whom a school maintains educational records or personally identifiable information but does not include someone who has not attended that school. Files retained on rejected applicants may be provided without prior permission or notification. (*Tarka v. Franklin*, 891 F.2d 102 (5th Cir. 1989))

I.3 (U//~~FOUO~~) ACCESSING STUDENT INFORMATION OR RECORDS IN PREDICATED INVESTIGATIONS

(U//~~FOUO~~) In addition to seeking voluntary production of records that can be voluntarily produced (see I.2 above), in a Predicated Investigation, FBI employees may **compel production** of education records without notice to the student or the student's parents as follows:

I.3.1 (U) *FEDERAL GRAND JURY SUBPOENA*

(U//~~FOUO~~) Schools shall disclose education records in response to a federal grand jury subpoena. In addition, the court may order the institution not to disclose to anyone the existence or contents of the subpoena or the institution's response. If the court so orders, then neither the prior notification requirements of 34 C.F.R. § 99.31(a)(9) nor the recordation requirements at 34 C.F.R. § 99.32 would apply (see DIOG Section 18.6.5).

I.3.2 (U) *ADMINISTRATIVE SUBPOENAS*

(U//~~FOUO~~) Schools may disclose education records in response to an administrative subpoena. Administrative subpoenas may be issued in narcotics investigations (see DIOG Section 18.6.4.3.2.1), sexual exploitation or abuse of children investigations (see DIOG Section 18.6.4.3.2.2), and health care fraud investigations (see DIOG Section 18.6.4.3.2.3). As with federal grand jury subpoenas, the issuing agency may, for good cause shown, direct the school not to disclose the existence or contents of the subpoena or the institution's response. If the subpoena includes a nondisclosure directive, the school is permitted to request a copy of the good cause determination.

I.3.3 (U) *FISA ORDER FOR BUSINESS RECORDS*

(U//~~FOUO~~) See DIOG Section 18.6.7.

I.3.4 (U) *EX PARTE ORDERS*

(U//~~FOUO~~) The USA Patriot Act amended FERPA to permit schools to disclose personally identifiable information from the student's education records to the Attorney General or his designee without the consent or knowledge of the student or parent in response to an *ex parte* order issued in connection with a terrorism investigation. Such disclosures are also exempt from the Buckley Act requirements that disclosure of information from a student's records be documented in the student's file.

This Page is Intentionally Blank

UNCLASSIFIED – ~~FOR OFFICIAL USE ONLY~~
Domestic Investigations and Operations Guide

J APPENDIX J: (U) CASE FILE MANAGEMENT AND INDEXING

J.1 (U) INVESTIGATIVE FILE MANAGEMENT

J.1.1 (U) OFFICE OF ORIGIN (OO)

(U//~~FOUO~~) Generally, the Office of Origin (OO) is determined by:

- A) (U//~~FOUO~~) The residence, location or destination of the subject of the investigation;
- B) (U//~~FOUO~~) The office in which a complaint is first received;
- C) (U//~~FOUO~~) The office designated by FBIHQ as OO in any investigation;
- D) (U//~~FOUO~~) The office in which the Foreign Police Cooperation investigation is opened (163 classification);
- E) (U//~~FOUO~~) The office in which the Domestic Police Cooperation investigation is opened (343 classification);
- F) (U//~~FOUO~~) The office in which the recovery of the vehicle occurred in an Interstate Transportation of Stolen Motor Vehicles (ITSMV) investigations;
- G) (U//~~FOUO~~) The office in which the contempt of court occurred;
- H) (U//~~FOUO~~) The office in which there is a violation of an order, judgment, or decree issued from any judicial district in an FBI civil Racketeer Influenced and Corrupt Organizations (RICO) investigation;
- I) (U//~~FOUO~~) The office in which the subject was convicted in investigations involving parole, probation, and mandatory release violators;
- J) (U//~~FOUO~~) The office in which the escape occurred, in Escaped Federal Prisoner and escaped deserter investigations;
- K) (U//~~FOUO~~) The New York Field Office in courier investigations;
- L) (U//~~FOUO~~) FBIHQ in all applicant, Background Investigation - Pardon Attorney's Office (73 classification) investigations;
- M) (U//~~FOUO~~) FBIHQ in OPM security referral (140A and 140C classification) investigations;
- N) (U//~~FOUO~~) FBIHQ, Counterterrorism Division (CTD), Counterterrorism Watch Unit in all Counterterrorism Major Cases (900 classification);
- O) (U//~~FOUO~~) FBIHQ, Critical Incident Response Group (CIRG) in all National Center for the Analysis of Violent Crime (NCAVC) cases (252A through 252E classifications); and
- P) (U//~~FOUO~~) FBIHQ, Office of Professional Responsibility (OPR) in OPR investigations (263 classification).

(U//~~FOUO~~) When special circumstances exist, however, the origin may be assumed by the field office which has the most compelling interest. Uncertainties and disagreements must be resolved by the appropriate FBIHQ operational division.

J.1.2 (U) *INVESTIGATIVE LEADS AND LEAD OFFICE (LO)*

(U//~~FOUO~~) Leads are sent by EC, or a Lead Request document, to offices and assigned to individuals/organizations in order to aid investigations. When the OO sets a lead to another office, that office is considered a Lead Office (LO).

(U//~~FOUO~~) There are only two types of investigative leads: “Action Required” and “Information Only.”

J.1.2.1 (U) *ACTION REQUIRED LEAD*

(U//~~FOUO~~) An action required lead must be used if the sending office requires the receiving LO to take some type of investigative action.

(U//~~FOUO~~) An action required lead may only be set by EC out of an open investigative file, including an:

- A) (U) Assessment file, including a zero sub-assessment file;
- B) (U) Predicated Investigation file;
- C) (U) pending inactive investigation file; or
- D) (U) unaddressed work file.

(U//~~FOUO~~) An action required lead cannot be set out of a closed investigative file, a zero (0) or double zero (00) file.

(U//~~FOUO~~) An action required lead must be assigned, and it must be covered before the underlying investigation has been completed/closed.

J.1.2.2 (U) *INFORMATION ONLY LEAD*

(U//~~FOUO~~) An information only lead must be used when no specific action is required or necessary from the receiving LO.

(U//~~FOUO~~) An information only lead may be set by EC out of an opened or closed investigative file, including a:

- A) (U) zero (0) file;
- B) (U) double zero (00) file;
- C) (U) Assessment file, including a zero sub-assessment file;
- D) (U) Predicated Investigation file;
- E) (U) pending inactive investigation file; or
- F) (U) unaddressed work file.

(U//~~FOUO~~) An information only lead does not have to be assigned in order to be covered, and they can be covered while they are in the "Set" status.

J.1.3 (U) *OFFICE OF ORIGIN’S SUPERVISION OF CASES*

(U//~~FOUO~~) The OO is responsible for proper supervision of Assessments and investigations in its own territory and being conducted in a LO. The FBI employee, usually an FBI Special Agent, to whom an investigation is assigned, is often referred to as the “Case Agent.” An FBI employee

UNCLASSIFIED – ~~FOR OFFICIAL USE ONLY~~
Domestic Investigations and Operations Guide

is personally responsible for ensuring all logical investigation is initiated without undue delay, whether the employee is assigned in the OO or in an LO; this includes setting forth [REDACTED] [REDACTED] leads as appropriate for other offices or other FBI employees in his/her own office. The OO Case Agent has overall responsibility for supervision of the investigation. When an LO has a delayed or delinquent investigation, it is the responsibility of the OO Case Agent to notify the LO (orally or in writing by email or EC, depending on the urgency of the situation) of its delinquency.

b7E

(U) Investigative information that may be within another field office's AOR can generally be obtained by setting an investigative lead to that field office. However, investigative circumstances may require employees to travel to another office's AOR to conduct investigative activity. In such circumstances, an employee, with the approval of [REDACTED] and the prior concurrence of the [REDACTED] may enter that office's AOR and conduct the necessary investigative activity (e.g. interview). However, if unplanned investigative activities or exigent circumstances prevent an employee from obtaining advance [REDACTED] approval and advance [REDACTED] concurrence before entering another field office's AOR, notification should be made as soon as practicable to the [REDACTED] and [REDACTED] in the other office's AOR, including the type of investigative activity(s) that occurred and the circumstances that made obtaining prior approval and concurrence unfeasible.

b7E

J.1.4 (U) INVESTIGATION AND OTHER FILES

(U//~~FOUO~~) There are several types of non-investigative files used in the FBI, including zero files, double zero files, administrative files, and control files. Additionally, there are several types of investigative files used in the FBI, including [REDACTED] Preliminary Investigation files, Full Investigation files, Full Enterprise Investigation files, positive foreign intelligence Full Investigation files, and unaddressed work files. Additionally, investigative files may have sub-files, named as specified in the DIOG and RMD policy. FBI files may be opened, closed, or placed in pending inactive status as specified below. Note that in each of these files, all communications related to previous communication must note the existing communication's FBI's central recordkeeping system serial numbers in the reference fields.

b7E

(U//~~FOUO~~) Certain records may be restricted based on the classification of the records, e.g., on the sensitivity of the investigation. See the Automatic Restriction of Access to Data in FBI Case Support Systems Based on Standard File Classification Designators Policy Directive, 0243D, dated October 13, 2009.

(U//~~FOUO~~) The types of files are:

J.1.4.1 (U) ZERO "O" FILES

b7E

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

J.1.1.4.2 (U) DOUBLE ZERO “OO” FILES

(U//~~FOUO~~) Double Zero files may be opened in all file classifications. Double Zero files may contain documentation, such as instructions, statutes, and decisions applicable to the classification, that do not require investigation. The documents contained within a double zero file must be electronically placed into the file. [REDACTED]

b7E

J.1.1.4.3 (U) ADMINISTRATIVE “A” FILES

(U//~~FOUO~~) Administrative files may be used only for administrative purposes; they cannot be used for investigative purposes. Administrative files may be used for documenting non-investigative matters, such as training matters (1 classification), administrative matters (319 classification), personnel files (67 classification), etc. **Note: Investigative activity must not be conducted out of an administrative file.** Administrative files are designated with the letter "A" before the case number, e.g., 319X-HQ-A12345.

(U//~~FOUO~~) FBI BUCAR accident files [REDACTED] and civil litigation or claim matters [REDACTED] are permitted to retain investigative information related to a BUCAR accident or civil matter as an exception to the general rule prohibiting the use of investigative activity in administrative files. The basis for permitting this exception is the investigative document, generally a witness interview on an FD-302 for the car accident, or taking a witness statement on an FD-302 in the civil matter, is intended to support the administrative functions of the organization and is not obtained in support of a law enforcement investigation or an intelligence collection function.

b7E

(U//~~FOUO~~) Information Only (non-investigative) Leads may be assigned out of administrative files. When referring to an administrative file in communications, the file number must include the letter "A" before the case number to indicate the file is an administrative file.

J.1.1.4.4 (U) CONTROL “C” FILES

(U//~~FOUO~~) Control files are separate files established for the purpose of managing programs. Control files may be opened in all file classifications.

(U//~~FOUO~~) Control files may be used only for documenting program management functions and communications, technical or expert assistance to another law enforcement or intelligence agency, or other managerial functions. Program management functions may include liaison contacts, training exercises, training received/provided, written intelligence products⁵⁶ that are prepared for program management purposes, etc. **Note: Investigative activity must not be**

⁵⁶ (U//~~FOUO~~) [REDACTED]
[REDACTED]

b7E

conducted⁵⁷ out of a control file. Control files are designated with the letter “C” before the case number, e.g., 29B-NF-C4456.

(U//~~FOUO~~) Information Only (non-investigative) Leads can be assigned out of control files. When referring to the file number of a control file in communications, the file number must include the letter "C" before the case number to indicate the file is a control file. The [redacted] control file must follow the [redacted] guidance on setting leads.

b7E

J.1.4.5 (U) INVESTIGATIVE FILES

J.1.4.5.1 (U) ASSESSMENT FILES

J.1.4.5.1.1

(U) [redacted]
[redacted]

(U//~~FOUO~~) [redacted] Type 1 &
2 Assessments [redacted]

[redacted] When completing the FD-71, Guardian or Assessment file lead for an Assessment involving a sensitive investigative matter, [redacted]

b7E

(U//~~FOUO~~) [redacted] can be set when using a [redacted]

(U//~~FOUO~~) Guardian may be used only for documenting those Assessments described in DIOG Section 5.6.3.1 regarding [redacted]

[redacted] The FD-71 or EC must be used to document all other Assessments, including criminal, counterintelligence, and non-terrorism WMD and Cyber. Guardian, the FD-71, the EC and [redacted] Lead Request form provide the ability to set action leads.

J.1.4.5.1.2 (U) INVESTIGATIVE CLASSIFICATION ASSESSMENT FILES (FOR TYPE 3, 4 AND 6 ASSESSMENTS) AND POTENTIAL CHS FILES (FOR TYPE 5 ASSESSMENTS)

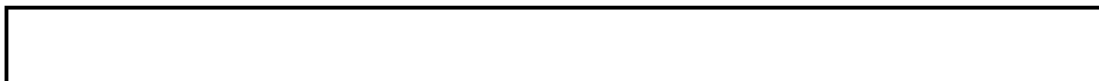
(U//~~FOUO~~) See DIOG Section 5 for the appropriate investigative file classification to be used when opening a Type 3, 4, 5, or 6 Assessment file.

(U//~~FOUO~~) Because these Assessments require prior supervisory approval, the file must begin with an opening EC (DIOG Section 5.6.3.2 through 5.6.3.5 type Assessments and DIOG Section 5.7 as discussed above). [redacted]

b7E

⁵⁷ (U) [redacted]

b7E



b7E

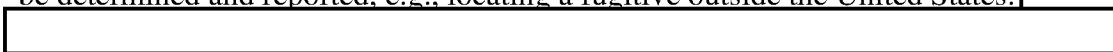
J.1.4.5.2 (U) *PRELIMINARY AND FULL INVESTIGATION (PREDICATED) FILES*

(U//~~FOUO~~) A Preliminary Investigation, Full Investigation, Full Enterprise Investigation, and Full Positive Foreign Intelligence Investigation must be opened as discussed in DIOG Sections 6, 7, 8, and 9, respectively. Investigative information related to these investigations must be placed in the investigative main file or sub-file, spun-off, or referred to another agency as authorized.

J.1.4.5.3 (U) *PENDING/INACTIVE FULL INVESTIGATION FILES*

(U//~~FOUO~~) A Full Investigation may be placed in a pending-inactive status when all investigation has been completed and only prosecutive action or other disposition remains to be determined and reported, e.g., locating a fugitive outside the United States. 

b7E



 A pending-inactive Full Investigation may be assigned to investigative personnel or a squad/unit.

J.1.4.5.4 (U) *UNADDRESSED WORK FILES*

(U//~~FOUO~~) 

b7E



(U//~~FOUO~~) 



(U//~~FOUO~~) 



(U//~~FOUO~~) The FD-71 and an Assessment file provide a mechanism to assign an Assessment to an Unaddressed Work file. In the FD-71, the Supervisor must select a reason for assigning the matter to the Unaddressed Work file and choose the appropriate classification. Upon serializing the FD-71, a new Unaddressed Work file will be opened. Guardian (FD-71a) does not have an “Unaddressed Work” option because Guardian leads cannot be placed in an Unaddressed Work status.

J.1.4.5.5 (U) SPIN OFF INVESTIGATION FILES

(U//~~FOUO~~) A spin-off investigation originates from an existing investigation. The spin-off investigation must have all the elements required to establish it as a separate investigation within the appropriate investigative classification.

J.1.5 (U) SUB-FILES

(U) The below standardized sub-file names must be used when creating sub-files to document the investigative or administrative activity described. However, other sub-file names may be utilized to document relevant investigative or administrative activities not specifically addressed by the following standardized sub-file list:

SUB-FILES		
Sub-file Name	DIOG Required	RMD and Other Policy
ADMIN	---	Administrative Matters
AFF	---	Affidavits
ANA	---	Analytical (not including Written Intelligence Products – see DIOG required INTELPRODS sub-file below)
BC	---	Background Information Re Subject (FD-160; FD-125; FD-809)
BIO	---	Biographical Info (NCIC; CLETS; DMV)
CART	---	Computer Analysis Response Team
CRIM	---	Criminal Records
CCTV	---	Closed Circuit Television/Video Surveillance
CE	---	Case Expenditures
CD	---	Classified Documents / Info
CRT	---	Court Orders

UNCLASSIFIED – ~~FOR OFFICIAL USE ONLY~~
Domestic Investigations and Operations Guide

---		---
EMAIL	---	E-Mail
FA	---	Financial Analysis
FF	---	Forfeiture

FISUR	---	Physical Surveillance Logs
FTP	---	Federal Taxpayer Information
FUG	---	Fugitives
GJ	Federal Grand Jury Subpoenas and Materials	---
INTEL	---	Intelligence

b7E

b7E

UNCLASSIFIED – ~~FOR OFFICIAL USE ONLY~~
Domestic Investigations and Operations Guide

INTELPRODS	Written Intelligence Products	---
LAB	---	Laboratory / Latent Reports
LEADS	---	Leads
LEGAL	---	Legal Documents
LIAISON	---	Liaison and FD-999s
LOC	---	Locations
MC	---	Mail Covers (Criminal and National Security)
MEDIA	---	Media Reports
MISC	---	Miscellaneous
NC	---	Newspaper Clippings and Press Releases



b7E

PEN	Pen Register / Trap And Trace	---
PH	---	Photographs (paper copies only)
PR	---	Police Reports
RECORDS	---	Bank / Tax / Financial Records
REPORTS	---	Reports
S	---	Suspects / Subjects
SBP	Administrative Subpoenas	---
SURV	---	Surveillance
SW	---	Search Warrants (Criminal)
T3	---	Consensual Monitoring Calls / Title III
TC	---	Trash Covers
TEL	---	Telephone Subscriber / Toll Information / Trap & Trace Calls

UNCLASSIFIED ~~—FOR OFFICIAL USE ONLY—~~
Domestic Investigations and Operations Guide

TERRFIN	---	Terrorist Financing-Related Information
TS	---	Top Secret Documents
TRANS	---	Transcripts
TVL	---	Travel
UCO	---	Undercover Operations (Group I and Group II UCOs)
VOU	---	Vouchers
1A	---	1A Exhibit
1B	---	Evidence Chain of Custody (FD-192s or successor form)
1C	---	Bulky, Non-Evidence (FD-192s or successor form)
1D	---	ELSUR
FD302	---	FD-302s (and other testimonial documents)
FD515	---	Accomplishments (FD-515s or successor documents)
FD542	---	Accomplishments (FD-542s or successor documents)

(U) When more than one sub-file is needed for a specific category, sequential numbers are to be used adjacent to the described sub-file name. For example, three forfeiture sub-files would be named: FF1, FF2, FF3, etc.

J.2 (U) INDEXING - THE ROLE OF INDEXING IN THE MANAGEMENT OF FBI INFORMATION

(U//~~FOUO~~) The text of FBI-generated records (including but not limited to FD-65, FD-786, and non-transitory electronic mail (e-mail) records) must be imported into the FBI's central recordkeeping system to be searchable, retrievable, and sharable through automated means. A full text search of the FBI's central recordkeeping system identifies only information that is available electronically and does not search for information that may be contained in the FBI's paper records. Regardless of whether a record is imported or created in the FBI's central recordkeeping system, it must be indexed.

(U//~~FOUO~~) The purpose of indexing is to record individual's names; non-individual's names, such as corporations; and property which are relevant to FBI investigations so that this information can be retrieved, if necessary. The most common use of indexed information is to respond to executive branch agencies' request name searches as part of their investigations to determine suitability for employment, trustworthiness for access to classified information and eligibility for certain government benefits. If employees do not properly index names and places

that arise in FBI investigations, the FBI could provide erroneous information to other federal agencies. Further advice about how to index and what should be indexed can be found on the RMD Intranet site.

This Page is Intentionally Blank

~~UNCLASSIFIED – FOR OFFICIAL USE ONLY~~
Domestic Investigations and Operations Guide

K APPENDIX K: (U) REPORTING OF SUSPECTED CHILD ABUSE, NEGLECT AND/OR SEXUAL EXPLOITATION

K.1 (U) REPORTING OF SUSPECTED CHILD ABUSE, NEGLECT AND/OR SEXUAL EXPLOITATION

K.1.1 (U) PURPOSE

(U) In October 2011, the Department of Justice (DOJ) released the updated *2011 Attorney General Guidelines for Victim and Witness Assistance* (the “*Guidelines*”); and in May 2012, released revised *Guidelines*. Among other obligations, the *Guidelines* require DOJ personnel, including FBI personnel, to report suspected child abuse. Special Agents (SAs) and other FBI personnel may encounter suspected child abuse, neglect and/or sexual exploitation during the course of their duties. This policy provides the most recent DOJ/FBI suspected child abuse reporting requirements. “This requirement is in addition to, not in place of, mandatory reporting requirements under state, tribal and federal law with which [FBI Personnel] shall also comply” [*Emphasis added*]. *Guidelines* at Art. III, L.1.c (1).

K.1.2 (U) OBLIGATION TO REPORT

(U) The FBI’s role as a law enforcement agency necessitates several reporting requirements for FBI personnel who have reasonable cause to believe a child is suffering from abuse, neglect and/or sexual exploitation.

(U) While certain FBI employees (e.g. law enforcement personnel and social workers) are defined as mandated reporters under state, tribal and federal law, all FBI employees shall report suspected child abuse, neglect and/or sexual exploitation to the state, local or tribal law enforcement agency or child protective services agency that has jurisdiction to investigate such reports or to protect the child.

K.1.3 (U) REPORTING TO THE APPROPRIATE OFFICIALS

(U) In every case of suspected child abuse, neglect and/or sexual exploitation, an immediate report shall be made to the appropriate state, local or tribal agency with authority to investigate such matters or to protect the child. FBI personnel should consult with the Chief Division Counsel (CDC) or the Office of the General Counsel (OGC) to determine the child abuse reporting laws applicable in their area of responsibility.

(U) Reporting is generally covered by state, local or tribal law and reports shall be made to the agency or entity identified in and in accordance with those laws. However, the report of suspected child abuse should be made by a method best suited to giving immediate notice. Use of a standardized form is encouraged, but shall not take the place of the immediate making of reports by other means when circumstances dictate.

(U) Reports may be made anonymously, although FBI personnel are strongly encouraged to provide sufficient identifying information. Reports are presumed to have been made in good faith and reports are immune from civil and criminal liability arising from the report, unless acting in bad faith.

(U) FBI personnel shall also immediately report suspected child abuse to the FBI's Designated Official in each office. The Designated Official will assist FBI personnel with reporting suspected child abuse, if no direct report is made, and will ensure completion of a 188D-Electronic Communication (188D-EC) to the FBI's Office of Victim Assistance (OVA).

(U) In rare circumstances, reporting may be temporarily delayed upon a determination by an FBI Component Responsible Official. Per the *Guidelines* and FBI implementing policy, the designated FBI Component Responsible Official is the head of the division or office. For Field Divisions the Component Responsible Official is the Special Agent-in-Charge (SAC), or where applicable, the Assistant Director in Charge (ADIC). For FBI Headquarters, the Component Responsible Official is the head of the Division or office (e.g., Assistant Director (AD) or equivalent).

K.1.4 (U) SCOPE OF REPORTING

(U) All cases of suspected child abuse must be reported. A report shall be made even if the information inadvertently comes to the attention of FBI personnel. In cases where there is reason to believe an incident was previously reported or is otherwise being investigated, FBI personnel shall err on the side of caution, and consult with the Designated Official, due to the possibility of there being multiple offenses, victims, and/or perpetrators. If there are any distinguishable elements (e.g. different day, time, or place) from the confirmed previous report and investigation, FBI personnel shall immediately report the new case and any additional information to the state, local or tribal law enforcement agency or child protective services agency that has jurisdiction to investigate such reports or to protect the child.

(U) Certain Indian Country, Special Jurisdiction and crimes against children matters already fall within the primary investigative jurisdiction of the FBI. Suspected child abuse, neglect and/or sexual exploitation in these areas, which are already the subject of an FBI investigation, do not warrant additional reporting unless such reporting is necessary to further protect the child.

K.2 (U) MANDATORY REPORTING LAWS

(U) FBI personnel should refer to their state child abuse reporting laws in cases of suspected child abuse, neglect and/or sexual exploitation. State laws vary substantially. Some states require mandatory reporting of child abuse, neglect and/or sexual exploitation by all persons within their boundaries; others require such reporting only from individuals engaged in expressly listed occupations. Reports of child abuse, neglect and/or sexual exploitation required by state, local or tribal laws shall be made to the agency or entity identified in and in accordance with those laws.

(U) The federal child abuse reporting law mandates certain professionals (including law enforcement personnel and social workers) working on federal land or in a federally operated (or contracted) facility must report suspected child abuse to an investigative agency designated by the Attorney General to receive and investigate such reports. (42 U.S.C. § 13031(a)). Reports of child abuse pursuant to 42 U.S.C. § 13031 shall be made to the local law enforcement agency or local child protective services agency that has jurisdiction to investigate such reports or to protect child abuse victims in the area or facility in question. When no such agency has entered into a formal written agreement with the Attorney General to investigate such reports, the FBI shall receive and investigate such reports. (28 C.F.R. § 81.3 (2010)).

(U) Reporting child abuse in Indian Country is governed by 18 U.S.C. §1169 (2006) and 25 U.S.C. §3203 (2006). Covered professionals shall report suspected cases of child abuse to the federal, state, or tribal agency with primary responsibility for child protection or investigation of child abuse within the portion of Indian Country involved. If the report involves a potential crime and either involves an Indian Child or an Indian suspect, the local law enforcement agency is required to make an immediate report to the FBI. (25 U.S.C. §3203(b) (2)).

(U) Although mandatory reporting laws vary by jurisdiction, FBI personnel must report suspected child abuse, neglect and/or sexual exploitation even if the FBI employee is not designated as a mandated reporter under the law.

K.3 (U) CHILD ABUSE DISCOVERED FROM A CONFIDENTIAL SOURCE OR INVESTIGATION

(U) When suspected child abuse, neglect and/or sexual exploitation is based on information gathered during a confidential investigation or from a confidential source, FBI personnel should make every effort to report the abuse to the appropriate state, local or tribal authorities in order to protect the safety of the child. If it is not possible to report the suspected child abuse without significantly compromising the investigation or other confidential source such as classified information, or endangering public safety, FBI personnel shall obtain guidance from the designated Component Responsible Official.

(U) The Component Responsible Official shall not delegate this responsibility. The Component Responsible Official must consult personnel with expertise in the subject matter of child abuse, neglect and/or sexual exploitation matters (e.g., Victim Specialist or OVA) and receive a legal opinion from the CDC, OGC, or DOJ on the basis for not reporting, to include the potential penalties, some of them criminal, and include it in a 188D-EC documenting the decision not to report. The Component Responsible Official must monitor the case, and no later than every 30 days, re-review the case for its ability to be reported, and document in a 188D-EC. Moreover, the Component Responsible Official must immediately report the suspected child abuse, neglect and/or sexual exploitation, in accordance with this policy, the instant the basis for withholding no longer exists.

K.4 (U) DESIGNATED OFFICIAL

K.4.1 (U) IDENTIFICATION OF A DESIGNATED OFFICIAL

(U) The Component Responsible Official must designate a Designated Official in writing via an Electronic Communication with case identification number 188D-HQ-A2450935. For field offices, the designee may be no lower than an ASAC. For HQ divisions or offices, the designee may be no lower than a Unit Chief.

K.4.2 (U) DUTIES OF A DESIGNATED OFFICIAL

(U) Receive reports of suspected child abuse, neglect and/or sexual exploitation from FBI personnel where the incident is alleged to have occurred in a Division or office's area of responsibility.

(U) Assist FBI personnel with the reporting of suspected child abuse, neglect and/or sexual exploitation if the report is not made directly to state, local or tribal authorities by FBI personnel.

(U) Ensure completion of an Electronic Communication to the FBI's OVA.

K.5 (U) CONTENTS OF THE 188D-EC

(U) Any 188D-EC prepared under this policy shall reflect all appropriate case identification numbers, case identification number 188D-HQ-A2450935, and include, to the extent known and applicable, the following information:

- A) (U) Person making the report
- B) (U) When the individual became aware of the suspected child abuse, neglect and/or sexual exploitation
- C) (U) Date/time reported to CPS, LE, and/or other investigative agency
- D) (U) CPS/agency ID number (if applicable)
- E) (U) How the report was made (in person, by phone, in writing)
- F) (U) Whether the report was anonymous
- G) (U) Work-related or non-work related incident
- H) (U) Source of the information (direct observation or other)
- I) (U) Location of the incident (federal land, federal facility, or other)
- J) (U) Synopsis of the facts that give reason to suspect child abuse, neglect and/or sexual exploitation
- K) 11. (U) General indexing, to include: subject, victim, and addresses

K.6 (U) REPORTING BY FBI PERSONNEL OUTSIDE OF THE UNITED STATES JURISDICTION

(U) FBI personnel assigned or on temporary duty (TDY) outside the United States (U.S.) are also responsible for reporting suspected child abuse, neglect and/or sexual exploitation. FBI personnel outside the U.S. on personal travel are encouraged to report suspected child abuse, neglect and/or sexual exploitation, when practicable.

(U) Suspected child abuse, neglect and/or sexual exploitation involving U.S. government employees or dependents under the Chief of Mission of the U.S. Embassy must be reported to the Regional Security Officer and the FBI Designated Official. If the suspected abuse involves foreign citizen perpetrators or victims, the FBI personnel should consult with the Legal Attaché (LEGAT) and/or Regional Security Officer in the Embassy regarding any reporting laws of the foreign country and act accordingly. Contact for the purpose of reporting or notice of the reporting contact may be made by the FBI LEGAT to the host government. FBI personnel should also notify the FBI's OVA via the division Designated Official and a 188D-EC.

K.7 (U) CONFLICTS OF LAW OR POLICY

(U) This policy does not authorize any exception to laws requiring mandatory reporting of suspected child abuse, neglect and/or sexual exploitation.

(U) If there is an apparent conflict with the law and this policy, consult your supervisory chain and seek a legal opinion from your respective CDC or the OGC.

K.8 (U) DEFINITIONS**K.8.1 (U) CHILD**

(U) A person under the age of 18 years. See also the *Guidelines* (Article IV.I.5; p.32) for notification obligations and specialized procedures on notifying child victims after they reach the age of majority.

K.8.2 (U) CHILD ABUSE

(U) The physical or mental injury, sexual abuse or sexual exploitation, or negligent treatment of a child.

K.8.3 (U) SEXUAL ABUSE

(U) Includes rape, molestation, or incest with children.

K.8.4 (U) SEXUAL EXPLOITATION

(U) Includes the production, distribution, receipt, possession, or access of child pornography, as well as the commercial sexual exploitation of children (prostitution), and the employment, use, persuasion, inducement, enticement, or coercion of a child to engage in, or assist another person to engage in, sexual abuse or sexual exploitation of children.

K.8.5 (U) NEGLIGENT TREATMENT

(U) The failure to provide adequate food, clothing, shelter, or medical care so as to seriously endanger the physical health of the child.

K.8.6 (U) NOT CHILD ABUSE

(U) Child abuse does not include discipline administered by a parent or legal guardian to his or her child provided it is reasonable in manner and moderate in degree and otherwise does not constitute cruelty.

K.9 (U) FBI PERSONNEL

(U) Any FBI employee or affiliated person authorized by appropriate authority to participate in an FBI investigation, activity or mission, who is under the control and authority of the FBI. As in accordance with DIOG Section 2.11.

(U) This “includes, but is not limited to: an operational/administrative professional support person, intelligence analyst, special agent, task force officer (TFO), task force member (TFM), task force participant (TFP), detailee, and FBI contractor;” as well as a confidential human source (CHS) “when operating pursuant to the tasking or instructions of an FBI employee.”

K.10 (U) “REASON TO SUSPECT CHILD ABUSE, NEGLECT OR EXPLOITATION”

(U) Reason to suspect child abuse, neglect and/or sexual exploitation means FBI personnel who witness suspected child abuse, neglect and/or sexual exploitation by either personally seeing or hearing it, or learning of facts that give reason to suspect child abuse, neglect and/or sexual exploitation. Becoming a witness includes if the suspected child abuse, neglect.

This Page is Intentionally Blank

UNCLASSIFIED//~~LES~~

Domestic Investigations and Operations Guide



(U) DOMESTIC INVESTIGATIONS AND OPERATIONS GUIDE

Appendix L

(U) Investigative Methods Conducted Online by FBI Employees

Table of Contents

1. (U) Introduction	1
2. (U) General	2
2.1. (U) Protecting Civil Liberties.....	2
2.2. (U) Scope of This Appendix	3
2.3. (U) Principles	3
2.3.1. (U) Personal Online Activity	3
2.3.2. (U) Disclosure of FBI Affiliation	3
2.4. (U) Preserving Electronic Communications	4
2.5. (U) Online News Media	5
3. (U//LES) Authorized Activities Conducted Online Prior to Opening an Assessment.....	6
3.1. (U// LES) Public Information.....	6
3.1.1. (U) Publicly Available Information on the Internet.....	6
3.1.2. (U) Public Chat Rooms.....	6
3.1.3. (U// LES) Obtaining Identifying Information about Users or Networks.....	7
3.2. (U// LES) Information Restricted to Law Enforcement.....	7
3.3. (U// LES) [REDACTED].....	8
3.3.1. (U) Definitions.....	8
3.4. (U) Documentation Requirements for Activities Authorized Prior to Opening an Assessment: Existing/Historical Information (DIOG 5.1.2).....	9
3.4.1. (U) Processing a Complaint.....	9
3.4.2. Conducting Proactive Internet Searches of “Publicly Available Information”.....	10
3.5. (U) Prohibited Activities Prior to Opening an Assessment.....	12
4. (U//LES) Authorized Investigative Methods Conducted Online: Assessments. 14	14
4.1. (U) Introduction.....	14
4.2. (U// LES) Publicly Available Information (DIOG 18.5.1).....	14
4.3. (U// LES) [REDACTED].....	14
4.3.1. (U) [REDACTED] Social Media.....	14
4.3.2. (U) Mandatory review.....	15
4.3.3. (U// LES) [REDACTED].....	15
4.3.4. (U// LES) [REDACTED].....	16
4.4. (U// LES) Private/Restricted Access	17
4.4.1. (U// LES) Consent Search: Obtaining Access to Restricted Online Web Sites with Consent	17
4.4.2. (U// LES) CHS Use and Recruitment (DIOG 18.5.5)	18
4.4.3. (U// LES) [REDACTED] (DIOG 18.5.6.1).....	18
4.5. (U// LES) [REDACTED].....	19

b7E

UNCLASSIFIED//~~LES~~
Domestic Investigations and Operations Guide

4.5.1.	(U// LES) Interacting with the Public While in a Nonaffiliated Status	19
4.6.	(U// LES) Monitoring/Recording of Real-Time Communications in Assessments (Distinction Between Public and Private).....	20
4.6.1.	(U// LES) Public Real-Time Communications in Assessments (Recording Permitted if FBI Employee/CHS/Consenting Party is Present).....	20
4.6.2.	(U// LES) Private, Real-Time Online Communications in Assessments (Recording not Permitted).....	22
5.	(U//LES) Investigative Methods Conducted Online: Predicated Investigations	23
5.1.	(U) Introduction.....	23
5.2.	(U// LES) Consensual Monitoring of Communications, Including Electronic Communications (DIOG 18.6.1).....	23
5.2.1.	(U// LES) Private, Real-time Online Communications in Predicated Investigations	23
5.3.	(U// LES) Intercepting the Communications of a Computer Trespasser (DIOG 18.6.2)	24
5.4.	(U// LES) Undercover Activity (DIOG 18.6.13.3)	24
5.5.	(U// LES) Undercover Operations (DIOG 18.6.13.3).....	25
5.5.1.	(U// LES) Interim Authority to Continue Online Contacts.....	26
5.5.2.	(U// LES) Defining Substantive Undercover Contact in the Online Context 27	
5.5.3.	(U// LES) [REDACTED]	28
5.5.4.	(U// LES) [REDACTED]	29
5.6.	(U// LES) [REDACTED]	31
6.	(U//LES) Online Activity Leading to Undisclosed Participation	33
7.	(U//LES) Extraterritorial Online Activity	35
7.1.	(U// LES) Overview	35
7.2.	(U// LES) [REDACTED]	36
7.3.	(U// LES) [REDACTED]	36
7.4.	(U// LES) [REDACTED]	37
7.5.	(U// LES) [REDACTED]	38
7.6.	(U// LES) [REDACTED]	38
8.	(U) DIOG Appendix L -Quick Reference Guide (QRG).....	40
9.	(U) Key Terms and Definitions.....	41

b7E

1. (U) Introduction

(U) **Purpose:** The purpose of this appendix is to assist Federal Bureau of Investigation (FBI) employees apply the Domestic Investigations and Operations Guide (DIOG) to investigative methods conducted online, prior to the opening of an Assessment or predicated investigation and within Assessments and predicated investigations. For guidance on extraterritorial (ET) matters pursuant to this appendix, please see Section 7 herein, entitled “Extraterritorial Online Activity.” See also DIOG Section 13, entitled “Extraterritorial Provisions” and the Foreign Technical Assistance Policy Directive and Policy Guide (0641DPG).

(U) **Background:** The guidance in this document is derived from various statutes, the “Online Investigative Principles for Federal Law Enforcement Agents” (OIP) (November 1999), previous electronic communications (EC), and other policy documents.

(U) This appendix establishes policies for online investigative methods.

(U) Online methods can present challenges and complexities that may not always be present in physical or “real-world” activities. These challenges, and the fast pace of evolving technology, lead to frequent changes in applicable laws. As a result, employees are urged to consult with their chief division counsels (CDC) and/or the FBI/Office of the General Counsel (OGC) before and during any proposed online activities.

(U) **Intended Audience:** The guidance in this appendix applies to all FBI personnel, as defined in DIOG Section 3, including FBI special agents (SA), analysts, other FBI employees, task force officers (TFO), task force members (TFM), FBI contractors, and others who engage in, supervise, or otherwise participate in online investigative activities and are bound by the Attorney General’s Guidelines for Domestic FBI Operations (AGG-Dom) and the DIOG

2. (U) General

2.1. (U) Protecting Civil Liberties

(U) The protections embodied in the DIOG are designed to ensure that the FBI adheres to the Constitution and laws of the United States and respects privacy, civil liberties, and First Amendment rights. These protections are particularly important when applied to online investigative methods because much of the content and many of the activities available or conducted on the Internet fall within some category of constitutionally protected information (e.g., freedom of individuals to associate, freedom to express an unpopular belief or opinion, or freedom to assemble). Accordingly, FBI employees must always carefully assess and analyze all investigative methods and communications conducted online.

(U) All principles stated previously in the DIOG that have been put in place to protect civil liberties also apply to investigative methods conducted online by FBI employees, such as the need to have a legitimate law enforcement purpose for all investigative activities, engaging in the least intrusive methods, sensitive investigative matters (SIM), and undisclosed participation (UDP).

(U) Example:

b7E

(U) The FBI may only collect, as defined in subsection 3.1, of this appendix, information relating to the exercise of a First Amendment right if (1) the collection is logically related to an authorized investigative purpose, (2) the collection does not materially interfere with the ability of an individual or a group to engage in the exercise of constitutionally protected rights, and (3) the method of collection is the least intrusive alternative that is reasonable, based upon the circumstances of the investigation. The FBI cannot ever base its conduct solely on an individual's legal exercise of his or her First Amendment rights. Further, every FBI employee has the responsibility to ensure that the activities of the FBI are "lawful, appropriate and ethical as well as effective in protecting the civil liberties and privacy of individuals in the United States." (See DIOG 4.1.3.)

(U) Consistent with the DIOG, FBI employees must always ensure that all online investigative activities are "focused in scope, time, and manner to achieve the underlying purpose." (See DIOG 4.1.2.) FBI employees must document this relationship, as necessary, in the case file.

2.2. (U) Scope of This Appendix

(U) This appendix only applies to investigative methods conducted online by FBI employees, as they are defined in DIOG Section 3. This appendix seeks to set out the standards for these investigative methods engaged in online by FBI employees in both affiliated and nonaffiliated capacities and in both public and private forums. Each online investigative method is defined below, in addition to whether or not it is permitted in an assessment or a predicated investigation.

(U) **Note:** Where possible, the corresponding DIOG cite for the specific investigative activity/method is provided.

2.3. (U) Principles

2.3.1. (U) Personal Online Activity

(U) FBI employees are not permitted to use any personal online accounts to access information for official purposes. Such use may inappropriately associate an employee's identity with official FBI activity and may inappropriately result in access to restricted information.

(U) An FBI employee is generally free to engage in solely personal, appropriate, online pursuits while off duty. If, however, the off-duty online activities of the FBI employee are within the scope of an ongoing investigation, serving the goals of an ongoing investigation, or undertaken for the purpose of developing investigative leads, the FBI employee is bound by the same policies and restrictions for online investigative activities as when he or she is on duty.

2.3.2. (U) Disclosure of FBI Affiliation

(U) When an FBI employee engages in investigative methods online, the same principles apply as in the physical world as they relate to when the individual must provide official identification as an FBI employee and when that requirement does not exist. When interacting with members of the public as part of their official duties, FBI employees must operate openly and consensually (DIOG 18.5.6). The use of the FBI UNet (unclassified network) to access the Internet can reveal government affiliation; however, this is not sufficient to satisfy the requirement to "disclose the employee's affiliation with the FBI" when seeking information from witnesses, subjects, or victims. The disclosure of FBI affiliation must be explicit and overt when requesting information from members of the public and from private entities, unless there is an authorized basis for not disclosing FBI affiliation. An employee can achieve this by explicitly stating his or her FBI affiliation within the content of a message.

(U) [REDACTED]

1. (U//~~LES~~) [REDACTED]

[REDACTED]

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

[REDACTED]

b7E

3. (U//~~FOUO~~) [REDACTED]

- (U//~~FOUO~~) Certified undercover employee (UCE) is defined as an employee of the FBI or other federal, state, or local law enforcement agency; another entity of the United States Intelligence Community (USIC); or a foreign intelligence agency, working under the direction and control of the FBI, and whose relationship with the FBI is concealed from third parties by the maintenance of a cover or an alias identity. A UCE's identity and alias must be guarded closely to protect the safety of the UCE and the integrity of the undercover operation (UCO).
- (U//~~FOUO~~) Certified online covert employee (OCE) is defined as an employee of the FBI, or another federal, state, or local law enforcement agency; another entity of the USIC; or a foreign intelligence agency, acting at the behest of the FBI in an online capacity, and whose identity is concealed from third parties by the maintenance of a cover or an alias identity. An OCE's identity and alias must be guarded closely to protect the safety of the OCE and the integrity of the UCO.

(U//~~FOUO~~) When interacting with the public online, employees must take necessary action to ensure they are sufficiently identified in true name/law enforcement affiliation, unless authorized as described above. In order to identify oneself fully when overtly interacting with the public online, the employee must include his or her true name and affiliation with law enforcement with each posted comment. For electronic mail (e-mail) communications, employees must use their fbi.gov e-mail addresses and/or other official, overt, government-sponsored e-mail account addresses and identify themselves by their law enforcement affiliations in the content of the messages. In short, in any overt online communications, enough indicators of name, official title, and the agency must be included such that a reasonable person would understand that he or she is providing information to law enforcement.

(U//~~LES~~) Example: [REDACTED]

(U//~~LES~~) Example: [REDACTED]

2.4. (U) Preserving Electronic Communications

(U//~~LES~~) Employees should retain the contents of stored electronic messages, such as e-mails, if they would have retained those messages had they been written on paper. [REDACTED]

[REDACTED] the employee should memorialize any information of [REDACTED]

UNCLASSIFIED//~~LES~~
Domestic Investigations and Operations Guide

investigative value in an FD-302 (“Form for Reporting Information That May Become the Subject of Testimony”). The contents must be preserved in a manner authorized by FBI procedures governing the preservation of electronic communications (e.g., see CPD 0423D, *Preservation and Disclosure of Electronic Communications in Federal Criminal Cases*; and CPD 0140D, *Electronic Discovery*).

2.5. (U) Online News Media

(U) The DIOG establishes additional oversight and approval requirements for assessments and predicated investigations involving SIMs. Investigations involving the activities of the news media on the Internet are SIMs. (See DIOG 10.1.2.2.5 for the definition of “news media” and DIOG 18.5.6.4.8 for rules on interviews or contact with the news media.)

3. (U//~~LES~~) Authorized Activities Conducted Online Prior to Opening an Assessment

(U//~~LES~~) Warning:

b7E

3.1. (U//~~LES~~) Public Information

(U//~~LES~~) DIOG 5.1.1.1 authorizes employees to search and review various forms of online information prior to the initiation of an assessment or a predicated investigation, including various government systems and paid-for-service databases, as well as information available to the public via the Internet. However, to protect the public's constitutional rights, privacy, and civil liberties, employees must review, analyze, and document their investigative activities carefully. For further discussion, see DIOG 4.2.

3.1.1. (U) Publicly Available Information on the Internet

(U//~~LES~~) Warning:

b7E

(U//~~LES~~) FBI employees may conduct Internet searches of “publicly available information” for authorized purposes prior to the initiation of an assessment or a predicated investigation. To be considered “publicly available information,” the online content must be available to the employee in the same manner that it is to the general public. Where the online resource requires the employee to register for access, access to that resource is considered available to the public if the registration process is designed to accept all applications from the public and in no other way creates a restriction as to who may access the information. Use of fictitious information to register for access is prohibited prior to opening an assessment.

(U//~~LES~~) **Note:** Online information that requires a fee for access is considered “publicly available information” if anyone in the general public can purchase access to the same information. In this situation, paying a fee for access is comparable to paying for a newspaper that is offered for sale to the public. (See DIOG subsection 18.5.1.1.D.)

(U//~~LES~~) **Example:**

b7E

3.1.2. (U) Public Chat Rooms

(U//~~LES~~) Information contained in a public chat room may fall within the category of “publicly available information.” Public chat rooms are comparable to attending a public

UNCLASSIFIED//~~LES~~
Domestic Investigations and Operations Guide

meeting and may be used to review public information prior to the opening of an assessment or a predicated investigation. (See DIOG subsections 5.1.1.1 and 18.5.1.E.)

b7E

(U//~~LES~~) **Example:**

(U//~~LES~~) **Response:**

3.1.3. (U//~~LES~~) Obtaining Identifying Information about Users or Networks

(U//~~LES~~) There are widely available software tools for obtaining publicly available identifying information about an individual or a host computer on a network.

Employees may use such tools in their intended, lawful manner under the same circumstances that the DIOG authorizes employees to look up similar identifying information (e.g., a telephone number) through nonelectronic means. Employees must be careful to use these information-gathering tools only as conventionally permitted and not in a manner unauthorized by the system, such as by exploiting design flaws in a program or using software tools to circumvent operating system protections or circumvent restrictions placed on system users.

(U//~~LES~~) **Example:**

b7E

(U//~~LES~~) Certain tools, even though commonly and openly available on the Internet and used by the public, are not permitted for use by law enforcement if their use would violate statutory restrictions such as the Electronic Communication and Privacy Act (ECPA) or Title III.

(U//~~LES~~) **Example:**

3.2. (U//~~LES~~) Information Restricted to Law Enforcement

(U//~~LES~~)

b7E

UNCLASSIFIED//~~LES~~
Domestic Investigations and Operations Guide

b7E

[redacted]
[redacted] (See the example at DIOG subsection 5.6.3.1.8.1.)

(U//~~LES~~) Some database providers offer access to the public through subscription while still reserving specific categories of information exclusively for law enforcement access (e.g., Lexis/Nexis). The FBI might contract for access to both the public and restricted portions of the database information. [redacted]

[redacted]

3.3. (U//~~LES~~) [redacted]

(U//~~LES~~) [redacted]

[redacted]

3.3.1. (U) Definitions

1. (U//~~LES~~) [redacted]
[redacted]

b7E

2. (U//~~LES~~) [redacted]
[redacted]

3. (U//~~LES~~) [redacted]
[redacted]

(U) [redacted]
[redacted]

b7E

(U//~~LES~~) **Example** [redacted]

[redacted]

3.4. (U) Documentation Requirements for Activities Authorized Prior to Opening an Assessment: Existing/Historical Information (DIOG 5.1.2)

(U//~~FOUO~~) FBI employees may conduct Internet searches of “publicly available information” for authorized purposes prior to the initiation of an assessment or a predicated investigation. The following documentation requirements differ, depending on whether the searches are being conducted pursuant to (1) processing a complaint, (2) responding to a tip or lead, or (3) conducting proactive Internet searches of “publicly available information”:

3.4.1. (U) Processing a Complaint

(U//~~FOUO~~) FBI employees are permitted to retain records checks and other information collected while processing a complaint or responding to a tip or lead using permitted DIOG 5.1.1 activities. This collection/retention is permitted if, in the judgment of the FBI employee, there is a law enforcement, intelligence, or public safety purpose. This documentation must be completed as soon as practicable, but not more than five business days from the receipt of the information. When permitted, such documentation must be retained in one of the following files:

- (A)(U//~~FOUO~~) Zero classification file, when no further investigative activity is warranted
- (B)(U//~~FOUO~~) Relevant, open or closed zero sub-assessment file
- (C)(U//~~FOUO~~) Relevant, open or closed assessment
- (D)(U//~~FOUO~~) Relevant, open or closed predicated investigation file
- (E)(U//~~FOUO~~) New assessment or predicated investigation file, when further investigative activity is warranted
- (F)(U//~~FOUO~~) Unaddressed work file
- (G)(U//~~FOUO~~) Example

(U//~~FOUO~~) Response:

(U//~~FOUO~~)

(U//~~FOUO~~) Response:

3.4.2. Conducting Proactive Internet Searches of “Publicly Available Information”

(U//~~FOUO~~) FBI employees are permitted to conduct proactive Internet searches of “publicly available information” to process observations or other information for authorized purposes, but they may only collect/retain this information if it is within the scope of an open assessment or a predicated case. This collection/retention is permitted if, in the judgment of the FBI employee, there is a law enforcement, intelligence, or public safety purpose. This documentation must be completed as soon as practicable, but not more than five business days from the receipt of the information. When permitted, such documentation must be retained in one of the following files (with a summary narrative tying the information to an FBI criminal or national security purpose):

- (A)(U//~~FOUO~~) A relevant, open assessment
- (B)(U//~~FOUO~~) A relevant, open predicated investigation file
- (C)(U//~~FOUO~~) A new assessment or predicated investigation file, when further investigative activity is warranted

(U//~~FOUO~~) If, however, in the judgment of the FBI employee, the records checks or other information obtained using permitted DIOG 5.1.1 activities, does not serve a law enforcement, intelligence, or public safety purpose, then those record checks, data, information, or documents cannot be retained and must be destroyed. This requirement to destroy applies to information printed or stored on removable media, stored within a public database (history of searches/queries), or stored in any other physical or digital

~~UNCLASSIFIED//LES~~
Domestic Investigations and Operations Guide

location capable of maintaining a search/query history that is within the control of the FBI employee.

(U//~~FOUO~~) Example 2:

[Redacted]

b7E

[Redacted]

(U//~~FOUO~~) Response 2:

[Redacted]

[Redacted]

(U//~~FOUO~~) Example 3:

[Redacted]

[Redacted]

(U//~~FOUO~~) Response 3:

[Redacted]

[Redacted]



3.5. (U) Prohibited Activities Prior to Opening an Assessment

The following activities are prohibited prior to opening an assessment:

- (U//LES) 

 See also
appendix L subsection 3.1.2.

b7E

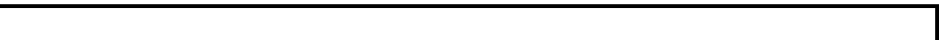
- (U) 


(U) Exception



- (U) 


b7E

- (U) 


(U//LES) Example



(U//LES) **Exception:** The only exception to this rule is that prior to opening an assessment or a predicated investigation, an employee may employ limited use of his or her official e-mail to conduct a “clarifying interview.” (See DIOG 5.1.1.1, 5.1.1.5, and 5.1.1.6.) In this limited circumstance, the employee must overtly identify himself or herself as being affiliated with the FBI  When conducting such clarifying interviews online, employees must use their official FBI Internet e-mail accounts (e.g., firstname.lastname@ic.fbi.gov) and/or other government-sponsored, overt e-mail account addresses and identify

b7E

UNCLASSIFIED//~~LES~~

Domestic Investigations and Operations Guide

themselves as FBI employees in the content of the e-mail messages. [REDACTED]

b7E

(U//~~LES~~)

UNCLASSIFIED//~~LES~~

4. (U//~~LES~~) Authorized Investigative Methods Conducted Online: Assessments

4.1. (U) Introduction

(U//~~LES~~) All investigative methods authorized prior to the opening of assessments or predicated investigations are authorized during assessments. Consistent with DIOG 18.5, the following online methods are authorized during an assessment.

4.2. (U//~~LES~~) Publicly Available Information (DIOG 18.5.1)

(U//~~LES~~) In addition to the online investigative methods defined in subsection 3.1 of this appendix, once an assessment has been opened, employees may also use automated regular searches (e.g., Google alerts) to conduct regular searches of publicly available information. However, as stated in subsection 3.1, to protect the public's constitutional rights, privacy, and civil liberties, employees must review, analyze, and document their investigative activities carefully. For further discussion, see DIOG 4.2.

4.3. (U//~~LES~~)

[REDACTED]

(U//~~LES~~) Warning

[REDACTED]

(U//~~LES~~) [REDACTED] the FBI should generally deal openly with the public during an assessment. It is permissible in an assessment (see DIOG 18.5.6.4.9 and 18.5.6.4.11.1.), [REDACTED]

[REDACTED]

4.3.1. (U) [REDACTED] Social Media

(U//~~LES~~)

[REDACTED]

[REDACTED]

b7E

b7E

UNCLASSIFIED//~~LES~~
Domestic Investigations and Operations Guide

4.3.2. (U) Mandatory review

(U//~~FOUO~~) Statements made by subjects of assessments and predicated investigations utilizing social media generally include content protected by the First Amendment. The FBI may only collect, as defined in subsection 3.1 of this appendix, information relating to the exercise of a First Amendment right if (1) the collection is logically related to an authorized investigative purpose, (2) the collection does not materially interfere with the ability of an individual or a group to engage in the exercise of constitutionally protected rights, and (3) the method of collection is the least intrusive alternative that is reasonable, based upon the circumstances of the investigation. While conducting file reviews and assessment justification reviews pursuant to DIOG 3.4.4, supervisory personnel must ensure that collection of content/materials [REDACTED]

[REDACTED] are consistent with subsection 3.1 of this appendix.

4.3.3. (U//~~LES~~) [REDACTED]

(U//~~LES~~) [REDACTED]

b7E

[REDACTED]

[REDACTED] (See DIOG 18.5.6.4.9.)

(U//~~FOUO~~) For Type 5 assessments, detailed policy requirements regarding [REDACTED]

b7E

[REDACTED] in
the Confidential Human Source Policy Guide (CHSPG), 0836PG.

(U//~~LES~~) **Warning:** [REDACTED]

[REDACTED]

(U//~~LES~~) **Note:** [REDACTED]

[REDACTED]

(U//~~LES~~) **Warning:** [REDACTED]

[REDACTED]

UNCLASSIFIED//~~LES~~
Domestic Investigations and Operations Guide

[redacted]
[redacted] (See
DIOG 18.5.6.4.9 and 18.5.6.4.11.9 and subsection 4.5.1 of this appendix for
additional information.)

(U//~~LES~~) Example: [redacted]
[redacted]

b7E

4.3.4. (U//~~LES~~) [redacted]
(U//~~LES~~) [redacted]
[redacted]
[redacted] (See
DIOG 18.5.6.4.11.1. [redacted]
[redacted] outlined in DIOG 18.5.6.4.9 (D). [redacted]
[redacted]

b7E

(U//~~LES~~) Example: [redacted]
[redacted]
(U//~~LES~~) Example: [redacted]
[redacted]
[redacted] (See DIOG
18.5.6.4.9.D.2.)

(U//~~LES~~) If justification develops to open of a preliminary investigation
("information or allegation" indicating the existence of federal criminal activity or
a threat to national security or to protect against such activity or threat [see DIOG
6.5]) the employee may seek oral approval [redacted]

Domestic Investigations and Operations Guide

[redacted] and obtain oral authority for consensual monitoring, consistent with DIOG 18.6.1, if necessary under the circumstances.

(U//~~LES~~) Example: [redacted]

b7E

(U//~~LES~~) Note: [redacted]

[redacted] (See DIOG 18.5.6.4.9.)

4.4. (U//~~LES~~) Private/Restricted Access

4.4.1. (U//~~LES~~) Consent Search: Obtaining Access to Restricted Online Web Sites with Consent

(U//~~LES~~) Note: A consenting party is someone with the authorization to “access and control” content on the site. This includes the account holder for a social-networking site, the system administrator, or a company official with authority to direct others regarding site content. An employee may also access a restricted site if the owner makes the site available to a category of Internet users that includes the employee [redacted]

b7E

(U//~~LES~~) In order to access private or restricted-access online forums, as in the physical world, an exception to the search warrant requirement is needed. The most commonly utilized exception during FBI investigative methods conducted online is consent. Internet content not available to the general public is considered restricted access. Access may be restricted to a few select persons [redacted]

[redacted] or may be restricted to a certain class of individuals [redacted]

Such sites are considered restricted sources of online information. An employee is authorized to obtain access to such sites during an assessment if the consenting party [redacted] is fully aware of the employee’s affiliation

with the FBI and has authority to consent, as demonstrated by the consenting party’s access and control. Written consent must be obtained whenever possible from the consenting party and documented in the case file. For CHSs, this documentation must be maintained in CHS files. If the consenting party declines to provide written consent, oral consent is acceptable, as long as two employees (one of whom must be an FBI agent) witness the consent, and the consent is documented in an FD-302 (“Form for Reporting Information That May Become the Subject of Testimony”) [redacted]

[redacted] This activity constitutes a consent search, and it is fully authorized during an assessment. (See DIOG 5.9.1.) As is the case with all consent searches, the employee must always be mindful of the exact consent given and whether the consenting party has the lawful authority to grant the actual consent provided to the employee.

UNCLASSIFIED//~~LES~~
Domestic Investigations and Operations Guide

4.4.2. (U//~~LES~~) CHS Use and Recruitment (DIOG 18.5.5)

4.4.2.1. (U//~~LES~~) Tasking a CHS/Nonconfidential Party to Access a Restricted Web Site (Authorized Access) [REDACTED]

(U//~~LES~~) A CHS/consenting party may be tasked to access a restricted Web site to gather information only if the CHS/consenting party has authorized access (consent). [REDACTED]

[REDACTED]

[REDACTED] See subsection 5.2. [REDACTED]

[REDACTED]

(U//~~LES~~) Example:

[REDACTED]

b7E

4.4.3. (U//~~LES~~) [REDACTED] (DIOG 18.5.6.1)

(U//~~LES~~)

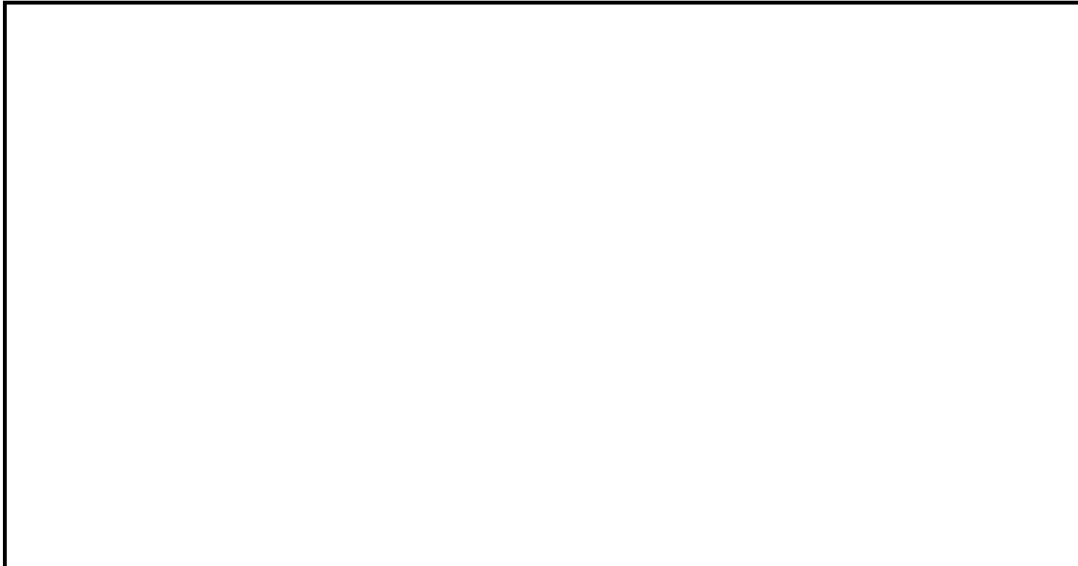
[REDACTED]

(U//~~LES~~) Example:

[REDACTED]

UNCLASSIFIED//~~LES~~
Domestic Investigations and Operations Guide

b7E



(U//~~LES~~) Warning



4.5. (U//~~LES~~)



(U//~~LES~~)



please see subsection

3.3.1. of this appendix.

4.5.1. (U//~~LES~~) Interacting with the Public While in a Nonaffiliated Status

(U//~~LES~~)



of

DIOG 18.5.6.4.9, as outlined below:

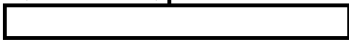
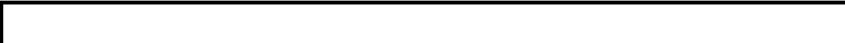
1. (U//~~FOUO~~)



2. (U//~~FOUO~~)



3. (U//~~FOUO~~)



4. (U//~~FOUO~~)



b7E

UNCLASSIFIED//~~LES~~
Domestic Investigations and Operations Guide

b7E

5. (U//~~FOUO~~)

[Redacted]

6. (U//~~FOUO~~)

(U//~~LES~~)

[Redacted]

(U//~~LES~~) Example:

[Redacted]

(U//~~LES~~)

[Redacted]

4.6. (U//~~LES~~) Monitoring/Recording of Real-Time Communications in Assessments (Distinction Between Public and Private)

4.6.1. (U//~~LES~~) Public Real-Time Communications in Assessments (Recording Permitted if FBI Employee/CHS/Consenting Party is Present)

4.6.1.1. (U//~~LES~~) Definition of Public Real-Time Communication

(U//~~LES~~) A key factor in determining if an exchange is occurring in real time is whether the exchange is preserved and made available on the site to viewers later on. Forums where the communications are preserved for future viewers are generally not real time. Typically, a blog or bulletin board system preserves posted comments to enable future viewers to see the information, meaning that communications posted on these forums are not real time. Further, even when several contributors to a bulletin board site are using it to rapidly engage in an exchange, it is not a real-time forum, as the content enjoys some degree of permanency, even though the information may only be posted online for as little as a week. In contrast, a typical chat room is designed to allow only users currently in the room to view the exchange and does not preserve the exchange for those entering

UNCLASSIFIED//~~LES~~
Domestic Investigations and Operations Guide

the room at a later point in time. [REDACTED]

(U//~~LES~~) Legal authority: The monitoring/recording of most real-time communications on the Internet is protected by the First and Fourth Amendments and/or statutes such as Title III and the Foreign Intelligence Surveillance Act (FISA). There is a unique section of the Wiretap Act (18 U.S.C. 2511(2)(g)(i)) that allows “any person” to intercept an electronic communication that is readily accessible to the general public (i.e., public real-time communications”). [REDACTED]

b7E

(U//~~LES~~) Approval requirement: Public real-time communications that are evidentiary in nature should be recorded if it is necessary to achieve the objective of the assessment and is the least intrusive means to do so. Once the public real-time communications are recorded, only pertinent information may be documented/indexed into an FBI Recordkeeping System (i.e., serialized via an FD-302). The complete recording must be stored as evidence in the investigative file and the communications must be preserved in a manner authorized by FBI procedures governing the preservation of electronic communications.

(U//~~LES~~) No real-time communications can be recorded if the employee is not present during the recording. While 18 U.S.C. 2511(2)(g)(i) allows the recording of public real-time communications without the presence of a consenting party or without a court order, as a matter of policy, FBI employees must be present to record public real-time communications during an assessment. [REDACTED]

[REDACTED] (See DIOG 18.6.3.5.) Additionally, in order to utilize the least intrusive means and to limit the collection of non-pertinent communications, the employee must observe the communications as they are being recorded.

(U//~~LES~~) Example: [REDACTED]

b7E

(U//~~LES~~) Example: [REDACTED]

(U//~~FOUO~~) The employee must ensure that information to be collected from the Internet is rationally related to his or her authorized purpose and can be lawfully obtained. The employee must properly document this analysis in the investigative file.

**4.6.2. (U//~~LES~~) Private, Real-Time Online Communications in Assessments
(Recording not Permitted)**

(U//~~LES~~) Significant amounts of real-time online communications are private communications (e.g., instant messaging or restricted chat rooms) requiring consensual monitoring authority to record. The AGG-Dom limits the use of consensual monitoring to predicated cases. In these situations, employees are permitted to monitor private, real-time online communications during an assessment (with or through a CHS or non-confidential party only), but cannot electronically record them.

5. (U//~~LES~~) Investigative Methods Conducted Online: Predicated Investigations

5.1. (U) Introduction

(U//~~LES~~) In predicated investigations (a preliminary investigation, a full investigation, an enterprise investigation, or a positive foreign intelligence investigation), all online investigative methods authorized prior to the opening of an assessment or during an assessment are authorized. The following online methods are also authorized during predicated investigations.

5.2. (U//~~LES~~) Consensual Monitoring of Communications, Including Electronic Communications (DIOG 18.6.1)

5.2.1. (U//~~LES~~) Private, Real-time Online Communications in Predicated Investigations

(U//~~LES~~) Monitoring of wire, oral, or electronic communications based on the consent of one party to the communication is referred to as consensual monitoring (DIOG 18.6.1.1). In the online environment, the recording of private real-time communications that is restricted from public access is considered consensual monitoring and is only authorized in predicated investigations.

(U//~~LES~~) A restricted online environment is defined as one that is not available to the general public. (See subsection 3.1 of this appendix for further discussion of publicly accessible).

(U//~~LES~~) Example:

[Redacted]

b7E

[Redacted]

(U//~~LES~~) Example:

[Redacted]

[Redacted]

(U//~~LES~~) There are many real-time online forums that involve many people communicating simultaneously (e.g., chat rooms). While employees are cautioned against recording communications not pertinent to the investigation, where feasible (see DIOG 18.6.1.5.1.3), it may not be possible to selectively record comments not pertinent to the

~~UNCLASSIFIED//LES~~
Domestic Investigations and Operations Guide

investigation that have been made by other participants. When nonpertinent communications are intermixed with pertinent communications, recording of the nonpertinent communications is sometimes unavoidable. The employee must always later review the recordings and redact or minimize, as necessary, particularly when disclosing the recording to a third party.

(U//~~LES~~) The employee or OCE must observe/be present during the online communications as they are recorded. No private real-time communications may be recorded if the employee is not present during the recording, that is, to provide the one-party consent.

(U//~~LES~~) As noted in appendix L subsection 4.1, the recording of public real-time communications and the collection of information from restricted forums (authorized in both assessments and predicated investigations) that are not real time do not require consensual monitoring authority. Therefore, when operating within a predicated investigation, it is critical to establish if the forum is restricted and real time to determine whether the employee needs consensual monitoring authority.

(U//~~LES~~) **Approval:** The employee must obtain [redacted] authority to conduct consensual monitoring prior to recording private real-time communications in a restricted forum, in accordance with DIOG 18.6.1. In the FD-759, "Notification of Authority Granted for Use of Electronic Monitoring Equipment Not Requiring a Court Order" (form for consensual monitoring), the employee must articulate how the information to be collected by the recording is relevant to the predicated investigation. When approving the FD-759, [redacted] must consider if recording the communications is the least intrusive method to obtain the evidentiary information, weighing the investigative value of the evidence to be obtained against the potential collection of First Amendment activity. Once recorded, only pertinent information may be uploaded into an FBI Recordkeeping System to minimize the use of non-pertinent information that is only collected because it is commingled with pertinent, case-related information. The complete recording must be stored as evidence.

(U//~~LES~~) **Extraterritorial Considerations:** [redacted]

b7E

[redacted] DIOG 18.6.1.6.1, entitled "Party Located Outside the United States."

5.3. (U//~~LES~~) Intercepting the Communications of a Computer Trespasser (DIOG 18.6.2)

(U//~~FOUO~~) For a full description of this investigative method and the corresponding approvals, please see DIOG section 18.6.2.

5.4. (U//~~LES~~) Undercover Activity (DIOG 18.6.13.3)

(U//~~LES~~) **Warning** [redacted]

b7E

UNCLASSIFIED//~~LES~~
Domestic Investigations and Operations Guide

(U//~~LES~~)

b7E

(U//~~LES~~)

(U//~~LES~~) Example:

(U//~~LES~~) Example:

5.5. (U//~~LES~~) Undercover Operations (DIOG 18.6.13.3)

(U//~~LES~~)

b7E

*Attorney General's Guidelines on
Federal Bureau of Investigation Undercover Operations (AGG-UCO).*

(U//~~LES~~)

~~UNCLASSIFIED//LES~~
Domestic Investigations and Operations Guide

[Redacted]

b7E

(U//~~LES~~) [Redacted]

[Redacted]

(U//~~LES~~) [Redacted]

[Redacted]

(U//~~LES~~) **Approval:** The approval process for UCOs is addressed in DIOG 18.6.13. This subsection applies equally to online UCOs. [Redacted]

[Redacted]

5.5.1. (U//~~LES~~) Interim Authority to Continue Online Contacts

(U//~~LES~~) This subsection is limited to cases governed by the AGG-UCO. (See AGG-UCO IV.I.5.) [Redacted]

b7E

[Redacted]

[Redacted] If interim authority is granted, the OCE must:

1. (U//~~LES~~) [Redacted]
2. (U//~~LES~~) [Redacted]
3. (U//~~LES~~) [Redacted]
[Redacted]
4. (U//~~LES~~) [Redacted]
5. (U//~~LES~~) [Redacted]
[Redacted]
6. (U//~~LES~~) [Redacted]
7. (U//~~LES~~) [Redacted]
[Redacted]

(U//~~LES~~) Employees must conform to all approval and documentation requirements

[Redacted]

5.5.2. (U//~~LES~~) Defining Substantive Undercover Contact in the Online Context

(U//~~LES~~) The nature of online communications makes counting substantive “undercover contacts” (UCAs) more difficult than in the physical world. Generally, a physical-world contact consists of a single communication or conversation, either face-to-face or over the telephone, naturally circumscribed in time. In the online world, each discrete online conversation between an FBI employee and a subject also constitutes a separate undercover contact. [REDACTED]

b7E

[REDACTED]
(U//~~LES~~) [REDACTED]
[REDACTED]

(U//~~LES~~) [REDACTED]
[REDACTED]

(U//~~LES~~) The relevant considerations are:

a. (U//~~LES~~) [REDACTED]
[REDACTED]

b7E

b. (U//~~LES~~) [REDACTED]
[REDACTED]

c. (U//~~LES~~) [REDACTED]
[REDACTED]

d. (U//~~LES~~) [REDACTED]
[REDACTED]

UNCLASSIFIED//~~LES~~
Domestic Investigations and Operations Guide

e. (U//~~LES~~)

b7E

(U//~~LES~~)

(U//~~LES~~) Note:

5.5.3. (U//~~LES~~)

b7E

(U//~~LES~~)

(U//~~LES~~)

(U//~~LES~~) Example:

(U//~~LES~~)

UNCLASSIFIED//~~LES~~
Domestic Investigations and Operations Guide

(U//~~LES~~) Approval:

b7E

- (U//~~FOUO~~)

- (U//~~FOUO~~)

- (U//~~FOUO~~)

- (U//~~FOUO~~)

(U//~~FOUO~~)

5.5.4. (U//~~LES~~)

b7E

5.5.4.1. (U//~~LES~~)

(U//~~LES~~)

(U//~~LES~~)

(U//~~LES~~) Example:

(U//~~LES~~) Example:

(U//~~LES~~)

~~UNCLASSIFIED//LES~~
Domestic Investigations and Operations Guide

b7E

(U//~~LES~~) [redacted]
[redacted] The employee should consult with
his or her CDC or OGC for additional guidance.

5.5.4.2. (U//~~LES~~) [redacted]

(U//~~LES~~) [redacted]
[redacted]

(U//~~LES~~) See subsection 4.4.3. above for the specific requirements for

[redacted]

5.5.4.3. (U//~~LES~~) [redacted]

(U//~~LES~~) [redacted]

[redacted]

(U//~~LES~~) Note [redacted]

[redacted]

(U//~~LES~~) [redacted]

[redacted]

1. (U//~~LES~~) [redacted]

2. (U//~~LES~~) [redacted]

(U//~~LES~~) [redacted]

(U//~~LES~~) **Approval:** (U//~~LES~~) Prior approval to use this method must be obtained from

[redacted]

[redacted] for

criminal cases, [redacted] For

national security cases [redacted]

[redacted]

UNCLASSIFIED//~~LES~~
Domestic Investigations and Operations Guide

b7E

(U//~~LES~~) **Emergency:**

(U//~~LES~~)

5.6. (U//~~LES~~)

(U//~~LES~~)

(U//~~LES~~) **Example:**

~~UNCLASSIFIED//LES~~
Domestic Investigations and Operations Guide

b7E

[Redacted]

(U//~~LES~~) Approval:

[Redacted]

[Redacted]

(U//~~LES~~)

[Redacted]

[Redacted]

(U//~~LES~~)

[Redacted]

[Redacted]

(U//~~LES~~)

[Redacted]

[Redacted]

(U//~~LES~~) Approval:

[Redacted]

[Redacted]

6. (U//~~LES~~) Online Activity Leading to Undisclosed Participation

(U//~~LES~~) UCEs and OCEs engaging in online communications need to be aware of circumstances amounting to UDP. UDP takes place when anyone acting on behalf of the FBI, including a UCE, an OCE, or a CHS, becomes a member of or participates in the activity of a legitimate organization on behalf of the United States government (USG) without disclosing FBI affiliation to an appropriate official of the organization. (See DIOG Section 16 for further discussion on UDP). All employees must understand and be aware of UDP concerns in their online investigations.

(U//~~FOUO~~) Note:

[Redacted]

b7E

[Redacted]

- (U//~~FOUO~~)

[Redacted]

- (U//~~FOUO~~)

[Redacted]

[Redacted]

- (U//~~FOUO~~)

[Redacted]

[Redacted]

- (U//~~FOUO~~)

[Redacted]

[Redacted]

(U//~~LES~~) Note:

[Redacted]

[Redacted]

(U//~~LES~~) Note:

[Redacted]

[Redacted]

UNCLASSIFIED//~~LES~~
Domestic Investigations and Operations Guide

(U//~~LES~~) Note:

[Redacted]

b7E

[Redacted]

(U//~~LES~~)

[Redacted]

[Redacted]

(U//~~LES~~) Example:

[Redacted]

[Redacted]

7. (U//~~LES~~) Extraterritorial Online Activity

7.1. (U//~~LES~~) Overview

(U//~~LES~~) This section has limited application to criminal investigations. For all other investigative activity, applicable ET guidance should be sought from DIOG Section 13 (“Extraterritorial Operations”), [REDACTED]. Additionally, DIOG Appendix G [~~SECRET//NOFORN~~ document] and the [REDACTED] [REDACTED] should be consulted for activities involving the use of technology outside the United States.

(U//~~LES~~) [REDACTED]
[REDACTED]

b7E

1. (U//~~LES~~) [REDACTED]
2. (U//~~LES~~) [REDACTED]
[REDACTED]
3. (U//~~LES~~) [REDACTED]
[REDACTED]
4. (U//~~LES~~) [REDACTED]
[REDACTED]
5. (U//~~LES~~) [REDACTED]
[REDACTED]
[REDACTED]
6. (U//~~LES~~) [REDACTED]
[REDACTED]

(U//~~LES~~) [REDACTED]
[REDACTED]

(U//~~LES~~) [REDACTED]
[REDACTED]

(U//~~LES~~) Note [REDACTED]
[REDACTED]

UNCLASSIFIED//~~LES~~
Domestic Investigations and Operations Guide

(U//~~LES~~)

b7E

(U//~~LES~~) Approval:

(U//~~LES~~) Guidance on ET issues and questions should be sought from

7.2. (U//~~LES~~)

b7E

(U//~~LES~~)

(U//~~LES~~)

(U//~~LES~~) Note:

7.3. (U//~~LES~~)

(U//~~LES~~)

UNCLASSIFIED//~~LES~~
Domestic Investigations and Operations Guide

(U//~~LES~~)

b7E

(U//~~LES~~)

(U//~~LES~~) Note:

7.4. (U//~~LES~~)

(U//~~LES~~)

(U//~~LES~~) Approval:

(U//~~LES~~) Note:

UNCLASSIFIED//~~LES~~
Domestic Investigations and Operations Guide

7.5. (U//~~LES~~) [Redacted]
[Redacted]

b7E

(U//~~LES~~) [Redacted]
[Redacted]

(U//~~LES~~) [Redacted]
[Redacted]

(U//~~LES~~) Note: [Redacted]
[Redacted]

7.6. (U//~~LES~~) [Redacted]
[Redacted]

(U//~~LES~~) [Redacted]
[Redacted]

(U//~~LES~~) Note: [Redacted]
[Redacted]

(U//~~LES~~) [Redacted]
[Redacted]

(U//~~LES~~) [Redacted]
[Redacted]

(U//~~LES~~) Note: [Redacted]
[Redacted]

UNCLASSIFIED//~~LES~~
Domestic Investigations and Operations Guide



b7E

(U//~~LES~~) As stated in subsection 7.1 of this appendix, this requirement does not apply to national security investigations.

8. (U) DIOG Appendix L -Quick Reference Guide (QRG)

DIOG Appendix L – Investigations Conducted Online by an FBI Employee QRG

9. (U) Key Terms and Definitions

(U) [REDACTED]

(U) **Employee:** Employee, as used in this appendix, is intended to be inclusive of FBI SAs, intelligence analysts (IA), OCEs, UCEs, and any other FBI employee engaged in activities authorized by the AGG-Dom and the DIOG, as well as any task force personnel, assignees, or detailees to the FBI who are expected to follow FBI operational policies when working on behalf of the FBI, as delineated by the cooperative agreement, memorandum, or other contract under which they are operating.

(U) [REDACTED]

b7E

(U) **Online covert employee:** a trained and certified employee of the FBI or a sworn law enforcement officer of a federal, state, or local law enforcement agency, working under the direction and control of the FBI, whose identity as an employee of the FBI or another law enforcement agency is concealed from third parties (subjects or persons of investigative interest) with whom the OCE is engaged in substantive online interactions and communications, usually in the context of a UCO. [REDACTED]

(U) [REDACTED]

(U) **Publicly available information:** information that has been published or broadcast for public consumption, is available on request to the public, is available to the public by subscription or purchase, is made available at a meeting open to the public, or is obtained by visiting any place or attending any event that is open to the public. For a further discussion regarding online publicly available information, see DIOG 18.5.1.

(U) **Real-time communication:** A key factor to determining if an exchange is occurring in real time is whether the exchange is preserved and made available later on the site to viewers. Forums where the communications are preserved for future viewers are generally not real time. Typically, a blog or bulletin board system preserves posted comments to enable future viewers to see the information, meaning that communications posted on these forums are not real time. Further, even when several contributors to a bulletin board site are using it to rapidly engage in an exchange, it is not a real-time forum, as the content enjoys some degree of permanency even though the information

Domestic Investigations and Operations Guide

may only be posted online for as little as a week. In contrast, a typical chat room is designed to allow only users currently in the room to view the exchange and does not preserve the exchange for those entering the room at a later point in time. Examples of real-time communications include most chat rooms, instant messaging, and Skype. These modes of communication are still considered real-time even if they are stored and accessible at a later date, because obtaining that information at a later date would require legal process. If the information remains on the online environment, and legal process is not required to obtain the contents, is it not considered real-time communications.

(U)

[Redacted]

b7E

[Redacted]

1. (U//~~LES~~) DIOG Appendix L -Quick Reference Guide (QRG)

INVESTIGATIVE AUTHORITY	ONLINE ACTIVITY
Authorized Activities Conducted Online Prior to Opening an Assessment	• Public information (DIOG 5.1.1.1) • Publicly available information on the Internet [redacted] [redacted] • Public chat rooms [redacted] • Obtaining identifying information about users or networks • Information restricted to law enforcement • [redacted]
Authorized Investigative Methods Conducted Online-Assessments	Everything above AND • Publicly available information (DIOG 18.5.1) [redacted] [redacted] • [redacted] • [redacted] • [redacted] • CHS use and recruitment (DIOG 18.5.5) • Tasking a CHS/consenting party to access a restricted Web site ○ Access is authorized ○ Consensual recording of restricted site's communications is prohibited in an assessment • [redacted] [redacted] (DIOG 18.5.6.1) • Interacting with the public while in a nonaffiliated status

b7E

b7E

INVESTIGATIVE AUTHORITY	ONLINE ACTIVITY
	• Recording of real-time communications in assessments (distinction between public and private) • Monitor public real-time communications in assessments (recording permitted if FBI) • Employee/CHS/consenting party is present • Monitor private real-time communications in assessments (recording not permitted)
Investigative Methods Conducted Online-Predicated	Everything above AND • Consensual recording of communications (DIOG 18.6.1) • Private, real-time online communications in predicated investigations • Intercepting the communications of a computer trespasser (DIOG 18.6.2) • Undercover activity (UCA) (DIOG 18.6.13.3) • Undercover operations (DIOG 18.6.13.3) •

b7E

UNCLASSIFIED – ~~FOR OFFICIAL USE ONLY~~
Domestic Investigations and Operations Guide

M APPENDIX M: (U) THE FAIR CREDIT REPORTING ACT (FCRA)

(U) (*Note:* The policy for The Fair Credit Reporting Act was not completed by the time of the DIOG publication. It will be linked in the DIOG once approved.)

This Page is Intentionally Blank

UNCLASSIFIED – ~~FOR OFFICIAL USE ONLY~~
Domestic Investigations and Operations Guide

N APPENDIX N: (U) FEDERAL TAXPAYER INFORMATION (FTI)

N.1 (U) SUMMARY

(U//~~FOUO~~) During the course of criminal investigations, the Federal Bureau of Investigation (FBI) often requests taxpayer records from the Internal Revenue Service (IRS) via *ex parte* orders. The Internal Revenue Code (IRC) reinforces the confidentiality of the relationship between the taxpayer and the IRS by making it a crime to violate that confidence. The sanctions of the IRC are designed to protect the privacy of taxpayers. Information obtained by the FBI directly from the IRS must be protected in accordance with the provisions of the IRC and IRS Publication 1075.⁵⁸ This appendix provides guidance on the proper procedures for obtaining, handling, and protecting the federal taxpayer information (FTI) received by the FBI directly from the IRS. As a condition of receiving FTI, the FBI is statutorily obligated to properly protect the information in accordance with the safeguarding provisions established under Title 26 United States Code (U.S.C.) Section (§) 6103(p)(4), the “Internal Revenue Code” (IRC hereafter referred to as “Code”). All FBI personnel who handle FTI must be familiar with these procedures and requirements. FBI personnel includes all FBI employees, applicants, contractors, consultants, interns, task force personnel, and other government agency (OGA) personnel detailed to the FBI in the course of their assigned duties.

(U//~~FOUO~~) The Code permits the IRS⁵⁹ to disclose tax returns and return information to certain federal, state, and local agencies, but only to the extent that such disclosure is specifically authorized within § 6103 of the Code. It is the responsibility of FBI personnel who handle FTI to comply with all requirements of 26 U.S.C. § 6103. All agencies receiving such information are prohibited from unlawfully disclosing such information. The IRS commonly refers to this category of information as “Federal Taxpayer Information” or “FTI.”⁶⁰ Agencies are statutorily obligated to properly protect this information in accordance with the safeguarding provisions established under 26 U.S.C. § 6103(p)(4). The information may only be accessible to persons whose duties or responsibilities require access and to whom disclosure is available under the statute. The FBI is required to establish a system of records relating to each request and receipt of information, as well as a secure area for storage with restricted access to that area and the information stored there. Once the information is no longer needed, the IRS requires that the FTI be disposed of in accordance with the Code’s requirements.⁶¹

(U//~~FOUO~~) Many FBI investigations involve “joint task forces” and may include the cooperation of state and local law enforcement authorities. Section 6103(i) of the Code does not authorize disclosure of tax information to nonfederal investigators, even if they are formally assigned to a federal task force, unless they qualify as federal employees. State and local task force officers who are deputized qualify as federal employees.

⁵⁸ (U) *Tax Information Security Guidelines for Federal, State and Local Agencies and Entities* (August 24, 2010) (IRS Pub.1075).

⁵⁹ (U) Specifically, the statute refers to the Secretary of the United States Department of the Treasury; however, throughout this document, all references to the IRS mean the Secretary of the Treasury.

⁶⁰ (U) See § 1.1 of IRS Pub. 1075.

⁶¹ (U) *Id.* at § 8, Disposal of Federal Tax Information. See also 26 U.S.C. § 6103(p)(4)(F).

(U//~~FOUO~~) The FBI can only accept FTI from the IRS or another agency when it is disclosed in accordance with an authority provided under the statute for disclosure of FTI. FTI can be received and used by several units within the FBI for the same case and purpose; however, safeguarding responsibilities must be centralized with consistent standards.

(U//~~FOUO~~) Any agency that receives FTI for an authorized use may not use that information in any manner or for any purpose not consistent with the authorized use.⁶² If the FBI requires FTI for a different authorized use under the Code, a separate request must be made. An unauthorized secondary use of information is specifically prohibited and may result in discontinuation of disclosures by the IRS and the imposition of civil and or criminal penalties on the responsible official.

N.2 (U) APPLICATION

(U//~~FOUO~~) FTI may be acquired from the IRS during a predicated investigation for use in any judicial or administrative proceeding pertaining to the enforcement of a federal criminal statute other than tax administration to which the United States or the FBI is a party.⁶³

(U//~~FOUO~~) Tax information acquired directly from the IRS is considered FTI and is protected under the IRC's confidentiality protections. [REDACTED]

b7E

N.3 (U) DEFINITIONS

N.3.1 (U) *FEDERAL TAX INFORMATION*

(U//~~FOUO~~) Information that is protected under the confidentiality provisions of 26 U.S.C. § 6103 is referred to as FTI and includes all information relating to the taxpayer that is received by the Department of the Treasury (hereinafter referred to as "IRS"). It specifically includes information obtained by the IRS from third parties, including informants [confidential human sources]; information derived from those third-party submissions; and the work product of the IRS in determining, assessing, and collecting taxes or investigating taxpayer criminality.

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

[REDACTED] The IRS guidelines for confidentiality protection apply specifically to information that agencies receive directly from the IRS.

N.3.2 (U) *RETURN*

(U//~~FOUO~~) As defined in 26 U.S.C. § 6103(b)(1), "The term 'return' means any tax or information return, declaration of estimated tax, or claim for refund" filed with the IRS and any amendments such as "supporting tax schedules, attachments, or lists which are supplemental to, or part of, the return so filed."

N.3.3 (U) *RETURN INFORMATION*

(U//~~FOUO~~) Return information is defined as any information (other than the return filed by the taxpayer) that is filed with the IRS by sources other than the taxpayer [REDACTED]

⁶² (U) IRS Publication 1075, § 2.2 ("Need and Use").

⁶³ (U) 26 U.S.C. § 6103(i)(A).

[REDACTED]

These documents become part of the individual's file and are maintained by the IRS for tax purposes.

N.3.4 (U//~~FOUO~~) TAXPAYER RETURN INFORMATION

(U//~~FOUO~~) Taxpayer return information is information filed with, or furnished to, the IRS by, or on behalf of, a taxpayer.⁶⁴ (See N.3.3. above.) [REDACTED]

[REDACTED]

(U//~~FOUO~~) “The term ‘taxpayer return information’ means return information as defined in paragraph (2) which is filed with, or furnished to, the Secretary by or on behalf of the taxpayer to whom such return information relates.” (26 U.S.C. § 6103 (b)(3))

N.3.5 (U//~~FOUO~~) RETURN INFORMATION (INFORMATION RETURNS) OTHER THAN TAXPAYER RETURN INFORMATION (OTRI)

(U//~~FOUO~~) OTRI includes return information that was NOT provided to the IRS by, or on behalf of, a taxpayer. It includes information obtained from third parties who are not representatives of the taxpayer and extends to the following types of information:

1. The books and records of a named taxpayer supplied to the IRS by a third party
2. The portion of an interview between the IRS agent and a third party discussing a named taxpayer
3. Information developed by IRS agents in the course of investigating a named taxpayer's return from sources other than a taxpayer's representative acting on behalf of the taxpayer
4. The fact that a named taxpayer filed or failed to file a return

N.3.6 (U) DERIVATIVE TAX INFORMATION

(U//~~FOUO~~) Any information taken from records obtained directly from the IRS retains its original classification as FTL. [REDACTED]

[REDACTED]

(U//~~FOUO~~) **Example:** [REDACTED]

[REDACTED]

⁶⁴ (U) See 26 U.S.C. § 6103(b)(3).

N.4 (U) DEPARTMENT OF JUSTICE (DOJ) REQUIREMENTS FOR OBTAINING AND SAFEGUARDING FTI⁶⁵

(U//~~FOUO~~) In order to receive tax information from the IRS, 26 U.S.C. § 6013 requires that the DOJ establish and maintain the following, to the satisfaction of the IRS:

1. (U//~~FOUO~~) A permanent system of records, with respect to any requests and any disclosures of tax information.
2. (U//~~FOUO~~) A secure area or place where the information will be stored.
3. (U//~~FOUO~~) Restricted access to the information by those individuals whose duties and responsibilities require such access and to whom disclosure may be made under the provisions in the Code.
4. (U//~~FOUO~~) Any other safeguards that the IRS determines to be necessary to protect the confidentiality of the information.
5. (U//~~FOUO~~) A report must be furnished to the IRS, containing information describing the procedures established and utilized for ensuring the confidentiality of tax information, as required by the IRS.

N.5 (U) DISCLOSURE TO FEDERAL OFFICERS OR EMPLOYEES FOR ADMINISTRATION OF FEDERAL LAWS NOT RELATING TO FEDERAL TAX ADMINISTRATION

N.5.1 (U) LEGAL PROCESS FOR OBTAINING FTI IN FBI INVESTIGATIONS

(U//~~FOUO~~) The IRS may disclose return and return information to federal officers or employees for use in criminal investigations unrelated to tax administration. FTI may be obtained from the IRS via *ex parte* order or written request from the head of the agency, either the Director of the FBI or a United States attorney (USA), for purposes of FBI investigations. It **cannot** be obtained from the IRS via grand jury subpoena or administrative subpoena. In certain circumstances, the IRS may elect to voluntarily provide the FBI with FTI in order to report possible violations of criminal law or in an emergency situation within the FBI's jurisdiction.

N.5.1.1 (U) EX PARTE ORDERS (26 U.S.C. § 6103(i)(1))

(U//~~FOUO~~) An application for an *ex parte* order may be submitted by the Attorney General, the Deputy Attorney General, the Associate Attorney General, any Assistant Attorney General, any USA, a special prosecutor appointed under 28 U.S.C. § 593, or any attorney in charge of a criminal division organized crime strike force (28 U.S.C. § 593). Prior to submitting an application for an *ex parte* order, the responsible official should notify the appropriate IRS district director that such an action is being planned.⁶⁶ The notice should include all relevant details so that the IRS can assemble the requested information and make

⁶⁵ (U) See DOJ Order 2620.5A, *Safeguarding Tax Returns and Tax Return Information* (February 23, 1981).

⁶⁶ (U) This responsibility would most likely rest with the United States Attorney's Office (USAO) prosecuting the case.

an appropriate determination, taking into consideration whether the disclosure would impair any civil or criminal tax investigation or reveal the identity of a confidential informant.

(U//~~FOUO~~) An *ex parte* disclosure will be granted by the court to provide information to all personnel who are personally and directly engaged in the preparation of any judicial or administrative proceeding pertaining to the enforcement of federal criminal statutes unrelated to tax administration; any investigation that may result in such a proceeding; or any federal grand jury proceeding pertaining to enforcement of criminal statutes. The information may only be used by those officers and employees.

(U//~~FOUO~~) The assistant United States attorney (AUSA) working with the FBI will prepare the order for the signature of the USA. A judge or magistrate may grant such an application for an order if there is a finding based upon the facts submitted that there is reasonable cause to believe that:⁶⁷

1. (U//~~FOUO~~) A specific crime has been committed.
2. (U//~~FOUO~~) The return or return information is or may be relevant to a matter relating to the commission of that crime.
3. (U//~~FOUO~~) The information is sought exclusively for use in a federal investigation, and the information cannot reasonably be obtained from another source.

(U//~~FOUO~~) Language in the application and order should track the statutory language as closely as possible, listing every statutory violation for which “reasonable cause” exists to request these records. [REDACTED]

b7E

[REDACTED]

(U//~~FOUO~~) Tax return information received pursuant to an *ex parte* order is limited for use solely for the incident, threat, or activity described in the application to the court.⁶⁸ FTI obtained via *ex parte* order may only be used by the employees working on the investigation(s) described in the *ex parte* application. The information cannot be shared among case files or among FBI squads investigating separate cases. A separate *ex parte* order must be obtained if the FTI is needed for a different investigation not described in the original *ex parte* application. Due to the sensitivity of tax information and the penalties that attach to the unauthorized inspection and dissemination of this information, FBI employees should consult with their chief division counsels (CDC) and the Office of the General Counsel (OGC), as needed, prior to requesting an *ex parte* order from an AUSA.

N.5.1.2 (U) WRITTEN REQUEST (LETTERHEAD)

(U//~~FOUO~~) A letterhead request may be made to the IRS by the Director of the FBI to obtain information “other than taxpayer return information.”⁶⁹ The IRS may disclose this information to the Director of the FBI, in writing, if the information may constitute evidence of a violation of any federal criminal law within the investigative jurisdiction of the FBI. The request must be made in writing to the appropriate IRS district director by the Director of the FBI (see 26 U.S.C. § 6103(i)(1)). The request must be for the intended use and must set forth the taxpayer’s name and address, the taxable periods for which the information is sought, the

⁶⁷ (U) 26 U.S.C. § 6103(i)(1)(B).

⁶⁸ (U//~~FOUO~~) This information is available in a Preliminary or Full Investigation.

⁶⁹ (U) 26 U.S.C. § 6103(i)(2)(A).

statutory authority under which the enforcement proceeding is being conducted, and the specific reason(s) why the information sought is relevant to the enforcement proceeding, and it must indicate that the agency is directly engaged in preparing for a judicial or administrative proceeding, an investigation which may result in such a proceeding, or a grand jury proceeding (see 26 U.S.C. § 6103(i)(1)(A)(iii)). The Secretary of the Treasury shall disclose this information to officers and employees of the FBI who are personally and directly engaged in the investigation solely for their use as needed to enforce such law.

(U//~~FOUO~~) This information is limited to the taxpayer's name, address, and SSN; whether a tax return has or has not been filed within the last three years; or the name and address of any individual who filed from a particular address for a requested period of time. If the information may constitute evidence of a violation by any taxpayer of any federal criminal law unrelated to tax administration, then the taxpayer's identity may also be disclosed (26 U.S.C. § 6103(i)(3)).

**N.5.1.3 (U) DISCLOSURE OF RETURN INFORMATION BY THE IRS
RELATED TO CRIMINAL, TERRORIST ACTIVITIES OR
EMERGENCY CIRCUMSTANCES (26 U.S.C. § 6103(i)(3))**

N.5.1.3.1 (U) POSSIBLE VIOLATIONS OF FEDERAL CRIMINAL LAW

(U//~~FOUO~~) Generally, the IRS may voluntarily disclose in writing, without a request, return information (OTRI) that may constitute evidence of a violation of any federal criminal law that does not involve tax administration in order to notify the head of the federal agency responsible for enforcement of that violation. If there is return information other than OTRI that may constitute evidence of such a crime, the taxpayer's identity may also be disclosed under that provision. Upon receipt of this information, the Director of the FBI may disclose the information to the officers and employees who are working or will be assigned to the investigation.

N.5.1.3.2 (U) EMERGENCY CIRCUMSTANCES⁷⁰

(U//~~FOUO~~) In circumstances where there is an imminent danger of death or physical injury to any individual, the IRS may voluntarily disclose return information to the extent necessary to apprise appropriate officers or employees of a federal or state law enforcement agency.

(U//~~FOUO~~) In situations involving fugitives (flight from federal prosecution) a voluntary disclosure of return information may be made by the IRS to apprise the appropriate law enforcement agency.

**N.5.1.3.3 (U) DISCLOSURE BY THE IRS OF INFORMATION RELATING TO
TERRORIST ACTIVITIES (26 U.S.C. § 6103(i)(3)(C))**

(U//~~FOUO~~)

b7E

⁷⁰ (U) 26 U.S.C. § 6103(i)(3)(C).

N.5.2 (U) **TERRORISM INVESTIGATIONS**

N.5.2.1 (U) **FBI APPROVAL REQUIREMENTS FOR OBTAINING FTI VIA AN
EX PARTE ORDER IN TERRORISM CASES**

(U//~~FOUO~~)

(U//~~FOUO~~)

b7E

(U//~~FOUO~~)

(U//~~FOUO~~)

(U//~~FOUO~~)

(U//~~FOUO~~)

(U//~~FOUO~~)

UNCLASSIFIED – ~~FOR OFFICIAL USE ONLY~~
Domestic Investigations and Operations Guide

[Redacted]

b7E

N.5.2.2 (U) WRITTEN REQUEST RELATED TO TERRORIST ACTIVITIES

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

[Redacted]

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

[Redacted]

- (U) [Redacted]
- (U) [Redacted]
- (U) [Redacted]
- (U) [Redacted]
- (U) [Redacted]
- (U) [Redacted]
- (U) [Redacted]
- (U) [Redacted]
- (U) [Redacted]

b7E

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

[Redacted]

⁷¹ (U) 26 U.S.C. § 6103(i)(7)(A).

⁷² (U//~~FOUO~~) Case ID [Redacted]

b7E

N.5.3 (U) **BACKGROUND INVESTIGATION REQUESTS**

(U//~~FOUO~~) The IRS may disclose the return of any taxpayer, or return information with respect to such taxpayer, to such individuals as the taxpayer may designate in a request for, or consent to, disclosure for the purposes of background investigations for employment.

(U//~~FOUO~~) In addition, § 6103(g)(1) and (2) discuss disclosure to the President and certain other persons provided for in the statute. It provides for disclosure of return information to Presidential appointees and certain other federal government appointees. Upon written request of the President or the head of any federal agency, the IRS may disclose to an authorized representative of the Executive Office of the President, federal agency head, or the FBI, return information with respect to an individual under consideration for an appointment to a position in the executive or judicial branch of the federal government. The information shall be limited to whether the individual has filed returns for the preceding three years; has failed to pay any tax within ten days after notice and demand; has been assessed a penalty in the current year or preceding three years; has been under investigation for possible criminal offenses under the internal revenue laws and the results of such an investigation; or has been assessed any civil penalty under the internal revenue laws for fraud. Within three days of receipt of the request for this information, the Secretary of the Treasury shall notify the individual in writing that the information has been requested under the Code.

(U//~~FOUO~~) The employee who receives this information from the Secretary may not disclose such information to any other person except the President or the head of the federal agency without the written direction of the President or head of the federal agency.

N.5.4 (U) **INFORMATION OBTAINED FROM STATE TAX ADMINISTRATION/AGENCY**

(U//~~FOUO~~) Information requested and obtained from state tax authorities is not considered FTI, and the requirements of Title 26 of the IRS Code do not apply to these types of records. However, each state may have specific requirements concerning the procedures for obtaining and maintaining these types of official records pertaining to their taxpayers. Many state tax returns are also protected by antidisclosure laws that are closely patterned after § 6103 of the Code. State returns may not be available through subpoenas, and the AUSA's access to them may not be covered by exceptions to the state disclosure laws. If the investigation demonstrates a need for these records, agents should consult with their CDC and local USAOs or state prosecutors to determine the appropriate methods for obtaining and safeguarding these records in compliance with state requirements.

N.5.5 (U) **OTHER THAN FTI**

(U//~~FOUO~~) Tax information obtained directly from an individual or from that individual's tax preparer [REDACTED] is not covered by the statutory requirements set forth in the Code and does not require the same treatment as FTI.

b7E

N.6 (U) HANDLING, STORING, AND SAFEGUARDING FTI

(U//~~FOUO~~) The IRS requires that certain specific safeguards be employed by an agency for the protection of FTI.⁷³ FTI must be protected from unauthorized disclosure to persons who do not possess the need to know. Access must be limited only to those individuals working on the specific case for which the FTI was requested, and the requested FTI may only be used for the specific reason that it was requested. If the FTI is to be used for a different purpose, a new request must be filed under a different provision of 26 U.S.C. § 6103.

(U//~~FOUO~~) The information must be protected using minimum protection standards, as defined in the Internal Revenue Code. This method establishes the minimum standards that will be applied on a case-by-case basis, considering local circumstances to determine space and containers for the basic framework of minimum security requirements. [REDACTED]

b7E

[REDACTED]

(U//~~FOUO~~) All tax information must be maintained in accordance with the requirements of the *United States Attorney's Manual* (Sections 3-6.300), DOJ Order 2620.5A (February 23, 1981), and the memorandum from the Executive Office for United States Attorneys (EOUSA) Director, entitled "Maintenance of Tax Returns and Return Information" (August 23, 1996) [REDACTED]

[REDACTED]

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

N.6.1 (U) TRACKING FTI

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

[REDACTED]

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

⁷³ (U) For more information, see *Tax Information Security Guidelines for Federal, State and Local Agencies* (August 24, 2010), IRS Publication 1075, available on the IRS website: www.irs.gov and on the Security Division Intranet site.

UNCLASSIFIED – ~~FOR OFFICIAL USE ONLY~~
Domestic Investigations and Operations Guide

(U//~~FOUO~~) All original FTI received from the IRS, both electronic and hard copies, must be protected in accordance with the guidance referenced above. [REDACTED]

b7E

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

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

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

N.6.2 (U) *MARKING FTI*

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

b7E

N.6.3 (U) *HANDLING AND TRANSPORTING OF FTI*

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

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

N.7 (U) *REMOVABLE ELECTRONIC MEDIA*

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

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

[REDACTED]

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

[REDACTED]

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

[REDACTED]

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

[REDACTED]

N.8 (U) DISPOSAL OF MATERIAL UPON DISPOSITION OF CASE

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

[REDACTED]

(U) [REDACTED]

[REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]

(U) [REDACTED]

(Note) [REDACTED]

[REDACTED]

N.8.1. (U) RETURN OF FTI

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

[REDACTED]

1. [REDACTED]
2. [REDACTED]

⁷⁴ (U) See IRS Publication 1075, subsection 8.3.

3. [REDACTED]
[REDACTED]

(U) [REDACTED]
[REDACTED]

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

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

N.8.1 (U) *FINAL DISPOSITION OF FTI SERIALIZED* [REDACTED]

(U) [REDACTED]

[REDACTED]

N.9 (U) TRAINING AND CERTIFICATION

(U//~~FOUO~~) All FBI employees, detailees, and contractors who could potentially come in contact with FTI are required to complete annual training on the proper safeguarding of FTI.

(U//~~FOUO~~) Annually, each field office or division will certify, by EC to the SecD Strategy, Policy, and Information Security Unit that all appropriate individuals have completed the FTI training on Virtual Academy.

(U//~~FOUO~~) The training provided before the initial certification, and annually thereafter, must also cover the incident response policy and procedures for reporting unauthorized disclosures and data breaches.

⁷⁵ (U) See Publication 1075, subsection 8.4.

This Page is Intentionally Blank

~~UNCLASSIFIED – FOR OFFICIAL USE ONLY~~
Domestic Investigations and Operations Guide

O APPENDIX O: (U) RIGHT TO FINANCIAL PRIVACY ACT (RFPA)

(U) (*Note:* The policy for the Right to Financial Privacy Act was not completed by the time of the DIOG publication. It will be linked in the DIOG once approved.)

This Page is Intentionally Blank

UNCLASSIFIED – ~~FOR OFFICIAL USE ONLY~~
Domestic Investigations and Operations Guide

b6
b7C

P APPENDIX P: (U) ACRONYMS

A/EAD	Associate Executive Assistant Director
AD	Assistant Director
ADD	Associate Deputy Director
ADIC	Assistant Director-in-Charge
AFID	Alias False Identification
AG	Attorney General
AGG	Attorney General Guidelines
AGG-CHS	Attorney General Guidelines Regarding the Use of FBI Confidential Human Sources
AGG-Dom	Attorney General's Guidelines for Domestic FBI Operations
AGG-UCO	The Attorney General's Guidelines on FBI Undercover Operations
AOR	Area of Responsibility
ARS	Assessment Review Standards
ASAC	Assistant Special Agent in Charge
ASC	Assistant Section Chief
ATF	Bureau of Alcohol, Tobacco, Firearms and Explosives
AUSA	Assistant United States Attorney
CALEA	Communications Assistance for Law Enforcement Act
CCRSB	Criminal Cyber Response and Services Branch
CD	Counterintelligence Division
CDC	Chief Division Counsel
C.F.R.	Code of Federal Regulations
CHS	Confidential Human Source
CHSPG	Confidential Human Source Policy Implementation Guide

UNCLASSIFIED – ~~FOR OFFICIAL USE ONLY~~
Domestic Investigations and Operations Guide

CIA	Central Intelligence Agency
CID	Criminal Investigative Division
CMS	Collection Management Section
CPO	Corporate Policy Office
CUORC	Criminal Undercover Operations Review Committee
CyD	Cyber Division
DAD	Deputy Assistant Director
DD	Deputy Director
DEA	Drug Enforcement Administration
DGC	Deputy General Counsel
DI	Directorate of Intelligence
DLAT	Deputy Legal Attache
DNI	Director of National Intelligence
DOD	Department of Defense
DOJ	Department of Justice
DOJ OEO	Office of Enforcement Operations, DOJ
DOS	Department of State
DPO	Division Policy Officer
EAD	Executive Assistant Director
EC	Electronic Communication
ECF	Electronic Case File
ECPA	Electronic Communication Privacy Act
ECS	Electronic Communication Service

b7E

UNCLASSIFIED – ~~FOR OFFICIAL USE ONLY~~
Domestic Investigations and Operations Guide

b7E

EI	Enterprise Investigation
ELSUR	Electronic Surveillance
EO	Executive Order
EOT	ELSUR Operations Technician
ERS	ELSUR Records System
ESN	Electronic Serial Number
ESU	DOJ OEO, Electronic Surveillance Unit
ETR	Electronic Technical Request
FBIHQ	FBI Headquarters
FGJ	Federal Grand Jury
FGUSO	Field Guide for Undercover and Sensitive Operations
FICP	Foreign Intelligence Collection Program
FIG	Field Intelligence Group
FISA	Foreign Intelligence Surveillance Act
FISC	Foreign Intelligence Surveillance Court
FRCP	Federal Rules of Criminal Procedure
GC	General Counsel
HIPAA	Health Insurance Portability and Accountability Act
HSC	Homeland Security Council
ICE	Department of Homeland Security Immigration and Customs Enforcement
ICM	Investigative Case Management

UNCLASSIFIED – ~~FOR OFFICIAL USE ONLY~~
Domestic Investigations and Operations Guide

IINI	Innocent Images National Initiative
ILB	Investigative Law Branch
ILU	Investigative Law Unit
IOB	Intelligence Oversight Board
IOD	International Operations Division
IP Address	Internet Protocol Address
IPG	Intelligence Policy Implementation Guide
ISP	Internet Service Provider
ITSMV	Interstate Transportation of Stolen Motor Vehicles
JDA	Juvenile Delinquency Act
JTTF	Joint Terrorism Task Force
LEGAT	Legal Attaché
LHM	Letterhead Memorandum
LO	Lead Office
MAR	Monthly Administrative Report
MLAT	Mutual Legal Assistance Treaties
MOU/MOA	Memorandum of Understanding/Agreement
MSIN	Mobile Station Identification Number
NARA	National Archives and Records Administration
NCMEC	National Center for Missing and Exploited Children
NISS	National Information Sharing Strategy
NSB	National Security Branch
NSC	National Security Council
NSD	National Security Division, DOJ

UNCLASSIFIED – ~~FOR OFFICIAL USE ONLY~~
Domestic Investigations and Operations Guide

NSL	National Security Letter
NSLB	National Security Law Branch
NSSE	National Special Security Events
NSUCOPG	National Security Undercover Operations Policy Implementation Guide
OCA	Office of Congressional Affairs
OCRS	Organized Crime and Racketeering Section, DOJ
OGC	Office of the General Counsel
OIA	Otherwise Illegal Activity
OIC	Office of Integrity and Compliance
OIO	Office of Operations, DOJ
OLC	Office of Legal Counsel, DOJ
OO	Office of Origin
OPA	Office of Public Affairs
OTD	Operational Technology Division
PBDM	Pattern Based Data Mining
PCHS	Potential CHS
PCLU	Privacy and Civil Liberties Unit
PCTDD	Post Cut-through Dialed Digits
PFI	Positive Foreign Intelligence
PG	Policy Implementation Guide
PI	Preliminary Investigation
PIA	Privacy Impact Assessment
PIAB	President's Intelligence Advisory Board
PSA	Performance Summary Assessments

UNCLASSIFIED – ~~FOR OFFICIAL USE ONLY~~
Domestic Investigations and Operations Guide

PTA	Privacy Threshold Analysis
RA	Resident Agency
RF	Radio Frequency
RFPA	Right to Financial Privacy Act
RICO	Racketeer Influenced and Corrupt Organizations
RIG	Regional Intelligence Group
RMD	Records Management Division
SA	Special Agent
SAC	Special Agent-in-Charge
SC	Section Chief
SIA	Supervisory Intelligence Analyst
SIM	Sensitive Investigative Matter
SOG	Special Operations Group
SORC	Sensitive Operations Review Committee
SSA	Supervisory Special Agent
SSG	Special Surveillance Group
SSRA	Supervisory Senior Resident Agent
TFM	Task Force Member
TFO	Task Force Officer
TFP	Task Force Participant
TMD	Technical Management Database
TTA	Technically Trained Agent
UC	Unit Chief

b7E

UNCLASSIFIED – ~~FOR OFFICIAL USE ONLY~~
Domestic Investigations and Operations Guide

UCE	Undercover Employee
UCFN	Universal Case File Number
UCO	Undercover Operation
UCRC	Undercover Review Committee
UDP	Undisclosed Participation
UNI	Universal Index
USA	United States Attorney
USAO	United States Attorney's Office
U.S.C.	United States Code
USG	United States Government
USIC	United States Intelligence Community
USPER	United States Person, United States Persons, US PER, USPERs, US Person, US Persons, U.S. Person, U.S. Persons
USPS	United States Postal Service
USSS	United States Secret Service
VICAP	Violent Criminal Apprehension Program
VS	Victim Specialist
WITT	Wireless Intercept Tracking Technology
WMD	Weapons of Mass Destruction
WMDD	Weapons of Mass Destruction Directorate

This Page is Intentionally Blank

Q APPENDIX Q: (U) DEFINITIONS

(U//~~FOUO~~) Academic Nexus SIM: [REDACTED]

b7E

(U) Aggrieved Person: [REDACTED]

(U//~~FOUO~~) **Assessments:** The AGG-Dom authorizes as an investigative activity called an “Assessment” which requires an authorized purpose and articulated objective(s). The DIOG defines five types of Assessments that may be carried out to detect, obtain information about, or prevent or protect against federal crimes or threats to the national security or to collect foreign intelligence. Although “no particular factual predication” is required, the basis of an Assessment cannot be arbitrary or groundless speculation, nor can an Assessment be based solely on the exercise of First Amendment protected rights or on the race, ethnicity, gender, national origin, religion, sexual orientation, or gender identity of the subject, or a combination of only those factors.

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

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

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

(U) **Electronic Communications System:** Any wire, radio, electromagnetic, photo optical or photo electronic facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications.

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

(U//~~FOUO~~) Electronic Tracking Device: [REDACTED]

b7E

(U//~~FOUO~~) **Employee:** For purposes of the AGG-Dom and DIOG, an “FBI employee” includes, but not limited to, an operational/administrative professional staff person, intelligence analyst, special agent, task force officer (TFO), task force member (TFM), task force participant (TFP), detailee, and FBI contractor. An FBI employee is bound by the AGG-Dom and DIOG. The FBI employee definition excludes a confidential human source (CHS).

(U//~~FOUO~~) **Enterprise:** The term “enterprise” includes any individual, partnership, corporation, association, or other legal entity, and any union or group of individuals associated in fact although not a legal entity.

(U//~~FOUO~~) **Enterprise Investigation:** An Enterprise Investigation (EI) examines the structure, scope, and nature of the group or organization including: its relationship, if any, to a foreign power; the identity and relationship of its members, employees, or other persons who may be acting in furtherance of its objectives; its finances and resources; its geographical dimensions; its past and future activities and goals; and its capacity for harm. (AGG-Dom, Part II.C.2)

(U//~~FOUO~~) Enterprise Investigations are a type of Full Investigation and are subject to the same requirements that apply to Full Investigations described in Section 7. Enterprise Investigations focus on groups or organizations that may be involved in the most serious criminal or national security threats to the public, as described in Section 8. Enterprise Investigations cannot be conducted as Preliminary Investigations or Assessments, nor may they be conducted for the sole purpose of collecting foreign intelligence. [REDACTED]

b7E

(U//~~FOUO~~) **Extraterritorial Guidelines:** 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); (iv) *The Attorney General Procedure for Reporting and Use of Information Concerning Violations of Law and Authorization for Participation in Otherwise Illegal Activity in FBI Foreign Intelligence, Counterintelligence or International Terrorism Intelligence Investigations* (August 8, 1988); and (v) the *Memorandum of Understanding Concerning Overseas and Domestic Activities of the Central Intelligence Agency and the Federal Bureau of Investigation* (2005).

(U//~~FOUO~~) FISA: The Foreign Intelligence Surveillance Act of 1978, as amended. The law establishes a process for obtaining judicial approval of electronic surveillance, physical searches, pen register and trap and trace devices, and access to certain business records for the purpose of collecting foreign intelligence.

(U) For or On Behalf of a Foreign Power: The determination that activities are for or on behalf of a foreign power shall be based on consideration of the extent to which the foreign power is involved in control or policy direction; financial or material support; or leadership, assignments, or discipline.

(U) Foreign Computer Intrusion: The use or attempted use of any cyber-activity or other means, by, for, or on behalf of a foreign power to scan, probe, or gain unauthorized access into one or more United States-based computers.

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

(U) Foreign Intelligence Requirements:

- A) (U//~~FOUO~~) National intelligence requirements issued pursuant to authorization by the Director of National Intelligence, including the National Intelligence Priorities Framework and the National HUMINT Collection Directives, or any successor directives thereto;
- B) (U//~~FOUO~~) Requests to collect foreign intelligence by the President or by Intelligence Community officials designated by the President; and
- C) (U//~~FOUO~~) Directions to collect foreign intelligence by the Attorney General, the Deputy Attorney General, or an official designated by the Attorney General.

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

(U) Full Investigation: A Full Investigation may be opened if there is an “articulable factual basis” for the investigation that reasonably indicates one of the following circumstances exists:

(U) An activity constituting a federal crime or a threat to the national security has or may have occurred, is or may be occurring, or will or may occur and the investigation may obtain information relating to the activity or the involvement or role of an individual, group, or organization in such activity;

- A) (U) An individual, group, organization, entity, information, property, or activity is or may be a target of attack, victimization, acquisition, infiltration, or recruitment in connection with criminal activity in violation of federal law or a threat to the national security and the investigation may obtain information that would help to protect against such activity or threat; or
- B) (U) The investigation may obtain foreign intelligence that is responsive to a PFI requirement, as defined in DIOG Section 7.4.3.

UNCLASSIFIED – ~~FOR OFFICIAL USE ONLY~~
Domestic Investigations and Operations Guide

(U) All lawful investigative methods may be used in a Full Investigation.

(U) A Full Investigation of a group or organization may be opened as an Enterprise Investigation if there is an articulable factual basis for the investigation that reasonably indicates the group or organization may have engaged, or may be engaged in, or may have or may be engaged in planning or preparation or provision of support for:

A) (U) Racketeering Activity:

1) (U) A pattern of racketeering activity as defined in 18 U.S.C. § 1961(5);

B) (U) International Terrorism:

1) (U) International terrorism, as defined in the AGG-Dom, Part VII.J, or other threat to the national security;

C) (U) Domestic Terrorism:

1) (U) Domestic terrorism as defined in 18 U.S.C. § 2331(5) involving a violation of federal criminal law;

2) (U) Furthering political or social goals wholly or in part through activities that involve force or violence and a violation of federal criminal law; or

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

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

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

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

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



b7E

(U//~~FOUO~~) Operational Division or Operational Unit: “Operational” division or operational unit as used in the DIOG means the FBIHQ division or unit responsible for management and program oversight of the file classification for the substantive investigative matter (i.e.,

Assessment or Predicated Investigation). Previously referred to as the FBIHQ “substantive” division or substantive unit.

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

(U//~~FOUO~~) **Physical Surveillance (Not Requiring a Court Order):** The deliberate observation by an FBI employee of persons, places, or events, on either a limited or continuous basis, in areas where there is no reasonable expectation of privacy. *Note:* DIOG Section 18.5.8 makes a distinction between “casual observation” and physical surveillance, and specifies factors to be considered when determining whether a particular plan of action constitutes casual observation or physical surveillance. (See DIOG Section 18.5.8)

(U) **Preliminary Investigation:** A Preliminary Investigation is a type of Predicated Investigation authorized under the AGG-Dom that may be opened (predicated) on the basis of any “allegation or information” indicative of possible criminal activity or threats to the national security. Preliminary Investigations may be opened to detect, obtain information about, or prevent or protect against federal crimes or threats to the national security [REDACTED]

b7E

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

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

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

(U) **Records:** Any records, databases, files, indices, information systems, or other retained information.

(U) **Relevance:** Information is relevant if it tends to make a fact of consequence more or less probable.

(U//~~FOUO~~) **Remote Computing Services:** [REDACTED]

b7E

(U//~~FOUO~~) **Sensitive Investigative Matter:** An investigative matter involving a domestic public official, domestic political candidate, religious or domestic political organization or individual prominent in such an organization, or news media, or an investigative matter having academic nexus, or any other matter which, in the judgment of the official authorizing an investigation, should be brought to the attention of FBIHQ and other DOJ officials.

(U) Sensitive Monitoring Circumstance: Investigation of a member of Congress, a federal judge, a member of the Executive Branch at Executive Level IV or above, or a person who has served in such capacity within the previous two years; (*Note:* Executive Levels I through IV are defined in 5 U.S.C. §§ 5312-5315.)

- A) (U) Investigation of the Governor, Lieutenant Governor, or Attorney General of any state or territory, or a judge or justice of the highest court of any state or territory, concerning an offense involving bribery, conflict of interest, or extortion related to the performance of official duties;
- B) (U) A party to the communication is in the custody of the Bureau of Prisons or the United States Marshals Service or is being or has been afforded protection in the Witness Security Program; or
- C) (U) The Attorney General, the Deputy Attorney General, or an Assistant Attorney General has requested that the FBI obtain prior approval for the use of consensual monitoring in a specific investigation.

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

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

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

(U//~~FOUO~~) Surveillance:

- A) (U//~~FOUO~~) **Electronic surveillance (ELSUR)** - under Title III and FISA 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.

b7E

- B) (U//~~FOUO~~) **Consensual monitoring of communications, including consensual computer monitoring, or electronic surveillance (ELSUR)** - where there is no reasonable expectation of privacy is permitted in Predicated Investigations. These methods usually do not require court orders or warrants unless they involve an intrusion into an area where there is a reasonable expectation of privacy or non-consensual monitoring of communications, but legal review is generally required to ensure compliance with legal requirements.

Domestic Investigations and Operations Guide

(U//~~FOUO~~) **Physical surveillance** - is the deliberate observation by an FBI employee of persons, places, or events, on either a limited or continuous basis, in areas where there may or may not be a reasonable expectation of privacy. (See DIOG Section 18.5.8 for physical surveillance in situations not requiring a court order and a discussion of the distinction between physical surveillance and casual observation). Factors to consider in determining whether observations are casual observation or physical surveillance include:

b7E

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

(U//~~FOUO~~) **Trap and Trace Device:** Captures the incoming electronic or other impulses that identify the originating number or other dialing, routing, addressing or signaling information reasonably likely to identify the source of a wire or electronic communication, provided that such information does not include the contents of any communication.

(U//~~FOUO~~) **Undercover Activity:** An “undercover activity” is any investigative activity involving the use of an assumed identity by an undercover employee for an official purpose, investigative activity, or function.

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

(U//~~FOUO~~) **Undercover Operation:** An “undercover operation” is an operation that involves a series of related “undercover activities” over a period of time by an “undercover employee.” A series of related undercover activities consists of more than five separate substantive contacts by an undercover employee with the individuals under investigation.

b7E

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

(U) United States Person (USPER): Any of the following, but not including any association or corporation that is a foreign power, defined as an entity that is openly acknowledged by a foreign government or governments to be directed and controlled by such foreign government or governments:

- A) (U) An individual who is a United States citizen or an alien lawfully admitted for permanent residence;
- B) (U) An unincorporated association substantially composed of individuals who are United States persons (USPERs); or
- C) (U) A corporation incorporated in the United States.

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

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

This Page is Intentionally Blank

UNCLASSIFIED – FOR OFFICIAL USE ONLY

Domestic Investigations and Operations Guide

b6
b7C

R APPENDIX R: (U) SUPERSEDED DOCUMENTS AND NFIPM, MIOG, AND MAOP SECTION

(U//FOUO) This guide supersedes the following FBI policies and procedures:

Part	Section	Section Title	DIOG Supersession
MIOG Intro	Preface	Section: Preface (1)	DIOG Preamble
MIOG Intro	Preface	Preface	DIOG Preamble
MIOG Intro	Section 1	Section: S1: Investigative Authority and Responsibility (12)	DIOG Preamble
MIOG Intro	Section 1	1-1 AUTHORITY OF A SPECIAL AGENT	DIOG Preamble
MIOG Intro	Section 1	1-2 INVESTIGATIVE RESPONSIBILITY	DIOG Preamble
MIOG Intro	Section 1	1-3 THE ATTORNEY GENERALS GUIDELINES ON GENERAL CRIMES, RACKETEERING ENTERPRISE AND TERRORISM ENTERPRISE INVESTIGATIONS	DIOG Preamble
MIOG Intro	Section 1	1-3 INTRODUCTION	DIOG Preamble
MIOG Intro	Section 1	1-3I. GENERAL PRINCIPLES	DIOG Preamble
MIOG Intro	Section 1	1-3 II. GENERAL CRIMES INVESTIGATIONS	DIOG Preamble
MIOG Intro	Section 1	1-3 III. CRIMINAL INTELLIGENCE INVESTIGATIONS	DIOG Preamble
MIOG Intro	Section 1	1-3 IV. INVESTIGATIVE TECHNIQUES	DIOG Preamble
MIOG Intro	Section 1	1-3 V. DISSEMINATION AND MAINTENANCE OF INFORMATION	DIOG Preamble
MIOG Intro	Section 1	1-3 VI. COUNTERTERRORISM ACTIVITIES AND OTHER AUTHORIZATIONS	DIOG Preamble
MIOG Intro	Section 1	1-3 VII. RESERVATION	DIOG Preamble
MIOG Intro	Section 1	1-4 INVESTIGATIVE AUTHORITY AND THE FIRST AMENDMENT	DIOG Preamble
MIOG Intro	Section 2	Section : S2: Management and Allocation Programs (57)	DIOG Preamble
MIOG Intro	Section 2	2-1 NATIONAL PRIORITY PROGRAMS	DIOG Preamble

UNCLASSIFIED – ~~FOR OFFICIAL USE ONLY~~
Domestic Investigations and Operations Guide

Part	Section	Section Title	DIOG Supersession
MIOG Intro	Section 2	2-1.1 Foreign Counterintelligence (FCI)	DIOG Preamble
MIOG Intro	Section 2	2-1.1.1 Definition	DIOG Preamble
MIOG Intro	Section 2	2-1.1.2 Objective	DIOG Preamble
MIOG Intro	Section 2	2-1.2 Organized Crime	DIOG Preamble
MIOG Intro	Section 2	2-1.2.1 Definition	DIOG Preamble
MIOG Intro	Section 2	2-1.2.2 Objective	DIOG Preamble
MIOG Intro	Section 2	2-1.2.3 Ranking of Organized Criminal Activities	DIOG Preamble
MIOG Intro	Section 2	2-1.3 Drug	DIOG Preamble
MIOG Intro	Section 2	2-1.3.1 Definition	DIOG Preamble
MIOG Intro	Section 2	2-1.3.2 Objective	DIOG Preamble
MIOG Intro	Section 2	2-1.4 Counterterrorism	DIOG Preamble
MIOG Intro	Section 2	2-1.4.1 Definition	DIOG Preamble
MIOG Intro	Section 2	2-1.4.2 Objective	DIOG Preamble
MIOG Intro	Section 2	2-1.5 White-Collar Crime	DIOG Preamble
MIOG Intro	Section 2	2-1.5.1 Definition	DIOG Preamble
MIOG Intro	Section 2	2-1.5.2 Objective	DIOG Preamble
MIOG Intro	Section 2	2-1.5.3 Ranking of Activities	DIOG Preamble
MIOG Intro	Section 2	2-1.6 Violent Crimes and Major Offenders	DIOG Preamble
MIOG Intro	Section 2	2-1.6.1 Fugitive Subprogram	DIOG Preamble
MIOG Intro	Section 2	2-1.6.2 Government Reservation Crimes Subprogram	DIOG Preamble
MIOG Intro	Section 2	2-1.6.3 Interstate Theft Subprogram	DIOG Preamble
MIOG Intro	Section 2	2-1.6.4 Violent Crimes Subprogram	DIOG Preamble
MIOG Intro	Section 2	2-1.6.5 Violent Crimes and Major Offenders-Organized Crime Drug Enforcement Task Force Subprogram	DIOG Preamble
MIOG Intro	Section 2	2-2 OTHER PROGRAMS	DIOG Preamble

UNCLASSIFIED – ~~FOR OFFICIAL USE ONLY~~
Domestic Investigations and Operations Guide

Part	Section	Section Title	DIOG Supersession
MIOG Intro	Section 2	2-2.1 Deleted	DIOG Preamble
MIOG Intro	Section 2	2-2.1.1 Deleted	DIOG Preamble
MIOG Intro	Section 2	2-2.1.2 Deleted	DIOG Preamble
MIOG Intro	Section 2	2-2.1.3 Deleted	DIOG Preamble
MIOG Intro	Section 2	2-2.2 Applicant Investigations - Reimbursable and Nonreimbursable	DIOG Preamble
MIOG Intro	Section 2	2-2.2.1 Definition	DIOG Preamble
MIOG Intro	Section 2	2-2.2.2 Objective	DIOG Preamble
MIOG Intro	Section 2	2-2.2.3 Ranking of Activities	DIOG Preamble
MIOG Intro	Section 2	2-2.3 Civil Rights	DIOG Preamble
MIOG Intro	Section 2	2-2.3.1 Definition	DIOG Preamble
MIOG Intro	Section 2	2-2.3.2 Objective	DIOG Preamble
MIOG Intro	Section 2	2-2.3.3 Ranking of Activities	DIOG Preamble
MIOG Intro	Section 2	2-2.4 FBI Security Program	DIOG Preamble
MIOG Intro	Section 2	2-2.4.1 Definition	DIOG Preamble
MIOG Intro	Section 2	2-2.4.2 Objective	DIOG Preamble
MIOG Intro	Section 2	2-2.4.3 Ranking of Activities	DIOG Preamble
MIOG Intro	Section 2	2-2.5 Deleted	DIOG Preamble
MIOG Intro	Section 2	2-2.5.1 Deleted	DIOG Preamble
MIOG Intro	Section 2	2-2.5.2 Deleted	DIOG Preamble
MIOG Intro	Section 2	2-2.5.3 Deleted	DIOG Preamble
MIOG Intro	Section 2	2-2.6 Deleted	DIOG Preamble
MIOG Intro	Section 2	2-2.6.1 Deleted	DIOG Preamble
MIOG Intro	Section 2	2-2.6.2 Deleted	DIOG Preamble
MIOG Intro	Section 2	2-2.6.3 Deleted	DIOG Preamble
MIOG Intro	Section 2	2-2.7 Deleted	DIOG Preamble

UNCLASSIFIED – ~~FOR OFFICIAL USE ONLY~~
Domestic Investigations and Operations Guide

Part	Section	Section Title	DIOG Supersession
MIOG Intro	Section 2	2-2.7.1 Deleted	DIOG Preamble
MIOG Intro	Section 2	2-2.7.2 Deleted	DIOG Preamble
MIOG Intro	Section 2	2-2.7.3 Deleted	DIOG Preamble
MIOG Intro	Section 2	2-2.8 Deleted	DIOG Preamble
MIOG Intro	Section 2	2-2.8.1 Deleted	DIOG Preamble
MIOG Intro	Section 2	2-2.8.2 Deleted	DIOG Preamble
MIOG Intro	Section 2	2-2.8.3 Deleted	DIOG Preamble
MIOG I.I	Section 7	7-5 CLARIFICATION REGARDING AN INVESTIGATION AS OPPOSED TO A PRELIMINARY INQUIRY	DIOG 5, 6 and 7
MIOG I.I	Section 7	7-6 DEPARTMENTAL INSTRUCTIONS REGARDING QUESTIONABLE CASES	Paragraphs #1 and 2 only. DIOG 5, 6 and 7
MIOG I.I	Section 7	7-20 ADMINISTRATIVE SUBPOENAS IN CHILD ABUSE AND CHILD SEXUAL EXPLOITATION (CSE) CASES	DIOG 18.6.4
MIOG I.I	Section 9	9-7.2 Use of Closed Circuit Television (CCTV)	Paragraphs #2 (all sub-parts); 3 (all sub-parts); and 4 only. DIOG 18.6.3
MIOG I.I	Section 62	62-3 DOMESTIC POLICE COOPERATION - STATUTE	
MIOG I.I	Section 62	62-3.3 Policy	Paragraphs # 5 and 6 only. DIOG 12
MIOG I.I	Section 62	62-3.4 Office of Origin	DIOG 14
MIOG I.I	Section 62	62-3.5 Classification	DIOG 12. See new 343 classification
MIOG I.2	Section 157	Section : S157 Civil Unrest (8)	DIOG 12
MIOG I.2	Section 157	157-1 RESPONSIBILITY OF THE BUREAU	DIOG 12
MIOG I.2	Section 157	157-1.1 Categories for Reporting	DIOG 12
MIOG I.2	Section 157	157-2 POLICY REGARDING REPORTING OF CIVIL DISORDERS	DIOG 12
MIOG I.2	Section 157	157-3 REPORTING OF DEMONSTRATIONS	DIOG 12

UNCLASSIFIED – ~~FOR OFFICIAL USE ONLY~~
Domestic Investigations and Operations Guide

Part	Section	Section Title	DIOG Supersession
MIOG I.2	Section 157	157-4 PHOTOGRAPHIC SURVEILLANCES	DIOG 12
MIOG I.2	Section 157	157-5 DISSEMINATION OF DATA PERTAINING TO CIVIL DISORDERS AND DEMONSTRATIONS	DIOG 12
MIOG I.2	Section 157	157-6 REPORTING PROCEDURES TO BE UTILIZED IN CIVIL DISORDERS AND DEMONSTRATIONS	DIOG 12
MIOG I.2	Section 157	157-7 CHARACTER	DIOG 12
MIOG I.2	Section 161	161-10 DISSEMINATION TO THE WHITE HOUSE COMPLEX (WHC)	DIOG 14, 18
MIOG I.2	Section 163	163-1.1 Investigative Request	DIOG 12
MIOG I.2	Section 163	163-2 INVESTIGATIVE INSTRUCTIONS AND PROCEDURES	DIOG 12
MIOG I.2	Section 163	163-2.1 Opening Foreign Police Cooperation (FPC) - General Criminal Matters (GCM)	DIOG 12.2
MIOG I.2	Section 163	163-2.1.1 Letter Rogatory Process	DIOG 12
MIOG I.2	Section 163	163-3 REQUESTS FOR TERRORISM ENTERPRISE INVESTIGATIONS	DIOG 8, 12
MIOG I.2	Section 163	163-6 REPORTING	DIOG 12
MIOG I.2	Section 163	163-7 RULE 6(E) MATERIAL	DIOG 18
MIOG I.2	Section 163	163-8 PRIVACY ACT	DIOG 14
MIOG I.2	Section 163	163-9 RIGHT TO FINANCIAL PRIVACY ACT	DIOG Appendix O
MIOG I.2	Section 288	288-5.1 Accessing Computer Records - Summary of Compelled Disclosure under Title 18, USC, Section 2703	DIOG 18.6.8
MIOG I.2	Section 288	288-5.1.1 Subpoena - ECPA Requirements	DIOG 18.6.8
MIOG I.2	Section 288	288-5.1.2 Subpoena with Prior Notice to the Subscriber or Customer	DIOG 18.6.8
MIOG I.2	Section 288	288-5.1.3 Section 2703(d) Order	DIOG 18.6.8
MIOG I.2	Section 288	288-5.1.4 Section 2703(d) Order with Prior Notice to the Subscriber or Customer	DIOG 18.6.8

UNCLASSIFIED – ~~FOR OFFICIAL USE ONLY~~
Domestic Investigations and Operations Guide

Part	Section	Section Title	DIOG Supersession
MIOG I.2	Section 288	288-5.1.5 Search Warrant	DIOG 18.7.1
MIOG I.2	Section 288	288-5.1.6 Voluntary Disclosure	DIOG 18.6.8
MIOG I.2	Section 289	289-13.3 Use of a Past or Present Prisoner-Witness in an Investigation (Formerly Part 2, 27-16.5)	DIOG 11.5, 18.6.1, 18.6.2
MIOG I.2	Section 308	308-1.1 Evidence Response Team Mission	generally, DIOG 12 for expert assistance.
MIOG I.2	Section 308	308-2 DEFINITION OF ERT CONCEPT	Paragraph # 4 only. DIOG 12
MIOG I.2	Section 308	308-3 PROPER TURNING	Paragraph # 2 only. DIOG 12
MIOG I.2	Section 308	308-4 ERT SUBCLASSIFICATIONS-ALPHA DESIGNATORS	Paragraph # 1 only. DIOG 12. See new classifications
MIOG I.2	Section 319	319-1 INTELLIGENCE PROGRAM	generally, DIOG 5
MIOG I.2	Section 319	319-2 FIELD INTELLIGENCE GROUP (FIG) STRUCTURE AND FUNCTIONS	generally, DIOG 5
MIOG I.2	Section 319	319-4 INTELLIGENCE COLLECTION	Paragraphs # 1 and 3 generally, DIOG 5
MIOG I.2	Section 319	319-5 COLLECTION MANAGEMENT	generally, DIOG 5
MIOG II	Section 2	2-5 COMPLAINTS (RULE 3)	DIOG 19
MIOG II	Section 2	2-5.1 Authorization of U.S. Attorney (USA)	DIOG 19
MIOG II	Section 2	2-5.3 State Prosecutions	DIOG 3, 12
MIOG II	Section 2	2-5.4 Authority for Issuance of Warrant	DIOG 19
MIOG II	Section 2	2-5.5 Notification to Special Agent in Charge (SAC)	DIOG 19
MIOG II	Section 2	2-6 WARRANT OF ARREST OR SUMMONS (RULE 4)	DIOG 18 and 19
MIOG II	Section 2	2-6.1 Forms of Warrant	DIOG 19
MIOG II	Section 2	2-6.2 Issuance of Warrant or Summons	DIOG 19
MIOG II	Section 2	2-6.3 Execution	DIOG 19

UNCLASSIFIED – ~~FOR OFFICIAL USE ONLY~~
Domestic Investigations and Operations Guide

Part	Section	Section Title	DIOG Supersession
MIOG II	Section 2	2-7 PROCEEDINGS BEFORE THE MAGISTRATE (RULE 5)	DIOG 18, 19
MIOG II	Section 2	2-7.1 Initial Appearance	DIOG 19
MIOG II	Section 2	2-9 GRAND JURY (RULE 6)	DIOG 11.9, 11.9.1, 18.5.9, 18.6.5
MIOG II	Section 2	2-9.1 Purpose	DIOG 18.5.9, 18.6.5
MIOG II	Section 2	2-9.2 Persons Present	DIOG 18.5.9, 18.6.5
MIOG II	Section 2	2-9.3 Disclosure	DIOG 18.5.9, 18.6.5
MIOG II	Section 2	2-9.4 Exceptions	DIOG 11.9, 11.9.1, 18.5.9, 18.6.5
MIOG II	Section 2	2-9.5 Limitation of Use	DIOG 18.5.9, 18.6.5
MIOG II	Section 2	2-9.5.1 Matters Occurring Before the Grand Jury	DIOG 11.9, 11.9.1, 18.5.9, 18.6.5
MIOG II	Section 2	2-9.5.2 Physical Evidence and Statements	DIOG 18.5.9, 18.6.5
MIOG II	Section 2	2-9.6 Documentation of Disclosures of Grand Jury Material	DIOG 18.5.9, 18.6.5
MIOG II	Section 2	2-9.6.1 Documentation of Internal Disclosures of Grand Jury Material	DIOG 18.5.9, 18.6.5
MIOG II	Section 2	2-9.7 Storage of Grand Jury Material	DIOG 11.9, 11.9.1, 18.5.9, 18.6.5
MIOG II	Section 2	2-9.8 Requests for Subpoenas in Fugitive Investigations	DIOG 11.9, 11.9.1, 18.5.9, 18.6.5
MIOG II	Section 4	S4 Juveniles and Juvenile Delinquency Act	DIOG 19
MIOG II	Section 4	4-1 GENERAL STATEMENT	DIOG 19
MIOG II	Section 4	4-1.1 Purpose of Act	DIOG 19
MIOG II	Section 4	4-2 SPECIFIC PROVISIONS OF THE ACT	DIOG 19
MIOG II	Section 4	4-2.1 Definitions	DIOG 19
MIOG II	Section 4	4-2.2 Arrest Procedure	DIOG 19
MIOG II	Section 4	4-2.2.1 Advice of Rights	DIOG 19

UNCLASSIFIED – ~~FOR OFFICIAL USE ONLY~~
Domestic Investigations and Operations Guide

Part	Section	Section Title	DIOG Supersession
MIOG II	Section 4	4-2.2.2 Notification of USA and Juveniles Parents	DIOG 19
MIOG II	Section 4	4-2.2.3 Fingerprinting and Photographing	DIOG 19
MIOG II	Section 4	4-2.2.4 Press Releases	DIOG 19
MIOG II	Section 4	4-2.2.5 Interviews of Juveniles	DIOG 18
MIOG II	Section 4	4-2.2.6 Initial Appearance Before Magistrate	DIOG 19
MIOG II	Section 4	4-2.3 Detention	DIOG 19
MIOG II	Section 4	4-2.4 Prosecution	DIOG 19
MIOG II	Section 4	4-2.5 Use of Juvenile Records	DIOG 19
MIOG II	Section 6	6-2.1 Statements of All Witnesses, Such as FD-302s	DIOG 18.5.6.4.15
MIOG II	Section 6	6-5.1 Statements of All Witnesses, Such as FD-302s	DIOG 18.5.6.4.15
MIOG II	Section 7	S7 Interviews	DIOG 18.5.6
MIOG II	Section 7	7-1 USE OF CREDENTIALS FOR IDENTIFICATION	DIOG 18.5.6
MIOG II	Section 7	7-2 THOROUGHNESS, PRECAUTIONS, TELEPHONIC AND USE OF INTERPRETERS	DIOG 18.5.6
MIOG II	Section 7	7-2.1 Thoroughness and Precautions During Interviews	DIOG 18.5.6
MIOG II	Section 7	7-2.2 Telephone Interviews	DIOG 18.5.6
MIOG II	Section 7	7-2.3 Use of Interpreters	DIOG 18.5.6
MIOG II	Section 7	7-3 REQUIRING FBIHQ AUTHORITY	DIOG 18.5.6
MIOG II	Section 7	7-4 ONE VS TWO AGENT INTERVIEW OF SECURITY SUBJECT	DIOG 18.5.6
MIOG II	Section 7	7-5 EVALUATION OF AN INTERVIEW	DIOG 18.5.6
MIOG II	Section 7	7-6 INTERVIEWING COMPLAINANTS AND SUBJECTS OF CRIMINAL	DIOG 18.5.6
MIOG II	Section 7	7-6.1 Interviews of Complainants	DIOG 18.5.6

UNCLASSIFIED – ~~FOR OFFICIAL USE ONLY~~
Domestic Investigations and Operations Guide

Part	Section	Section Title	DIOG Supersession
MIOG II	Section 7	7-6.2 Subjects of Criminal Investigations	DIOG 18.5.6
MIOG II	Section 7	7-7 DEVELOPMENT OF DEROGATORY INFORMATION DURING INTERVIEWS	DIOG 18.5.6
MIOG II	Section 7	7-8 IDENTIFICATION OF SUSPECTS	DIOG 18.5.6
MIOG II	Section 7	7-9 INTERVIEWS INVOLVING OR RELATING TO COMPLAINTS	DIOG 18.5.6 and 5
MIOG II	Section 7	7-9.1 Complaints Received at the Field Office	DIOG 18.5.6 and 5
MIOG II	Section 7	7-9.2 Complaints in Person or by Telephone	DIOG 18.5.6 and 5
MIOG II	Section 7	7-9.3 Complaints By Letter	DIOG 18.5.6 and 5
MIOG II	Section 7	7-9.4 Complaints Critical of the FBI or Its Employees	DIOG 18.5.6 and 5
MIOG II	Section 7	7-9.5 Legal Requirements of the Privacy Act of 1974 (Title 5, USC, Section 552a)	DIOG 14
MIOG II	Section 9	S9 Surveillances	DIOG 18.5.8
MIOG II	Section 9	9-1 GENERAL GUIDELINES	DIOG 18.5.8
MIOG II	Section 9	9-1.1 Surveillance Restrictions	DIOG 18
MIOG II	Section 9	9-7.5 Surveillance Logs	DIOG 3
MIOG II	Section 10	S10 Records Available and Investigative Techniques	DIOG 18
MIOG II	Section 10	10-1 INTRODUCTION	DIOG 18
MIOG II	Section 10	10-2 RECORDS AVAILABLE	DIOG 18
MIOG II	Section 10	10-3 INVESTIGATIVE TECHNIQUES	in-part DIOG 18
MIOG II	Section 10	10-6 MAIL COVERS	DIOG 18.6.10
MIOG II	Section 10	10-6.1 United States Postal Service (USPS) Regulations	DIOG 18.6.10
MIOG II	Section 10	10-6.2 Policy	DIOG 11.3, 18.6.10
MIOG II	Section 10	10-6.3 Requesting Approval	DIOG 11.3, 18.6.10
MIOG II	Section 10	10-6.3.1 Fugitive or Criminal Cases	DIOG 18.6.10

UNCLASSIFIED – ~~FOR OFFICIAL USE ONLY~~
Domestic Investigations and Operations Guide

Part	Section	Section Title	DIOG Supersession
MIOG II	Section 10	10-6.3.2 National Security Cases	DIOG 18.6.10
MIOG II	Section 10	10-7 STOP NOTICES	DIOG
MIOG II	Section 10	10-7.1 Definition	DIOG
MIOG II	Section 10	10-7.2 Placement of Stops	DIOG
MIOG II	Section 10	10-7.3 Indexing Stops	DIOG
MIOG II	Section 10	10-7.4 Removal of Stops	DIOG
MIOG II	Section 10	10-7.5 Types of Stops	DIOG
MIOG II	Section 10	10-7.5.1 Savings Bonds	DIOG
MIOG II	Section 10	10-7.5.2 Immigration and Naturalization Service (INS)	DIOG
MIOG II	Section 10	10-7.5.3 Bureau of Prisons	DIOG
MIOG II	Section 10	10-8 STORED WIRE AND ELECTRONIC COMMUNICATIONS AND TRANSACTIONAL RECORDS ACCESS	DIOG 18.6.8
MIOG II	Section 10	10-8.1 Compelled Disclosure of the Contents of Stored Wire or Electronic Communications	DIOG 11.12, 18.6.8
MIOG II	Section 10	10-8.2 Access to Transactional Information	DIOG 18.6.8
MIOG II	Section 10	10-8.3 Access to and Use of Electronic Communications Located on the Internet, E-Mail, and Bulletin Board Systems	DIOG 18.6.8
MIOG II	Section 10	10-8.3.1 Definitions	DIOG 18.6.8
MIOG II	Section 10	10-8.3.2 Interception of Electronic Communications	DIOG 11.12, 18.6.8
MIOG II	Section 10	10-8.3.3 Undercover Use of the Internet	DIOG 18.6.8
MIOG II	Section 10	10-8.4 Monitoring the Internet	DIOG 18.6.8
MIOG II	Section 10	10-9 ELECTRONIC SURVEILLANCE (ELSUR) PROCEDURES AND REQUIREMENTS	DIOG 11.12, 18.7.2
MIOG II	Section 10	10-9.1 Definitions	DIOG 11.6.4 and 5, 18.7.2

UNCLASSIFIED – ~~FOR OFFICIAL USE ONLY~~
Domestic Investigations and Operations Guide

Part	Section	Section Title	DIOG Supersession
MIOG II	Section 10	10-9.2 Instructions for Maintaining ELSUR Indices	Appendix H
MIOG II	Section 10	10-9.3 Requests for ELSUR Checks	Appendix H
MIOG II	Section 10	10-9.4 ELSUR Searching Procedures	DIOG 11.6.6, 18.7.2, Appendix H
MIOG II	Section 10	10-9.5 Transmitting ELSUR Material to FBIHQ	
MIOG II	Section 10	10-9.6 Retention of ELSUR Files and Related Records	DIOG 3.3
MIOG II	Section 10	10-9.8 Marking File Cover "ELSUR":	DIOG 18.7.2
MIOG II	Section 10	10-9.8.2 Removable Recording Media	DIOG 18.7.2
MIOG II	Section 10	10-9.9 Recordkeeping Procedures for ELSUR Information Generated Through Joint FBI Operations	DIOG 18.7.2
MIOG II	Section 10	10-9.10 Electronic Surveillance - Title III Criminal Matters	DIOG 11.12, 18.7.2
MIOG II	Section 10	10-9.11 Emergency Provisions, Title III Criminal Matters	DIOG 18.7.2 and 05/22/2008 memo
MIOG II	Section 10	10-9.11.1 Form 2 Report	DIOG 18
MIOG II	Section 10	10-9.11.2 Completion of Form 2 Report	DIOG 18
MIOG II	Section 10	10-9.11.3 Submissions of Form 2 Report to FBIHQ	DIOG 18
MIOG II	Section 10	10-9.11.4 Supplemental Form 2 Reports	DIOG 18
MIOG II	Section 10	10-9.12 ELSUR Indexing in Title III Criminal Matters	DIOG 18
MIOG II	Section 10	10-9.13 Marking of Recordings for Identification	DIOG 18
MIOG II	Section 10	10-9.14 Loan of Electronic Surveillance Equipment to State and Local Law Enforcement Agencies	DIOG 12
MIOG II	Section 10	10-9.15 Submission of Recordings	DIOG 18

UNCLASSIFIED – ~~FOR OFFICIAL USE ONLY~~
Domestic Investigations and Operations Guide

Part	Section	Section Title	DIOG Supersession
MIOG II	Section 10	10-9.16 Transcription of Recordings	DIOG 18
MIOG II	Section 10	10-10 CONSENSUAL MONITORING - CRIMINAL MATTERS	DIOG 18.6.1, 18.6.2
MIOG II	Section 10	10-10.1 Use of Consensual Monitoring in Criminal Matters	DIOG 11.5, 18.6.1, 18.6.2
MIOG II	Section 10	10-10.2 Monitoring Telephone Conversations in Criminal Matters	DIOG 11.5, 18.6.1, 18.6.2
MIOG II	Section 10	10-10.2.1 Access to Recordings and Information Concerning Monitored Inmate Telephone Calls in Federal Prisons	DIOG 11.5, 18.6.1, 18.6.2
MIOG II	Section 10	10-10.3 Monitoring Nontelephone Communications in Criminal Matters	DIOG 11.5, 18.6.1, 18.6.2
MIOG II	Section 10	10-10.4 Monitoring Communications with Persons Outside the United States	DIOG 11.5, 18.6.1, 18.6.2
MIOG II	Section 10	10-10.5 ELSUR Indexing in Consensual Monitoring Matters	DIOG 11.5, 18.6.1, 18.6.2
MIOG II	Section 10	10-10.5.1 Administration of ELSUR Records Regarding Informants and Assets	DIOG 11.5, 18.6.1, 18.6.2
MIOG II	Section 10	10-10.6 Use of Consensual Monitoring in National Security Matters	DIOG 11.5, 18.6.1, 18.6.2
MIOG II	Section 10	10-10.7 Pen Registers (Dialed Number Recorder)	DIOG 11.11, 18.6.9
MIOG II	Section 10	10-10.7.1 Emergency Provisions	DIOG 18.6.9
MIOG II	Section 10	10-10.8 Electronic Tracking Devices	DIOG 11.6.3, 18.7.2
MIOG II	Section 10	10-9.8.1	DIOG 18.6.3.9
MIOG II	Section 10	10-10.9 Closed Circuit Television (CCTV) (Video Only) - Criminal Matters	DIOG 18.6.3
MIOG II	Section 10	10-10.9.1 CCTV Authorization - Criminal Matters	DIOG 18.6.3.4-5
MIOG II	Section 10	10-10.9.2 CCTV - ELSUR Records - Criminal Matters	DIOG 18.6.3
MIOG II	Section 10	10-10.9.3 CCTV (Audio and Video) - ELSUR Indexing - Criminal Matters	DIOG 18.6.3

UNCLASSIFIED – ~~FOR OFFICIAL USE ONLY~~
Domestic Investigations and Operations Guide

Part	Section	Section Title	DIOG Supersession
MIOG II	Section 10	10-10.9.4 CCTV - Preservation of the Original Tape Recording	DIOG 18.6.3.7
MIOG II	Section 10	10-10.10 Media Recorders (Formerly Tape Recorders)	DIOG 18.6.1
MIOG II	Section 10	10-10.11 Radio Monitoring	DIOG 18.6.1
MIOG II	Section 10	10-10.11.1 Paging Devices	DIOG 18.6.1
MIOG II	Section 10	10-10.11.2 Cordless Telephones and Other Types of Radio Monitoring	DIOG 18.6.1
MIOG II	Section 10	10-10.11.3 Cellular Telephones	DIOG 18.6.1
MIOG II	Section 10	10-10.17 Trap-Trace Procedures	DIOG 11.11, 18.6.1
MIOG II	Section 10	10-11 FBI UNDERCOVER ACTIVITIES - CRIMINAL MATTERS	DIOG 18.6.13
MIOG II	Section 10	10-18 FBI PRINCIPLES AND POLICIES FOR ONLINE CRIMINAL INVESTIGATIONS	DIOG Appendix L
MIOG II	Section 10	10-18.1 Online Communications	DIOG Appendix L
MIOG II	Section 10	10-18.2 Monitoring Online Communications	DIOG Appendix L
MIOG II	Section 10	10-18.3 Access to Stored Electronic Information	DIOG Appendix L
MIOG II	Section 10	10-18.4 Record Retention and Dissemination	DIOG 14, Appendix L
MIOG II	Section 10	10-18.5 Undercover Online Communications	DIOG Appendix L
MIOG II	Section 10	10-18.6 International Issues	DIOG Appendix L
MIOG II	Section 10	10-19 HANDLING AND PRESERVATION OF AIRCRAFT-MOUNTED VIDEO AND [REDACTED] EVIDENCE	DIOG 11.6.6, DIOG 18.6.3.6
MIOG II	Section 10	10-20 MAJOR CASES	DIOG Appendix K - Major cases
MIOG II	Section 11	S11 Techniques and Mechanics of Arrest	DIOG 19
MIOG II	Section 11	11-1 ARREST TECHNIQUES	DIOG 19

b7E

UNCLASSIFIED – ~~FOR OFFICIAL USE ONLY~~
Domestic Investigations and Operations Guide

Part	Section	Section Title	DIOG Supersession
MIOG II	Section 11	11-1.1 General	DIOG 19
MIOG II	Section 11	11-1.2 Initial Approach	DIOG 19
MIOG II	Section 11	11-1.3 Search of the Person	DIOG 19
MIOG II	Section 11	11-1.3.1 High-Risk Search-Full-Body Search-Handcuffing	DIOG 19
MIOG II	Section 11	11-1.3.2 Final Search and Collection of Evidence	DIOG 19
MIOG II	Section 11	11-1.4 Transportation of Arrested Persons	DIOG 19
MIOG II	Section 11	11-1.5 Handcuffing	DIOG 19
MIOG II	Section 11	11-2 PROCEDURES FOR ARREST	DIOG 19
MIOG II	Section 11	11-2.1 Arrests and Searches	DIOG 19
MIOG II	Section 11	11-2.1.1 Types of Arrest Warrants	DIOG 19
MIOG II	Section 11	11-2.1.2 Authority to Serve Arrest Warrants	DIOG 19
MIOG II	Section 11	11-2.1.3 Summons and Subpoenas	DIOG 18
MIOG II	Section 11	11-2.1.4 Arrests Without Warrants	DIOG 19
MIOG II	Section 11	11-2.1.5 Forcible Entry	DIOG 19
MIOG II	Section 11	11-2.1.6 Search of the Person	DIOG 19
MIOG II	Section 11	11-2.2.2 Property of Prisoner	DIOG 19
MIOG II	Section 11	11-2.2.3 Removal of Prisoner from the Custody of the U.S. Marshal	DIOG 19
MIOG II	Section 11	11-2.3.2 Medical Attention for Bureau Subjects	DIOG 19
MIOG II	Section 11	11-2.3.3 Arrest of Foreign Nationals	DIOG 19
MIOG II	Section 11	11-4.7.1 Juveniles	DIOG 19
MIOG II	Section 12	12.1.3.1	DIOG 19
MIOG II	Section 12	12-2.1 Deadly Force - Standards for Decisions	DIOG has pdf of policy in Appendix F
MIOG II	Section 13	Section 13	DIOG 18.5.6.4.15.1

UNCLASSIFIED – ~~FOR OFFICIAL USE ONLY~~
Domestic Investigations and Operations Guide

Part	Section	Section Title	DIOG Supersession
MIOG II	Section 14	14-16.9 Fingerprinting of Juveniles by Federal Agencies under the Violent Crime Control and Law Enforcement Act of 1994 (Hereinafter, the Act)	DIOG 19
MIOG II	Section 16	16-4.1.2 Dialed Number Recorders (Pen Registers)	Paragraph #1, last two sentences only. DIOG 18.6.9
MIOG II	Section 16	16-4.1.3 Consensual Monitoring (Formerly 16-7.4.1)	Paragraphs # 3 and 4 only. DIOG 18.6.1
MIOG II	Section 16	16-4.1.4 Electronic Surveillance - Title III	DIOG 18.7.2
MIOG II	Section 16	16-4.1.5 Electronic Surveillance FISA	DIOG 18.7.3
MIOG II	Section 16	16-4.1.6 Telephone Toll Records	DIOG 18
MIOG II	Section 16	16-4.2.2 Court-Ordered Electronic Surveillance (RCU)	DIOG 18.6.9; 18.7.2; and 18.7.3
MIOG II	Section 16	16-4.2.3 Computing Time for Title III Electronic Surveillance (RCU)	DIOG 18.7.2
MIOG II	Section 16	16-4.2.4 Emergency Electronic Surveillance (RCU)	DIOG 18.6.9; 18.7.2; and 18.7.3
MIOG II	Section 16	16-4.2.5 Roving Electronic Surveillance (RCU)	DIOG 18.7.2 and 18.7.3
MIOG II	Section 16	16-4.3 Consensual Monitoring - Technical Assistance (RCU)	Paragraph # 1, first two sentences only. DIOG 18.6.1 and 18.6.2
MIOG II	Section 16	16-4.4 Electronic Surveillance (ELSUR) Interceptions (RCU)	Paragraph # 1, first sentence only. DIOG 18.7.2 and 18.7.3
MIOG II	Section 16	16-4.4.2 Telecommunications Interceptions - Reporting Requirements (TICTU)	DIOG 18.7.2 and 18.7.3
MIOG II	Section 16	16-4.4.3 Telecommunications - Use of Pen Registers and Traps-Traces (TICTU)	Paragraph # 1 only. DIOG 18.6.9
MIOG II	Section 16	16-4.4.4 Pen Registers and Traps-Traces Reporting Requirements (TICTU)	DIOG 18.6.9
MIOG II	Section 16	16-4.8.1 Authorized Use of Technical Devices in Conducting Physical Surveillances (TTU)	Paragraph # 1, second, third and fourth sentences only. DIOG 18

UNCLASSIFIED – ~~FOR OFFICIAL USE ONLY~~
Domestic Investigations and Operations Guide

Part	Section	Section Title	DIOG Supersession
MIOG II	Section 16	16-4.8.4 Technical Devices in Physical Surveillance - Technical, Practical, and Legal Considerations (TTU)	Paragraph # 1 only. DIOG 18
MIOG II	Section 16	16-4.8.9 Authorized Use of Electronic Tracking and Locating Devices and Techniques (TTU)	DIOG 18
MIOG II	Section 16	16-4.8.12 Tracking - Technical, Practical, and Legal Considerations (TTU)	Paragraph # 1; Paragraph # 2, third sentence; Paragraph # 4, second sentence only. DIOG 18
MIOG II	Section 16	16-4.9 Closed Circuit Television (CCTV) (VSU)	DIOG 18.6.3
MIOG II	Section 16	16-4.13.1 Availability and Control of Technical Equipment	Paragraphs # 2 and 3 only. DIOG 18
MIOG II	Section 16	16-4.13.4 Loan of Electronic Surveillance Equipment	DIOG 12
MIOG II	Section 21	21-12 APPREHENSION OF BUREAU FUGITIVES	Paragraph # 1 only. DIOG 19
MIOG II	Section 21	21-13.4 Policy	Paragraphs # 2 and 3 only. DIOG 19
MIOG II	Section 21	21-20 FUGITIVE INVESTIGATIONS FOR OTHER FEDERAL AGENCIES	Paragraph # 3, new classification 343 replaces 62. DIOG 12.5
MIOG II	Section 21	21-20.1 Fugitive Inquiries Abroad on Behalf of U.S. Marshals Service (USMS)	Paragraph # 4, new classification 343 replaces 62. DIOG 12.5
MIOG II	Section 23	23-2 THE FAIR CREDIT REPORTING ACT	DIOG Appendix M - FCRA
MIOG II	Section 23	23-2.1 Section 1681a. Definitions	DIOG Appendix M - FCRA
MIOG II	Section 23	23-2.2 Section 1681b. Permissible Purposes of Consumer Reports	DIOG Appendix M - FCRA
MIOG II	Section 23	23-2.3 Section 1681f. Disclosures to Government Agencies	DIOG Appendix M - FCRA
MIOG II	Section 23	23-2.4 Section 1681g. Disclosure to Consumers	DIOG Appendix M - FCRA

UNCLASSIFIED – ~~FOR OFFICIAL USE ONLY~~
Domestic Investigations and Operations Guide

Part	Section	Section Title	DIOG Supersession
MIOG II	Section 23	23-2.5 Section 1681e. Compliance Procedures	DIOG Appendix M - FCRA
MIOG II	Section 23	23-2.6 Summary	DIOG Appendix M - FCRA
MIOG II	Section 23	23-2.7 Penalties	DIOG Appendix M - FCRA
MIOG II	Section 23	23-2.8 Section 1681n, o, q, and r. Civil and Criminal Liability for Willful or Negligent Noncompliance	DIOG Appendix M - FCRA
MIOG II	Section 23	23-3.1 Information Desired from Outside the Field Office Territory	DIOG 18.1.4, Appendix J
MIOG II	Section 23	23-4.4 Interviews in Foreign Countries	DIOG 18
MIOG II	Section 23	23-4.10 Extraterritorial Investigative Activity	DIOG 11.5, 18.6.1, 18.6.2
MIOG II	Section 23	23-6 TITLE XI, RIGHT TO FINANCIAL PRIVACY ACT OF 1978 (RFPA)	DIOG Appendix O - RFPA
MIOG II	Section 23	23-6.1 Statute	DIOG Appendix O - RFPA
MIOG II	Section 23	23-6.2 Access to Financial Records	DIOG Appendix O - RFPA
MIOG II	Section 23	23-6.2.1 Intent	DIOG Appendix O - RFPA
MIOG II	Section 23	23-6.2.2 Methods Available to FBI	DIOG Appendix O - RFPA
MIOG II	Section 23	23-6.2.3 Methods Not Available to FBI	DIOG Appendix O - RFPA
MIOG II	Section 23	23-6.3 Definitions	DIOG Appendix O - RFPA
MIOG II	Section 23	23-6.3.1 Financial Institution	DIOG Appendix O - RFPA
MIOG II	Section 23	23-6.3.2 Financial Record	DIOG Appendix O - RFPA
MIOG II	Section 23	23-6.3.3 Government Authority	DIOG Appendix O - RFPA

UNCLASSIFIED – ~~FOR OFFICIAL USE ONLY~~
Domestic Investigations and Operations Guide

Part	Section	Section Title	DIOG Supersession
MIOG II	Section 23	23-6.3.4 Customers Covered	DIOG Appendix O - RFPA
MIOG II	Section 23	23-6.3.5 Law Enforcement Inquiry	DIOG Appendix O - RFPA
MIOG II	Section 23	23-6.4 Responsibility of Financial Institutions	DIOG Appendix O - RFPA
MIOG II	Section 23	23-6.5 Certification of Compliance	DIOG Appendix O - RFPA
MIOG II	Section 23	23-6.6 Methods of Access	DIOG Appendix O - RFPA
MIOG II	Section 23	23-6.6.1 Customer Authorization	DIOG Appendix O - RFPA
MIOG II	Section 23	23-6.6.2 Search Warrants	DIOG Appendix O - RFPA
MIOG II	Section 23	23-6.6.3 Formal Written Request	DIOG Appendix O - RFPA
MIOG II	Section 23	23-6.6.4 Judicial Subpoena	DIOG Appendix O - RFPA
MIOG II	Section 23	23-6.6.5 Grand Jury Subpoena	DIOG Appendix O - RFPA
MIOG II	Section 23	23-6.7 Customer Notice	DIOG Appendix O - RFPA
MIOG II	Section 23	23-6.7.1 Contents of Notice	DIOG Appendix O - RFPA
MIOG II	Section 23	23-6.7.2 Delay of Notice	DIOG Appendix O - RFPA
MIOG II	Section 23	23-6.8 Customer Challenges	DIOG Appendix O - RFPA
MIOG II	Section 23	23-6.9 Emergency Access	DIOG Appendix O - RFPA
MIOG II	Section 23	23-6.10 Exceptions to RFPA	DIOG Appendix O - RFPA
MIOG II	Section 23	23-6.10.1 Financial Institutions	DIOG Appendix O - RFPA

UNCLASSIFIED – ~~FOR OFFICIAL USE ONLY~~
Domestic Investigations and Operations Guide

Part	Section	Section Title	DIOG Supersession
MIOG II	Section 23	23-6.10.2 Corporations or Other Legal Entities	DIOG Appendix O - RFPFA
MIOG II	Section 23	23-6.10.3 Not Identifiable with Customer	DIOG Appendix O - RFPFA
MIOG II	Section 23	23-6.10.4 Parties in Interest	DIOG Appendix O - RFPFA
MIOG II	Section 23	23-6.10.5 Federal Grand Jury	DIOG Appendix O - RFPFA
MIOG II	Section 23	23-6.10.6 Foreign Counterintelligence	DIOG Appendix O - RFPFA
MIOG II	Section 23	23-6.10.7 Telephone Company Toll Records	DIOG Appendix O - RFPFA
MIOG II	Section 23	23-6.10.8 Other	DIOG Appendix O - RFPFA
MIOG II	Section 23	23-6.11 Dissemination of Information	DIOG Appendix O - RFPFA
MIOG II	Section 23	23-6.11.1 To Department of Justice	DIOG Appendix O - RFPFA
MIOG II	Section 23	23-6.11.2 To Other Departments	DIOG Appendix O - RFPFA
MIOG II	Section 23	23-6.12 Penalties	DIOG Appendix O - RFPFA
MIOG II	Section 23	23-6.12.1 Civil	DIOG Appendix O - RFPFA
MIOG II	Section 23	23-6.12.2 Disciplinary Action	DIOG Appendix O - RFPFA
MIOG II	Section 23	23-6.12.3 Other	DIOG Appendix O - RFPFA
MIOG II	Section 23	23-6.13 Cost Reimbursement	DIOG Appendix O - RFPFA
MIOG II	Section 23	23-6.14 Reporting Requirements	DIOG Appendix O - RFPFA
MIOG II	Section 23	23-6.14.1 Dissemination of Information Obtained	DIOG Appendix O - RFPFA

UNCLASSIFIED – ~~FOR OFFICIAL USE ONLY~~
Domestic Investigations and Operations Guide

Part	Section	Section Title	DIOG Supersession
MIOG II	Section 23	23-6.14.2 Statistical Reporting	DIOG Appendix O - RFPFA
MIOG II	Section 28	28-1 ATTORNEY GENERAL'S GUIDELINES ON METHODS OF OBTAINING DOCUMENTARY MATERIALS HELD BY THIRD PARTIES	DIOG Appendix C
NFIPM	Section 1	01-2: (U) The National Security List	DIOG Appendix G
NFIPM	Section 1	01-3: (U) Acronyms	DIOG Appendix P
NFIPM	Section 1	01-4: (U) File Classifications and Alpha Designations for Investigative and Administrative Activities Which Uniquely Fall Within the Purview of the FBI's National Foreign Intelligence Program	CPD #0015D. See RPO web-page.
NFIPM	Section 2	02-1: (U) General Investigative and Administrative Activities	Appendix M for definitions: #2, 6, 7, 10, 12, 14, 15, 18, 19, 20, 25, 26 and 27.
NFIPM	Section 2	02-2: (U) National Security Investigations	DIOG 5, 6, 7, 8, 9
NFIPM	Section 2	02-3: (U) Summary Guidance and Applicability of Threat Assessments	DIOG 5
NFIPM	Section 2	02-4: (U) Summary Guidance and Applications for Preliminary Investigations	DIOG 6, 18
NFIPM	Section 2	02-5: (U) Summary Guidance and Application for Full Investigations (FI)	DIOG 7, 8, 9, 18
NFIPM	Section 2	02-6: (U) Collection of Foreign Intelligence	DIOG 9
NFIPM	Section 2	02-8: (U) Office of Origin	DIOG 14
NFIPM	Section 2	02-9: (U) Physical and Photographic Surveillances	DIOG 18.5.8
NFIPM	Section 2	02-10: (U) Interviews in National Security Investigations	DIOG 18.5.6
NFIPM	Section 2	02-11: (U) Education Records (Buckley Amendment)	DIOG Appendix I
NFIPM	Section 2	02-12: (U) Polygraph Examinations	DIOG 18.6.11
NFIPM	Section 2	02-14: (U) 	DIOG 19.2 and Appendix G

b7E

UNCLASSIFIED – ~~FOR OFFICIAL USE ONLY~~
Domestic Investigations and Operations Guide

Part	Section	Section Title	DIOG Supersession
NFIPM	Section 2	02-15: (U) Physical Searches in Which a Warrant is Not Required	DIOG 11.4, 18.6.12
NFIPM	Section 2	02-16: (U) Monitoring Devices Which Do Not Impose Upon Reasonable Expectations of Privacy	DIOG 18.6.3
NFIPM	Section 2	02-17: (U) National Security Letters (NSL)	DIOG 11.9-11.9.3, 18.6.6
NFIPM	Section 2	02-19: (U) Business Records	DIOG 18.6.7
NFIPM	Section 2	02-21: (U) Mail Covers	DIOG 11.3, 18.6.10
NFIPM	Section 2	02-22: (U) Operations Conducted Outside the United States [REDACTED]	See CPO MOU Library
NFIPM	Section 2	02-23: (U) The Role of Legal Attaches in Foreign Counterintelligence, Foreign Intelligence and Counterterrorism Investigations	See CD PG
NFIPM	Section 2	02-24: (U) Otherwise Illegal Activities	DIOG 17
NFIPM	Section 2	02-25: (U) Arrests, Interdictions, Demarches and Declarations	DIOG 19 - Arrest Procedure
NFIPM	Section 2	02-29: (U) Laboratory Assistance	See Lab web-page
NFIPM	Section 2	02-32: (U) [REDACTED]	DIOG 19.3, 19.4 and appendix G -12.C
NFIPM	Section 2	02-33: (U) [REDACTED] [REDACTED]	DIOG Appendix G - 12.C
NFIPM	Section 2	02-34: (U) Special Surveillance Group (SSG) Program	DIOG 18.5.8
NFIPM	Section 2	02-35: (U) The Behavioral Analysis Program (BAP)	DIOG 19.4
NFIPM	Section 2	02-36: (U) Investigations of Current and Former Department of State Personnel, and Diplomatic Missions Personnel Abroad	DIOG 10, generally
NFIPM	Section 2	02-37: (U) Investigations of Current and Former Central Intelligence Agency Personnel	DIOG 10, generally

b7E

UNCLASSIFIED – ~~FOR OFFICIAL USE ONLY~~
Domestic Investigations and Operations Guide

Part	Section	Section Title	DIOG Supersession
NFIPM	Section 2	02-38: (U) Investigations of Current and Former Military and Civilian Department of Defense Personnel	DIOG 10, generally
NFIPM	Section 2	02-39: (U) Investigations of Current and Former Department of Energy Personnel	DIOG 10, generally
NFIPM	Section 2	02-40: (U) Investigations of Other Government Agency Personnel	DIOG 10
NFIPM	Section 2	02-41: (U) Investigations of White House Personnel	DIOG 10
NFIPM	Section 2	02-42: (U) Investigations of Presidential Appointees	DIOG 10
NFIPM	Section 2	02-43: (U) Investigations of Members of the Judiciary	DIOG 10
NFIPM	Section 2	02-44: (U) Investigations of Members of the U.S. Congress and their Staffs	DIOG 10
NFIPM	Section 2	02-45: (U) Disseminating Information to Other Agencies in the Federal Government	DIOG 12.4/DIOG 14
NFIPM	Section 2	02-47: (U) Disseminating Information to Congressional Committees	DIOG 12.4 and 14.3(A)(4)
NFIPM	Section 2	02-48: (U) Disseminating Information to the Federal Judiciary	DIOG 12.4
NFIPM	Section 2	02-49: (U) Disseminating Information to the White House	DIOG 12.4 and 14.5
NFIPM	Section 2	02-50: (U) Disseminating Information to Foreign Governments and Investigations at their Behest	DIOG 12.4/DIOG 14.5
NFIPM	Section 2	02-51: (U) Disseminating Information to State and Local Government Agencies	DIOG 12 and 14
NFIPM	Section 2	02-52: (U) Disseminating Information to the Private Sector	DIOG 14.3 (A)(6-8)
NFIPM	Section 2	02-54: (U) [REDACTED] [REDACTED]	See IIIA web-page
NFIPM	Section 2	02-56: (U) Intelligence Oversight Board Matters	DIOG 4/DIOG 18.6.6 (Re: NSLs) and CPD 0188PG

b7E

UNCLASSIFIED – ~~FOR OFFICIAL USE ONLY~~
Domestic Investigations and Operations Guide

Part	Section	Section Title	DIOG Supersession
NFIPM	Section 2	02-57: (U) Alpha Designations	CPD #0015D. See RPO web-page.
NFIPM	Section 3	03-1: (U) Consensual Monitoring	DIOG 11.5, 18.6.1
NFIPM	Section 3	03-2: (U) Volunteered Tape Recordings	DIOG 6.9(B)(7), 18.5.7
NFIPM	Section 3	03-4: (U) Pen Registers and Trap and Trace Devices	DIOG 11.11-11.12, 18.6.9
NFIPM	Section 3	03-5: (U) Unconsented Electronic Surveillance	DIOG 11.12, 18.7.3
NFIPM	Section 3	03-6: (U) Electronic Surveillance Minimization, Logs and Indexing	0137PG
NFIPM	Section 3	03-8: (U) Operational Support to the Intelligence Community	DIOG 12, 12.5, 14.5
NFIPM	Section 3	03-9: (U) Operational Technology Division (OTD) Technical Assistance	CPD #0170D
NFIPM	Section 3	Section 3-10 (U) Operational Technology Division (OTD) Technical Assistance Support to the Intelligence Community	DIOG 12 (generally)
NFIPM	Section 3	03-11: (U) Unconsented Physical Searches	DIOG 11.13. 18.7.1
NFIPM	Section 3	03-12: (U) Tax Return Information	Appendix N - Tax Return Info
NFIPM	Section 3	03-13: (U) Searches of Mail Without Consent	DIOG 18.7.1
NFIPM	Section 3	03-14: (U) Unconsented Physical Search Minimization, Logs and Indexing	DIOG 18.7.1 and SMP PG
NFIPM	Section 4	04-1: (U) The Domain Program	DIOG 5, type 4 assessments generally.
NFIPM	Section 5	05-2: (U) Countries on the Current National Security List	Appendix G
NFIPM	Section 5	05-23: (U) Alpha Designations	CPD #0015D. See RPO web-page.
NFIPM	Section 6	06-12: (U) Alpha Designations	CPD #0015D. See RPO web-page.
NFIPM	Section 8	08-11: (U) Alpha Designations	CPD #0015D. See RPO web-page.

UNCLASSIFIED – ~~FOR OFFICIAL USE ONLY~~
Domestic Investigations and Operations Guide

Part	Section	Section Title	DIOG Supersession
NFIPM	Section 9	09-8: (U) Alpha Designations	CPD #0015D. See RPO web-page.
NFIPM	Section 11	11-4: (U) Alpha Designations	CPD #0015D. See RPO web-page.
NFIPM	Section 12	12-4: (U) Alpha Designations	CPD #0015D. See RPO web-page.
NFIPM	Section 13	13-4: (U) Alpha Designations	CPD #0015D. See RPO web-page.
NFIPM	Section 14	14-4: (U) Alpha Designations	CPD #0015D. See RPO web-page.
NFIPM	Section 15	15-4: (U) Alpha Designations	CPD #0015D. See RPO web-page.
NFIPM	Section 16	16-13: (U) Alpha Designations	CPD #0015D. See RPO web-page.
NFIPM	Section 18	18-3: (U) Issue Threat Preliminary Investigations	DIOG 6
NFIPM	Section 18	18-4: (U) Issue Threat Full Investigations	DIOG 7
NFIPM	Section 18	18-6: (U) Issue Threat File Numbers	CPD #0015D. See RPO web-page.
NFIPM	Section 19	19-3: (U) Procedural Requirements in International Terrorism Investigations	DIOG 5, 6, 7, 8
NFIPM	Section 19	19-4: (U) Closing International Terrorism Investigations	DIOG 5, 6, 7, 8
NFIPM	Section 19	19-11: (U) The Behavioral Analysis Program	DIOG 19.4
NFIPM	Section 19	19-13: (U) Alpha Designations	CPD #0015D. See RPO web-page.
NFIPM	Section 20	20-9 (U) The Behavioral Analysis Program	DIOG 19.4
NFIPM	Section 20	20-10 (U) Alpha Designations	CPD #0015D. See RPO web-page.
NFIPM	Section 21	21-6: (U) Alpha Designations	CPD #0015D. See RPO web-page.
NFIPM	Section 22	22-2: (U) Alpha Designations	CPD #0015D. See RPO web-page.

UNCLASSIFIED – ~~FOR OFFICIAL USE ONLY~~
Domestic Investigations and Operations Guide

Part	Section	Section Title	DIOG Supersession
NFIPM	Section 27	Confidential Human Sources Manual	CHSPM
NFIPM	Section 27	Confidential Human Source Validation Standards Manual	CSHVSM
NFIPM	Section 28	Section : 28 (U) Undercover Operations (4)	DIOG and NSUCOPG
NFIPM	Section 28	28-1: (U) UC Operations	DIOG 11.12, 18.6.3, and NSUCOPG
NFIPM	Section 28	28-2: (U) Group I	DIOG 11.12, 18.6.3, and NSUCOPG
NFIPM	Section 28	28-3: (U) Group II	DIOG 11.12, 18.6.3, and NSUCOPG
NFIPM	Section 28	28-4: (U) UC Administrative Matters	DIOG 11.12, 18.6.3, and NSUCOPG
NFIPM	Section 30	30-11: (U) The Behavioral Analysis Program	DIOG 19.4
MAOP I	0-1	Authority of the Director	DIOG 3.2.1
MAOP I	21-7 (6)	Monitoring, documenting and reviewing	DIOG 3.4.D
MAOP II	1-1	SAC and ASAC Supervisory Responsibility	Paragraphs # 2 and # 5. DIOG 3.4.C and Succession and delegation policy
MAOP II	1-1.4 (# 1)	Supervision of Cases	Paragraph # 1 - DIOG 14
MAOP II	1-1.4 (# 2 and # 3 a-f)	Supervisory File Reviews	Paragraph # 2 and # 3 (a-f) - # 2 Supervisory File reviews and # 3 PSAs. DIOG 3.4.D
MAOP II	1-1.5.1	Official Channels	Paragraph (5) b only - superseded by CPD 0152D - FBI Policy Cycle Directive.
MAOP II	1-3.5	Designation of Senior Resident Agent and Alternate	Second and third sentences only - DIOG 3.4.C and succession and delegation policy ____?

UNCLASSIFIED – ~~FOR OFFICIAL USE ONLY~~
Domestic Investigations and Operations Guide

Part	Section	Section Title	DIOG Supersession
MAOP II	1-3.6	Reporting to HQ City	First and second sentence - file reviews every 90 days: DIOG 3.4.D
MAOP II	1-3.13..2 (1)	Supervision of Investigations	Paragraph (1) - DIOG 3.4.C and succession and delegation policy ____?
MAOP II	1-3.13.3 (all)	Case Reviews	All (paragraphs 1-6) - DIOG 3.4.D
MAOP II	2-3	Indexing	DIOG 14
MAOP II	2-3.1	Purpose	DIOG Appendix J
MAOP II	2-4	Management of Files	DIOG 14
MAOP II	2-4.1	Investigative Files	DIOG 14
MAOP II	2-4.1.1	Serializing	DIOG 14
MAOP II	2-4.1.2	Zero Files	Paragraph (2) only. DIOG 14
MAOP II	2-4.1.3	Double Zero Files	DIOG 14
MAOP II	2-4.1.4	Dead Files - No Pending Investigation	DIOG 14
MAOP II	2-4.1.5	Control Files	Paragraph (1) first four sentences only. DIOG 14
MAOP II	2-4.2	Administrative Files	DIOG 14
MAOP II	2-4.2.1	Noninvestigative Files	DIOG 14
MAOP II	2-4.3.6	Consolidation of Files	DIOG 14
MAOP II	2-4.3.7	Reclassification of Files	DIOG 14
MAOP II	2-5	Case Management - Field Offices	DIOG 14
MAOP II	2-5.1	Opening Cases	Paragraphs 1, 2, 3, 4 (initial paragraph only before sub-letters), 4d, 4e, 4f, and 5 (first sentence only). DIOG various sections

~~UNCLASSIFIED – FOR OFFICIAL USE ONLY~~
Domestic Investigations and Operations Guide

Part	Section	Section Title	DIOG Supersession
MAOP II	2-5.1.1	Leads	Paragraph (2), delete "Discretionary Action" leads in first sentence only; and delete 2b. DIOG 14
MAOP II	2-5.2	Status of Cases	DIOG 14
MAOP II	2-5.2.1	Pending Case	DIOG 14
MAOP II	2-5.2.2	Pending Inactive	Paragraphs 2, 2a-c, and 3 only. DIOG 14
MAOP II	2-5.2.3	Referred Upon Completion to the Office of Origin (RUC)	DIOG 14
MAOP II	2-5.2.4	Closed	DIOG 6.11, 7.11, 8.8, 9.12
MAOP II	2-5.2.5	Unaddressed Work	DIOG 14
MAOP II	3-1	FBI Classifications/Sub-classifications and Program Groupings	CPD 0015D. RPO/RAU is now responsible for this area by EC 66F-HQ-1079817 serial 705. Link to RPO web-site. Supersede section 3.1 and all subparts.
MAOP II	3-1.1	FBI Classifications and Subdivided Classifications	only 62D; 62E replaced with new 343 classification. 163 M-U classification added. DIOG 12
MAOP II	3-3 (3c)	Task Force Officers (defined)	DIOG 3.3.2
MAOP II	3-3.2 (1)	Special TURK Recording Procedures (1) Major Cases	#1a-g. DIOG Appendix J-Major Cases
MAOP II	3-4.5 (9 a-g)	Case Count Information (# 9 re: closings)	Paragraph # 9 a-g was supersede by DIOG 6.11; 7.11; 8.8; and 9.12.
MAOP II	3-4.6	Reclassifying Cases and Error Correction	DIOG 6.11.C; 7.11.C; 8.8.C; and 9.12.C

UNCLASSIFIED – ~~FOR OFFICIAL USE ONLY~~
Domestic Investigations and Operations Guide

Part	Section	Section Title	DIOG Supersession
MAOP II	3-4.8	Criminal Preliminary Inquires	Paragraph #1 only. DIOG Section 6.7 - PIS are authorized for 6 months; extension authorized for 6 additional months by SAC; and FBIHQ SC.
MAOP II	3-4.10 (1)	Spin-off Cases (paragraph #1 - defined)	DIOG 14
MAOP II	3-4.10 (2)	Spin-off Cases (paragraph #2 - who can authorize)	DIOG 5, 6, 7, 8, and 9.
MAOP II	3-4.11(1)	Control Files (Paragraph #1 - defined)	superseded paragraph #1, defined in DIOG 14
MAOP II	3-4.11 (2)	Control Files (Paragraph #2 - leads)	superseded paragraph # 2, DIOG 14
MAOP II	3-4.11 (3)	Control Files (paragraph #3, third sentence only)	delete third sentence only, DIOG 14
MAOP II	9	Dissemination of Information	DIOG 14.3 (generally)
MAOP II	9-3	Information to Be Disseminated	DIOG 14.3, 14.4, 14.5 and 14.6
MAOP II	9-3 (paragraph 1)		DIOG 14.3.A and B
MAOP II	9-3 (paragraph 2)	AG Memo 9/21/2001 - "Disseminating Information to Enhance Public Safety and National Security."	DIOG 14
MAOP II	9-3 (paragraph 3)		DIOG 14.3.A.5
MAOP II	9-3.1	Dissemination to State and Local Criminal Justice and Noncriminal Justice Agencies	DIOG 14.3.A.3
MAOP II	9-3.1.1	Dissemination to State and Local Criminal Justice Agencies	DIOG 14.3
MAOP II	9-3.2	Information Totally Within Jurisdiction of Other Federal Agencies	DIOG 14.4.B
MAOP II	9-3.3	Information within FBI Jurisdiction and of interest to another Federal Agency	DIOG 3.4.E
MAOP II	9-3.4.2	Interested Agency Outside a Field Office Territory	DIOG 12.4

~~UNCLASSIFIED – FOR OFFICIAL USE ONLY~~
Domestic Investigations and Operations Guide

Part	Section	Section Title	DIOG Supersession
MAOP II	9-3.4.3	Interested Agency Within a Field Office's Territory	DIOG 12.4
MAOP II	9-3.4.4	Reporting Information Furnished	DIOG 12.4 and 12.5
MAOP II	9-3.5	Method of Dissemination to Outside Agencies	DIOG 12.4 and 12.5
MAOP II	9-3.5.3	Oral Dissemination to Outside Agencies	DIOG 12 and 14, generally
MAOP II	9-3.5.4	Accounting of Dissemination	DIOG 12.4 and 12.5
MAOP II	9-4.2.6	Investigative Activity in Congressional Offices	Interview or CHS - DIOG 18.5.6 and CHSPM
MAOP II	9-4.2.9	Dissemination to the White House Complex	Interview or CHS - DIOG 18.5.6. Paragraph (2) Superseded by AGG-Dom, DIOG and AG Memo WH Contacts
MAOP II	9-6	Major Cases - Dissemination of Information	DIOG Appendix K - Major Cases
MAOP II	9-7	Threat to Life - Dissemination of Information	DIOG 14
MAOP II	9-7.1	Information Concerning Threats Against the President and Other Designated Officials	DIOG 14
MAOP II	9-7.2	Information Concerning Threats, Possible Violence or Demonstrations Against Foreign Establishments or Officials in the US	DIOG 14
MAOP II	9-7.2.1	Information Received Through other Than Technical Surveillance	DIOG 14
MAOP II	9-7.2.2	Information Received Through Technical Surveillance	DIOG 14
MAOP II	9-7.2.3	Miscellaneous	DIOG 14
MAOP II	9-8	Replies to Foreign Police and Intelligence Contacts	DIOG 14
MAOP II	9-8.1	Letterhead Memoranda Prepared by Bureau's Foreign Offices	DIOG 14
MAOP II	9-8.2	Dissemination of Classified Information	DIOG 12, 14

UNCLASSIFIED – ~~FOR OFFICIAL USE ONLY~~
Domestic Investigations and Operations Guide

Part	Section	Section Title	DIOG Supersession
MAOP II	9-9	Dissemination of Grand Jury Material	DIOG 18.6.5
MAOP II	9-10	Dissemination of Title XI, Right to Financial Privacy Act of 1978	DIOG Appendix O - RFPA
MAOP II	9-13	Dissemination By Field Intelligence Groups	DIOG 14
MAOP II	10-9	General Rules Regarding Recording and Notification of Investigations	Supersede Paragraphs # 1a-c; 2a-c; 5; 6; 7; 9; 10a-c; 11-16; and 23-24. DIOG, various sections.
MAOP II	10-10.9.1	Approval by individuals Delegated to Act on Behalf of Higher Bureau Officials	DIOG 3.4.C
MAOP II	10-12	Notes made During Investigations - Interviews	DIOG 3, 14
MAOP II	10-13, 10-13.1, 10-13.2, 10-13.3, 10-13.4	FD-302	DIOG subsection 18.5.6.4.15.1
MAOP II	1-1.4 (3)	File Review	DIOG 3.4.4.1
MAOP II	2-5.1.4 (a) and (b)	Sub-file	Appendix J 1.5
MAOP II	2-4.1.5 (4)		Appendix J 1.4.4
MAOP II	10-16.2	Office of Origin	DIOG 14
MAOP II	13	FD-302	DIOG subsection 18.5.6.4.15.1
MAOP P1	21-7 (6)	Monitoring, Documenting and Reviewing	Remove second to last and last sentence only. Remove citation to MAOP at the end of Paragraph # 6 and add citation "See DIOG 3.4.4"
N/A	EC		34.D
N/A	EC	Legal Advice and Opinions, Tax Return Information, and Return information Relevant to Terrorism Cases; Ex Parte Orders	Appendix N

b7E

UNCLASSIFIED – ~~FOR OFFICIAL USE ONLY~~
Domestic Investigations and Operations Guide

Part	Section	Section Title	DIOG Supersession
N/A	EC	[redacted] Tax Return Information Other than Taxpayer Return Information to Terrorism-related Cases; delegation of Authority	Appendix N
N/A	EC	To Provide Guidance on Least Intrusive Techniques in National Security and Criminal Investigations - OGC EC [redacted] 12/20/2007	DIOG 4, 4.1, 4.4, 11.1.1, 18.1.1-2
N/A	EC	Mail Cover Cites - EC dated 12/22/2004	DIOG 11.3, 18.6.10
MIOG II	10-10.17.1, and form	FD-670, Consensual Monitoring - Telephone Checklist	DIOG 11.5, 18.6.1
N/A	form	FD-671, Consensual Monitoring - Non-telephone Checklist	DIOG 11.5, 18.6.1
N/A	EC	Electronic Surveillance - EC dated 12/20/2007	DIOG 11.12, 18.7.2-3
N/A	EC	Civil Liberties and Privacy EC issued by OGC dated 3/19/2004	DIOG 4.1, 6.3, 8.3, 9.3, 15.3
N/A	EC	Civil Liberties and Privacy EC issued by OGC dated 9/8/2005	DIOG 4.1, 7.3
N/A	EC	Least Intrusive Techniques in National Security and Criminal Investigations - EC issued by OGC on 12/20/2007, file number [redacted]	DIOG 4, 4.4, 18.1.1-2
N/A	EC	Protection of First Amendment Rights EC issued by OGC dated 3/19/2004 EC issued by CTD dated 09/01/2004 EC issued by OGC dated 12/05/2003	DIOG 4.2
N/A	EC	FBI National Collection Requirements EC issued by DO dated 01/30/2003	DIOG 5.11
N/A	EC	Retention and Dissemination of Privacy Act Records EC issued by OGC dated 03/19/2004	DIOG 5.13
N/A	EC	Authorized Investigative Methods in Assessments ECs issued by OGC dated 03/19/2004 and 9/18/2005	DIOG 18.3, 18.5
N/A	EC	Authorized Investigative Methods in Full Investigations EC issued by OGC dated 10/29/2003	DIOG 18.3, 18.7

b7E

b7E

UNCLASSIFIED – ~~FOR OFFICIAL USE ONLY~~
Domestic Investigations and Operations Guide

Part	Section	Section Title	DIOG Supersession
N/A	EC	Federal Grand Jury Subpoena EC issued by OGC dated 06/01/2007	DIOG 18.5.9, 18.6.5
N/A	EC	Administrative Subpoena EC issued by CID dated 06/06/2001	DIOG 18.6.4
N/A	EC	Voluntary Disclosure of Non-Content Customer Records	DIOG 18.6.8
N/A	EC	Definition of Investigative Method EC issued by OGC dated 10/14/2003	DIOG 18.6.9.3
N/A	EC	FISA Review Board for RISA Renewals EC issued by Director's Office dated 02/06/2006	DIOG 18.7.3.1.5.3
N/A	EC	Assistance to Other Agencies EC Issued by OGC dated 12/5/2003	DIOG 12
N/A	EC	Emergency Disclosure Provision for Information from Service Providers Under 18 U.S.C. Section 2702(b) - EC issued by OGC 08/25/2005, file number [REDACTED] [REDACTED] and [REDACTED]	DIOG 18
LHSA	7-4.1(7)	Consolidated Legal Handbook for Special Agents Section 7-4.1(7) into Interview Section of DIOG	DIOG 18
N/A	EC	Electronic Recording of Confessions and Witness Interviews - EC issued by OGC on 03/23/2006, file number [REDACTED] and [REDACTED] and EC dated 7/16/11, file [REDACTED]	DIOG 18
N/A	EC	FBI Mandated File Review Process - EC issued by INSD on 07/07/2010, file number [REDACTED]	DIOG 3
N/A	EC	Procedural and Operational Issuance - Guidance for Legislative Corruption - EC issued by CID on 08/08/2006, file number [REDACTED]	DIOG 18
N/A	CPD 0227	Designation of an Acting Official to Issue National Security Letters	DIOG 18.6.6.3
N/A	PD 0242D	Requirement for Written Operations Order- Field Operations	DIOG 19.2.3
N/A	CPN 0382N	Notice, National Security Mail Cover Request Approval Authority	DIOG 18.6.10.5

b7E

UNCLASSIFIED – ~~FOR OFFICIAL USE ONLY~~
Domestic Investigations and Operations Guide

Part	Section	Section Title	DIOG Supersession
N/A	CPN 00541N	Recordkeeping Policy for ELSUR Administrative Information Resulting from Joint Criminal Investigative Operations	DIOG 18.7.2.13
NA	EC/SAC Memo	March 5, 2003 Director's Memorandum to All Special Agents in Charge Re: Pre-Title III Electronic Surveillance (ELSUR) Search Policy, and the April 14, 2008, All Field Offices EC from RMD. Case ID# [REDACTED] [REDACTED]	Appendix H
N/A	RAP Tool User Guide v1.1	Resource Allocation Planning (RAP) Tool, User Guide v1.1 - delete definition of task force officer and task force member on page 1	DIOG 3

b7E

This Page is Intentionally Blank

UNCLASSIFIED – ~~FOR OFFICIAL USE ONLY~~
Domestic Investigations and Operations Guide

S APPENDIX S: (U) LISTS OF INVESTIGATIVE METHODS

S.1 INVESTIGATIVE METHODS LISTED BY NAME (ALPHABETIZED)

- (U) Administrative subpoenas. (Section 18.6.4)
- (U) CHS use and recruitment. (Section 18.5.5)
- (U) Closed-circuit television/video surveillance, direction finders, and other monitoring devices. (Section 18.6.3)
- (U) Consensual monitoring of communications, including electronic communications. (Section 18.6.1)
- (U) Closed-circuit television/video surveillance, direction finders, and other monitoring devices. (Section 18.6.3)
- (U) Electronic surveillance – FISA and FISA Title VII (acquisition of foreign intelligence information). 18.7.3)
- (U) Electronic surveillance – Title III. (Section 18.7.2)
- (U) FISA Order for business records. (Section 18.6.7)
- (U) Grand jury subpoenas. (Section 18.6.5)
- (U) Grand jury subpoenas – to providers of electronic communication services or remote computing services for subscriber or customer information only in Type 1 & 2 Assessments. (Section 18.5.9)
- (U) Information voluntarily provided by governmental or private entities. (Section 18.5.7)
- (U) Intercepting the communications of a computer trespasser. (Section 18.6.2)
- (U) Interview or request information from the public or private entities. (Section 18.5.6)
- (U) Mail covers. (Section 18.6.10)
- (U) National Security Letters. (Section 18.6.6)
- (U) On-line services and resources. (Section 18.5.4)
- (U) Pen registers and trap/trace devices. (Section 18.6.9)
- (U) Physical Surveillance (not requiring a court order). (Section 18.5.8)
- (U) Polygraph examinations. (Section 18.6.11)
- (U) Public information. (Section 18.5.1)
- (U) Records or information - FBI and DOJ. (Section 18.5.2)
- (U) Records or information - Other federal, state, local, tribal, or foreign government agency. (Section 18.5.3)
- (U) Searches that Do Not Require a Warrant or Court Order [REDACTED]
[REDACTED] and
Inventory Searches Generally. (Section 18.6.12)

b7E

- (U) Searches – with a warrant or court order. (Section 18.7.1)
- (U) Stored wire and electronic communications and transactional records. (Section 18.6.8)
- (U) Undercover Operations (Section 18.6.13)

S.2 INVESTIGATIVE METHODS LISTED BY ORDER IN DIOG SECTION 18

- 18.5.1 (U) Public information
- 18.5.2 (U) Records or information - FBI and DOJ.
- 18.5.3 (U) Records or information - Other federal, state, local, tribal, or foreign government agency.
- 18.5.4 (U) On-line services and resources.
- 18.5.5 (U) CHS use and recruitment.
- 18.5.6 (U) Interview or request information from the public or private entities.
- 18.5.7 (U) Information voluntarily provided by governmental or private entities.
- 18.5.8 (U) Physical Surveillance (not requiring a court order).
- 18.5.9 (U) Grand jury subpoenas – to providers of electronic communication services or remote computing services for subscriber or customer information only in Type 1 & 2 Assessments.
- 18.6.1 (U) Consensual monitoring of communications, including electronic communications.
- 18.6.2 (U) Intercepting the communications of a computer trespasser.
- 18.6.3 (U) Closed-circuit television/video surveillance, direction finders, and other monitoring devices.
- 18.6.4 (U) Administrative subpoenas.
- 18.6.5 (U) Grand jury subpoenas.
- 18.6.6 (U) National Security Letters.
- 18.6.7 (U) FISA Order for business records.
- 18.6.8 (U) Stored wire and electronic communications and transactional records.
- 18.6.9 (U) Pen registers and trap/trace devices.
- 18.6.10 (U) Mail covers.
- 18.6.11 (U) Polygraph examinations.
- 18.6.12 (U) Searches that Do Not Require a Warrant or Court Order (Trash Cover

and Inventory Searches Generally.
- 18.6.13 (U) Undercover operations.
- 18.7.1 (U) Searches – with a warrant or court order.

b7E

UNCLASSIFIED – ~~FOR OFFICIAL USE ONLY~~
Domestic Investigations and Operations Guide

18.7.2 (U) Electronic surveillance – Title III

18.7.3 (U) Electronic surveillance – FISA and FISA Title VII (acquisition of foreign intelligence information).