18.5.8 *(U) INVESTIGATIVE METHOD: PHYSICAL SURVEILLANCE (NOT REQUIRING A COURT ORDER)*

(U) *Note:* Consent Searches are authorized in Assessments.

(U)

b7E

18.5.8.1 (U) SCOPE

(U//~~FOUO~~) **Physical Surveillance Defined:** Physical surveillance is the deliberate observation of persons, places, or events, on either a limited or continuous basis, in areas where there is no reasonable expectation of privacy. (AGG-Dom, Part II.A.4.h)

(U//~~FOUO~~)

b7E

(U//~~FOUO~~)

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

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

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

b7E

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

(U//~~FOUO~~) **Surveillance Enhancement Devices:** The use of mechanical devices operated by the user (e.g., binoculars; hand-held photographic or video cameras;

is authorized as part of physical surveillance provided that the device is not used to collect information in which a person has a reasonable expectation of privacy

b7E

b7E

18.5.8.2 **(U) APPLICATION**

(U//~~FOUO~~)

18.5.8.3 **(U) APPROVAL**

(U//~~FOUO~~) During an Assessment, physical surveillance may be approved for a period of time not to exceed as explained further below. b7E

18.5.8.3.1 ***(U//~~FOUO~~) STANDARDS FOR OPENING OR APPROVING PHYSICAL SURVEILLANCE DURING AN ASSESSMENT***

(U//~~FOUO~~) During an Assessment, in addition to the standards contained in DIOG Sections 5.5 and 5.8, the FBI employee and supervisor must consider the following:

A) (U//~~FOUO~~) Whether the physical surveillance is rationally related to the articulated purpose and objective of the Assessment;

B) (U//~~FOUO~~) Whether the physical surveillance is the least intrusive alternative for acquiring needed information;

C) (U//~~FOUO~~) If the physical surveillance is for the purpose of determining a pattern of activity, whether there is a logical nexus between the purpose of the Assessment and the pattern of activity the employee is seeking to determine; and

D) (U//~~FOUO~~) If being conducted in order to gather positive foreign intelligence, whether the surveillance is consistent with the requirement that the FBI employee operate openly and consensually with a USPER, to the extent practicable.

18.5.8.3.2 ***(U//~~FOUO~~) PERIOD FOR ASSESSMENTS*** b7E

(U//~~FOUO~~) In an Assessment, an FBI employee must use a Guardian FD-71a, a Sentinel Lead Request form, or an EC

Guardian FD-71a, or EC

(U//~~FOUO~~)

b7E

b7E

18.5.8.3.3 ***(U//~~FOUO~~)***

(U//~~FOUO~~)

n a Guardian FD-71a, an EC, or other appropriate form requesting Assistant Special Agent in Charge (ASAC) approval. (*Note:* The 72 hour approval standard, renewable for additional is

b7E

(U//~~FOUO~~)

18.5.8.3.4 ***(U)***

(U//~~FOUO~~)

b7E

18.5.8.3.4.1 **(U//~~FOUO~~) APPROVAL REQUIREMENTS**

(U//~~FOUO~~)

must document the reason and objective for its use and be approved by an ASAC. The request and approval must be documented in an a Guardian FD-71a, an EC, or other appropriate form and electronically placed into the appropriate investigative file.

18.5.8.3.4.2 **(U//~~FOUO~~)**

b7E

(U//~~FOUO~~)

18.5.8.3.4.2.1 ***(U//~~FOUO~~)***

b7E

(U//~~FOUO~~)

(U//~~FOUO~~)

b7E

(U//~~FOUO~~)

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

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

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

4) (U//~~FOUO~~)

5) (U//~~FOUO~~)

(U//~~FOUO~~)

18.5.8.3.4.3 **(U//~~FOUO~~)** b7E

(U//~~FOUO~~)

(U//~~FOUO~~) *Note:*

18.5.8.3.4.4 **(U//~~FOUO~~) COMPLIANCE AND MONITORING**

(U//~~FOUO~~) The request and approval documentation for the use of must be electronically placed into the appropriate investigative file.

18.5.8.4 **(U) OTHER PHYSICAL SURVEILLANCE**

(U//~~FOUO~~) Physical surveillance conducted by employees, other than through use of the resources discussed above [redacted] during a predicated investigation does not require supervisory approval. In addition [redacted] b7E

18.5.8.5 **(U) MAINTAIN A "SURVEILLANCE LOG" DURING PHYSICAL SURVEILLANCE**

(U//~~FOUO~~) A surveillance log must generally be maintained for the purpose of documenting observations made during the period of physical surveillance. The log is a chronological narrative detailing the observations noted during the surveillance. A team member must be assigned to maintain the surveillance log. At the end of the surveillance, each individual must initial on the surveillance log the notations of the activities he or she observed. Completed physical surveillance logs must be placed in a 1A envelope in the investigative file. Surveillance logs must be concise and factual. When reporting locations, the surveillance log must be as specific as possible, but must avoid over-reporting and including unnecessary information. Logs are subject to discovery in legal proceedings.

(U) Surveillance observations may also be documented in an FD-302. All FBI employees present during the surveillance must be identified by name on the FD-302, and must review the FD-302 for accuracy prior to approval.

18.5.8.6 **(U) USE/DISSEMINATION**

(U//~~FOUO~~) The use or dissemination of information obtained by this method must comply with the AGG-Dom and DIOG Section 14

This Page is Intentionally Blank.

18.5.9 *(U) INVESTIGATIVE METHOD: GRAND JURY SUBPOENAS – TO PROVIDERS OF ELECTRONIC COMMUNICATION SERVICES OR REMOTE COMPUTING SERVICES FOR SUBSCRIBER OR CUSTOMER INFORMATION (ONLY IN TYPE 1 & 2 ASSESSMENTS)*

(U) See DIOG Section 18.6.5 for additional information on use of Federal Grand Jury (FGJ) subpoenas in predicated investigations.

18.5.9.1 (U) SCOPE

(U//~~FOUO~~) During a Type 1 & 2 Assessment, an agent or TFO may request from an appropriate USAO the issuance of an FGJ subpoena for the limited purpose of obtaining subscriber or customer information from providers of electronic communication services or remote computing services [redacted] A FGJ subpoena, under this provision, may not be requested for the purpose of collecting positive foreign intelligence. (AGG-Dom, Part II.A.4.i) b7E

18.5.9.2 (U) APPLICATION

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

18.5.9.3 (U) APPROVAL

(U//~~FOUO~~) In Type 1 & 2 Assessments, subscriber or customer information from providers of electronic communication services or remote computing services [redacted] may be requested through the use of an FGJ subpoena without supervisory approval. An agent or TFO requesting an FGJ subpoena during an Assessment must advise the Assistant United States Attorney (AUSA), who will issue the subpoena, that the FBI is conducting an Assessment. The AUSA must determine whether there is sufficient connection between the Assessment and possible criminal conduct to warrant issuance of an FGJ subpoena. FGJ subpoenas may not be sought during a Type 3, 4, 5, or 6 Assessment. b7E

18.5.9.3.1 *(U) MEMBERS OF THE NEWS MEDIA*[65]

(U//~~FOUO~~) [redacted] b7E

[65] Note: Due to an administrative error, the version of the DIOG released on September 17, 2021, prematurely included new requirements pertaining to the use of compulsory processes to obtain information from, or records of, members of the news media. As of October 25, 2021, those changes (including some that erroneously appeared on this page) have been reverted to the previous release of the DIOG, dated March 31, 2020. Additional updates about this topic are coming soon. Questions should be directed to CDCs or IPO.

b7E

(U) *Note:* 28 CFR § 50.10(b)(1)(ii) provides guidance on categories of individuals and entities not covered under the requirements set out above.

18.5.9.4 (U) GRAND JURY SUBPOENAS TO PROVIDERS OF ELECTRONIC COMMUNICATION SERVICES OR REMOTE COMPUTING SERVICES FOR SUBSCRIBER OR CUSTOMER INFORMATION (ECPA 18 U.S.C. § 2703)

(U//~~FOUO~~) Title 18 U.S.C. Section 2703 governs the disclosure of customer communications or records maintained by providers of electronic communication services or remote computing services when sought by a government agency through legal process. Subsection (c)(2) of Section 2703 specifies the types of records that may be obtained by the government pursuant to a subpoena.

(U//~~FOUO~~)

a. (U)

b. (U)

b7E

c. (U)

d. (U)

e. (U)

(U//~~FOUO~~) If any information is received in response to a FGJ subpoena issued pursuant to this subsection exceeds the limitations set forth above, that information must be treated as an overproduction and handled in accordance with the instructions set forth in section 18.6.5.15.

18.5.9.5 (U) RESTRICTIONS ON USE AND DISSEMINATION

(U//~~FOUO~~) Because judicial districts vary as to whether subscriber records obtained through use of an FGJ subpoena must be handled pursuant to the FGJ secrecy rules as "matters

b7E

[66] (U)

occurring before the federal grand jury," subscriber records obtained pursuant to an FGJ subpoena should be protected as required by the judicial district in which the FGJ subpoena is issued. See DIOG Section 18.6.5 for additional guidance.

(U//~~FOUO~~) In addition, in those judicial districts in which subscriber records obtained pursuant to an FGJ subpoena are considered to be matters occurring before the grand jury, no documentation of the actual subscriber records should be made in the unrestricted portion of the Guardian FD-71a. Instead, a copy of the FGJ subpoena and the responsive subscriber records must be [redacted] within the Guardian FD-71a [redacted] in the FBI's central record keeping system (Sentinel). b7E

(U//~~FOUO~~) [redacted] b7E

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

(U//~~FOUO~~) The use or dissemination of information obtained by this method must always comply with the AGG-Dom, DIOG Section 14, and the Federal Rules of Criminal Procedure (FRPC) Rule 6. FRCP 6(e), which is discussed below in DIOG subsections 18.6.5.11 and 12, and controls the release of information obtained as part of the FGJ proceeding.

[67] (U//~~FOUO~~) Telephone Applications has been replaced by Meta and Scales of Justice; however, the legal analysis in this EC still applies.

This Page Is Intentionally Blank.

18.6 (U) AUTHORIZED INVESTIGATIVE METHODS IN PRELIMINARY INVESTIGATIONS

(U) AGG-Dom, Part II.B and Part V.A.1-10.

(U) In Preliminary Investigations the authorized methods include the following:

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 18.5.3.1)

4) (U) Online 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) Consensual monitoring of communications, including electronic communications. (See Section 18.6.1)

C) (U) Intercepting the communications of a computer trespasser. (See Section 18.6.2)

D) (U) Closed-circuit television/video surveillance, direction finders, and other monitoring devices. (See Section 18.6.3)

E) (U) Administrative subpoenas. (See Section 18.6.4)

F) (U) Grand jury subpoenas. (See Section 18.6.5)

G) (U) National Security Letters. (See Section 18.6.6)

H) (U) FISA Order for business records. (See Section 18.6.7)

I) (U) Stored wire and electronic communications and transactional records. (See Section 18.6.8)[68]

J) (U) Pen registers and trap/trace devices. (See Section 18.6.9)

K) (U) Mail covers. (See Section 18.6.10)

L) (U) Polygraph examinations. (See Section 18.6.11)

M) (U) Searches that Do Not Require a Warrant or Court Order (Trash Cover, Abandoned Property from a Public Receptacle, Administrative Inventory Search of a Lost/Misplaced Item) and Inventory Searches Generally (See Section 18.6.12)

N) (U) Undercover operations. (See Section 18.6.13).

---

[68] (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)

This Page is Intentionally Blank.

18.6.1 *(U) INVESTIGATIVE METHOD: CONSENSUAL MONITORING OF COMMUNICATIONS, INCLUDING ELECTRONIC COMMUNICATIONS*

18.6.1.1 (U) SUMMARY

(U) Monitoring of wire, oral or electronic communications based on the consent of one party to the communication is referred to as consensual monitoring. The consent exception applies to the interception of wire, oral, and electronic communications. Consensual monitoring requires review by the CDC or the OGC. (AGG-Dom, Part V.A.4)

18.6.1.2 (U) APPLICATION

(U//~~FOUO~~)

b7E

(U//~~FOUO~~) See the *Advanced Electronic Surveillance and Searches Policy Directive and Policy Guide* (0626DPG) for additional guidance.

18.6.1.3 (U) LEGAL AUTHORITY

A) (U) The Fourth Amendment to the United States Constitution and case law interpreting the same.

B) (U) The Wiretap Statute, 18 U.S.C. § 2511-2522 , prohibits the intentional interception and use of wire, voice, or electronic communications absent an exception.

C) (U) The consensual monitoring exceptions, 18 U.S.C. § 2511(2)(c) & (d), require one party to the communication to consent to monitoring.

D) (U) The Foreign Intelligence Surveillance Act of 1978 (FISA), 50 U.S.C. §§ 1801 et seq., provides that if a party to the communication has consented to monitoring, a FISA court order is not required.

18.6.1.4 (U) DEFINITION OF INVESTIGATIVE METHOD

(U) Generally, the Wiretap Statute (also referred to as Title III), 18 U.S.C. §§ 2510-2522, prohibits the intentional interception of wire, oral, or electronic communications unless one of several exceptions applies. One such exception is based on the consent of a party to the communication. Two other statutory exceptions to the general prohibition include (1) the warrant or court order exception, and (2) the computer trespasser exception. This section discusses the monitoring of communications under the consent exception.

(U) Consensual monitoring is the monitoring of communications based on the consent of a party to the communication (*AGG-Dom*, Part VII.A.). For purposes of this policy, at least one of the parties to the communication must be located, or the interception of the consensual communication must occur within, the United States or the United States territories. The consensual monitoring of communications is subject to legal review by the CDC or OGC, as applicable. (*AGG-Dom*, Part V.A.4). Consensual monitoring includes the interception of the content of communications and typically falls into one of three general categories:

A) (U) ***Wire communications***, which include conventional telephone communications or other means of transmitting the human voice through cable, wire, radio frequency (RF), Voice over Internet Protocol (VoIP), or other similar connections.

B) (U) ***Oral communications***, typically intercepted through the use of devices that monitor and record oral conversations (e.g., a body transmitter or recorder; a fixed-location transmitter; or recorder used during face-to-face communications during which a person would have a reasonable expectation of privacy but for the consent of the other party).

C) (U) ***Electronic communications*** that are intercepted and recorded at the time of transmission. Electronic communications include any transfer of signs, signals, writing, images, sounds, data, or intelligence by a wire, radio, electronic, or optical system or network (e.g., e-mail, instant message, chat sessions, text messaging, nonvoice peer-to-peer communications), as that term is defined in 18 U.S.C. § 2510(12)(14) and (17). The monitoring of electronic communications based on one-party consent is sometimes referred to as "consensual computer monitoring." "Consensual computer monitoring" applies to "real-time" electronic surveillance based on consent and does not include retrieving or obtaining records of communications that have been stored on the computer or elsewhere after the communication has occurred.

(U) *Note regarding electronic communications monitoring:* Agents seeking to consensually monitor electronic communications (specifically, communications to, through, or from a computer) must consider whether the party who has consented is a party to all of the communications that they want to monitor or whether some of the communications involve a computer trespasser, as defined by the computer trespasser exception. (See DIOG Section 18.6.2) The trespasser exception and the consensual monitoring of communications exceptions are related but are separate exceptions to the Wiretap Statute. The owner, operator, and authorized users of a protected computer or computer network can consent to the monitoring of only those communications they send or receive (i.e., to which they are a party), which typically does not include a trespasser's communications. The trespasser exception allows the interception of the communications transmitted to or from the trespasser.

(U) When applicable, the exceptions to the Wiretap Statute can be used together, permitting the interception of the communications of both authorized users and trespassers on the protected computer. This is particularly useful when it is difficult to discern the trespasser communications from other communications. If it is possible to obtain consent to monitor the communications of the authorized users, use of both the consent and trespasser exceptions together can mitigate the risk of over or under collection of the trespasser's communications.

18.6.1.5 (U) STANDARDS AND APPROVAL/REVIEW REQUIREMENTS FOR CONSENSUAL MONITORING

18.6.1.5.1 *(U) GENERAL APPROVAL AND LEGAL REVIEW REQUIREMENTS*

(U//~~FOUO~~) Except as provided below, an employee must obtain prior CDC or OGC review and SSA approval for consensual monitoring of communications if the information likely to be obtained is relevant to an ongoing predicated investigation. CDC or OGC review and SSA approval must be documented with an FD-759 and serialized into the appropriate investigative ELSUR subfile, [redacted] b7E

(U//~~FOUO~~) Should an employee seek oral CDC or OGC review and SSA approval for the use of this method, they must be documented in an FD-759 as soon as practicable [redacted]

[redacted] after the oral authorization. Although AUSA concurrence is no longer required for consensual monitoring, providing notice to the AUSA is encouraged. b7E

18.6.1.5.1.1 **(U) REASONS FOR MONITORING**

(U//~~FOUO~~) The synopsis section of the FD-759 must include sufficient factual information supporting the need for the monitoring. It must provide the relationship between the monitoring and the investigative purpose (e.g., obtain evidence of drug trafficking or public corruption).

18.6.1.5.1.2 **(U) DOCUMENTED CONSENT OF A PARTY TO THE COMMUNICATION TO BE MONITORED**

(U//F~~OUO~~) Consent must be obtained from one of the parties to be monitored, and the consent must be documented. Having the consent of one of the parties provides an exception to the Title III statute. The requirement to obtain and document consent also applies to the monitoring of computer communications.

(U//F~~OUO~~) [redacted]

(U//F~~OUO~~) [redacted] b7E

(U//F~~OUO~~) [redacted]

(U//F~~OUO~~) [redacted]

18.6.1.5.1.2.1 ***(U) CONSENSUAL MONITORING OF COMPUTERS***

(U//F~~OUO~~) [redacted] b7E

b7E

[redacted] the CDC or OGC must review the document at issue to ensure that the implied consent is legally sufficient.

18.6.1.5.1.2.2 ***(U) CONSENT OF MORE THAN ONE PARTY REQUIRED FOR CONSENSUAL MONITORING***

(U//~~FOUO~~) Pursuant to *Attorney General Order No. 3594-2015* (November 18, 2015), the FBI may engage in the consensual monitoring of communications in accordance with FBI policies, even if it is considered a crime under state, local, territorial, or tribal law that may require all-party consent and does not sanction or provide a law enforcement exception [redacted]

b7E

18.6.1.5.1.2.3 ***(U)*** [redacted]

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

18.6.1.5.1.3 **(U) SUBJECT**

(U//~~FOUO~~) Agents conducting consensual monitoring must not intentionally intercept third-parties who are not of interest to the investigation except for unavoidable or inadvertent overhears.

18.6.1.5.1.4 **(U) LOCATION OF DEVICE**

(U//~~FOUO~~) Consensual monitoring can only be approved if appropriate safeguards are in place to ensure that the consenting party remains a party to the communication throughout the course of monitoring. For example, if a fixed-location monitoring device is being used, the consenting party must be admonished and must agree to be present during the duration of the monitoring. If practicable, technical means must be used to activate monitoring only when the consenting party is present.

18.6.1.5.1.5 **(U) NOTICE OF CONSENSUAL MONITORING TO OTHER FIELD OFFICES**

(U//~~FOUO~~) If an employee, CHS, or nonconfidential third party is operationally tasked to conduct consensual monitoring outside the field office's area of responsibility, the FBI employee requesting approval to conduct the monitoring must provide notice to the SSA who is responsible for the investigative program in the field office where the monitoring will occur. This notice must be documented with an FD-759 or other written documentation (e.g., and EC or a record e-mail) serialized in the investigative file. [redacted]

b7E

b7E

(U//~~FOUO~~) *For example:*

18.6.1.5.1.6 **(U) DURATION OF APPROVAL**

(U//~~FOUO~~) The request for approval must state the length of time needed for monitoring. Unless otherwise warranted, approval may be granted for the duration of the investigation, subject to a substantial change of circumstances. If one or more sensitive monitoring circumstances are present, DOJ may limit its approval to a shorter duration. See DIOG Section 18.6.1.6.2 below.

18.6.1.5.1.7 **(U) CHANGE OF MONITORING CIRCUMSTANCES**

(U//~~FOUO~~) Whenever the monitoring circumstances change substantially, a new FD-759 must be executed, requiring new supervisory approval, and the CDC or OGC must be contacted to obtain a new CDC or OGC legal review. (AGG-Dom, Part V.A.4.) The following are examples of substantial changes in monitoring circumstances which require a new FD-759: a different consenting party, a change in the location of a fixed monitoring device, or the addition of a new computer system, or a party to the communication relocates to another country.

(U//~~FOUO~~)

b7E

18.6.1.5.1.8 **(U) INVESTIGATION-SPECIFIC APPROVAL**

(U//~~FOUO~~)

18.6.1.5.1.9 **(U) CONSENSUAL MONITORING IN JOINT INVESTIGATIONS**

(U//~~FOUO~~) In joint investigations, consensual monitoring conducted by FBI employees or FBI CHSs is generally governed by FBI policies. However, consensual monitoring conducted by a nonconfidential party (e.g., witness or a victim) will be controlled by the agency that is primarily responsible for the nonconfidential party. In a joint investigation, the employees should reach an understanding as to which agency is responsible for the

nonconfidential party; that agency's policies will govern approval and documentation requirements for consensual monitoring.

18.6.1.6 (U) Consensual Monitoring Situations Requiring Additional Notice or Approval

18.6.1.6.1 *(U) Party Located Outside the United States*

18.6.1.6.1.1 (U//~~FOUO~~) Consensual Monitoring of Communications

(U//~~FOUO~~) This subsection applies to forms of consensual monitoring except for the use of consensual computer monitoring discussed in subsection 18.6.1.6.1.2.

(U//~~FOUO~~)

(U//~~FOUO~~)

b7E

(U//~~FOUO~~) **NOTE:**

(U//~~FOUO~~)

b7E

(U//~~FOUO~~)

b7E

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

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

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

18.6.1.6.1.2 **(U//~~FOUO~~) CONSENSUAL COMPUTER MONITORING OF PARTIES OUTSIDE THE UNITED STATES**

(U//~~FOUO~~)

b7E

18.6.1.6.2 ***(U) SENSITIVE MONITORING CIRCUMSTANCE***

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

A) (U) Investigation of a member of Congress, a federal judge, a member of the executive branch at Executive Level IV or above or a person who has served in such capacity within the previous two years. (Executive Levels I through IV are defined in 5 U.S.C. §§ 5312-5315.)

B) (U) Investigation of the governor, lieutenant governor, or attorney general of any state or territory, or a judge or a justice of the highest court of any state or territory, concerning an offense involving bribery, conflict of interest, or extortion related to the performance of official duties.

C) (U) The Attorney General, the deputy Attorney General, or an assistant Attorney General has requested that the FBI obtain prior approval for the use of consensual monitoring in a specific investigation.

D) (U) A party to the communication is in the custody of the Bureau of Prisons (BOP) or the United States Marshals Service (USMS) or is being or has been afforded protection in the Witness Security Program.

(U//~~FOUO~~) *Note:*

E) (U//~~FOUO~~)

b7E

F) (U//~~FOUO~~) See *DIOG Appendix G – Classified Provisions* [links to a ~~SECRET//NOFORN~~ document] for additional information regarding consensual monitoring.

18.6.1.6.2.1 **(U//~~FOUO~~) PROCEDURE FOR OBTAINING DOJ APPROVAL FOR A SENSITIVE MONITORING CIRCUMSTANCE:**

(U//~~FOUO~~)

b7E

18.6.1.6.2.2 **(U//~~FOUO~~) EMERGENCY REQUESTS INVOLVING SENSITIVE MONITORING CIRCUMSTANCES**

(U//~~FOUO~~)

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

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

(U//~~FOUO~~) *Note:*

b7E

(U//~~FOUO~~)

(U//~~FOUO~~) b7E

18.6.1.7 **(U) DOCUMENTING THE USE OF CONSENSUAL MONITORING WITH AN FD-302**

(U) b7E

18.6.1.8 **(U) COMPLIANCE AND MONITORING**

(U//~~FOUO~~) Case agents and supervisors must regularly monitor the use of this method to ensure that the continued interception of communications is warranted and has been lawfully obtained by virtue of consent, express or implied, from a party to the communication. Such monitoring must include a review of the investigative file to ensure that consent and authorization forms are properly completed and appropriately filed in the 1A section of the investigative file (FD-472 and FD-1071 consent forms) and in ELSUR subfile (FD-759, "Notification of Authority Granted for Use of Electronic Monitoring Equipment - Not Requiring a Court Order"). ELSUR program personnel must review all submitted FD-759s and consent forms (FD-472s and FD-1071s) to confirm that proper approval has been documented for the consensual monitoring of communications.

18.6.1.9 **(U) EVIDENCE HANDLING** b7E

(U//~~FOUO~~)

(U//~~FOUO~~) For additional information see the

This Page Is Intentionally Blank.

18.6.2 *(U) INVESTIGATIVE METHOD: INTERCEPTING THE COMMUNICATIONS OF A COMPUTER TRESPASSER*

18.6.2.1 (U) SUMMARY

(U) The wire or electronic communications of a computer trespasser to, from, or through a protected computer may be intercepted and collected during a predicated investigation. Use of this method requires SSA approval and review by the CDC or the OGC. (AGG-Dom, Part V.A.4)

18.6.2.2 (U) APPLICATION

(U//~~FOUO~~)

b7E

18.6.2.3 (U) LEGAL AUTHORITY

A) (U) The Fourth Amendment to the United States Constitution and case law interpreting the same;

B) (U) The Wiretap Statute, 18 U.S.C. § 2511, prohibits the intentional interception and use of wire, oral, or electronic communications absent an exception;

C) (U) Computer Trespasser Exception, 18 U.S.C. § 2511(2)(i); and

D) (U) The Foreign Intelligence Surveillance Act of 1978 (FISA), 50 U.S.C. §§ 1801 et seq., requires court authorization for "electronic surveillance." FISA specifically provides, however, that the acquisition of computer trespasser communications that would be permissible under 18 U.S.C. § 2511(2)(i) are not subject to the FISA court order requirement for electronic surveillance of wire communication under 101(f)(2) of FISA. 50 U.S.C. § 1801(f) (2).

18.6.2.4 (U) DEFINITION OF THE COMMUNICATIONS OF A COMPUTER TRESPASSER

(U) Generally, the Wiretap Statute (also referred to as Title III), 18 U.S.C. §§ 2510-2522, prohibits the intentional interception of wire, oral, or electronic communications unless one of several exceptions applies. One such exception is the interception of a computer trespasser's wire or electronic communications to, through, or from a protected computer based on the authorization of the owner or operator of that computer. Another statutory exception is based on the consent of a party to the communication. This section relates specifically to the computer trespasser exception; the policy on consensual recording of computer communications can be found at DIOG Section 18.6.1.

(U) The computer trespasser exception to the Wiretap Statute, 18 U.S.C. § 2511(2)(i), permits a person acting under color of law to intercept the wire or electronic communications of a computer trespasser that are transmitted to, through, or from a protected computer when the owner or operator of that computer authorizes the interception. The use of this method does not include retrieving or obtaining records of communications that have been stored on the computer or elsewhere after the communication has occurred.

(U) The statute requires:

A) (U) The owner or operator of the protected computer to authorize the interception of the trespasser's communications on the protected computer;

B) (U) The person acting under color of law to be engaged in a lawful investigation;

C) (U) The person acting under color of law to have reasonable grounds to believe that the contents of the trespasser's communications will be relevant to the investigation; and

D) (U) The interception is limited to the communications transmitted to or from the trespasser.

(U) The case agent is responsible for documenting the basis for the conclusion that the person who provided authorization to intercept the trespasser's communications is either the owner or operator of the protected computer. The "owner or operator" must have sufficient authority over the protected computer/computer network system to authorize access across the entire system. This could be a corporate officer, CIO, or system administrator, if the system administrator has authority across the entire system. In any instance in which the identification of the owner or operator is not plainly evident, the case agent must seek the assistance of the CDC or the OGC to identify the proper owner or operator.

(U) A "protected computer," defined in 18 U.S.C. § 1030(e), has been generally interpreted to be any computer or computer network device connected to the Internet, although it also includes most computers used by a financial institution or the United States Government regardless of whether the computer is connected to the Internet.

(U) A "computer trespasser" is a person who accesses a protected computer without authorization and thus has no reasonable expectation of privacy in any communication transmitted to, from, or through the protected computer. The definition of computer trespasser does not include a person known by the owner or operator to have exceeded their authority or to have an existing contractual relationship with the owner or operator for access to all or part of the computer. (18 U.S.C. § 2510(21))

(U) The trespasser exception and the consensual monitoring of communications exception are related, but separate, exceptions to the Wiretap Statute. The owner, operator, and authorized users of a protected computer can consent to the monitoring of only those communications they send or receive (i.e., communications to which they are a party), which do not include a trespasser's communications. (See DIOG Section 18.6.1) In comparison, under the trespasser exception, the owner or operator may only authorize the interception of the communications of a trespasser transmitted to, through, or from the protected computer.

(U) When applicable, the computer trespasser and consensual monitoring of communications exceptions to the Wiretap Statute can be used together, permitting the interception of communications of both authorized users and trespassers on the protected computer. This is particularly useful when it is difficult to discern the trespasser communications from other communications. If it is possible to obtain consent to monitor the communications of the authorized users, using the consent and trespasser exceptions together can mitigate the risk of over or under collection of the trespasser's communications. See DIOG Section 18.6.1 for the policy regarding consensual monitoring of computer communications.

18.6.2.5 (U//FOUO) USE AND APPROVAL REQUIREMENTS FOR INTERCEPTING THE COMMUNICATIONS OF A COMPUTER TRESPASSER

18.6.2.5.1 *(U) GENERAL APPROVAL REQUIREMENTS*

(U//~~FOUO~~) An SSA may approve the use of the computer trespasser exception, subject to CDC or OGC review. Approval is conditioned on the following criteria being met and documented on the FD-759 and through other supporting documentation in the investigative file:

18.6.2.5.1.1 (U) REASONS FOR THE INTERCEPTION

(U//~~FOUO~~) The synopsis portion of the FD-759 must include sufficient facts to support the need for the interception and to explain how the contents of the trespasser's communications will be relevant to the investigative purpose.

18.6.2.5.1.2 (U) OWNER OR OPERATOR AUTHORIZATION

(U//~~FOUO~~) The authorization of the owner or operator of the protected computer (who may be the system administrator, as stated above) to a person acting under color of law to intercept the trespasser communications on the protected computer system or network must be documented using the FD-1070, "Authorization to Intercept the Communications of a Computer Trespasser." The steps the case agent takes to ensure that the person providing the authorization is the actual or appropriate owner or operator of the protected computer must be documented in the investigative file. See 18.6.2.6 below for specific procedures.

18.6.2.5.1.3 (U) ACQUIRING ONLY TRESPASSER COMMUNICATIONS

(U//F~~OUO~~) When intercepting communications under the computer trespasser exception alone (i.e., not in conjunction with consensual monitoring of electronic communications), the collection must not intentionally acquire communications other than those to or from the trespasser. This can often be technically complicated to accomplish depending on the use and configuration of the protected computer and the sophistication of the trespasser. The steps to be taken to identify trespasser communications and to isolate such communications from those of authorized users must be considered by the approving and reviewing officials and documented in the investigative file. See DIOG Section 18.6.2.6 below for specific procedures.

18.6.2.5.1.4 (U) OWNER OR OPERATOR COLLECTION

(U//F~~OUO~~) The interception of trespasser communications may be conducted by the FBI or by the owner or operator of the protected computer at the FBI's request. In either instance, the interception is being conducted under color of law. If the collection is not being conducted by the FBI, the case agent must document that he or she has informed the person conducting the interception that it must be accomplished in conformity with the statute.

18.6.2.5.1.5 (U) LOCATION OF INTERCEPT

(U//F~~OUO~~) If the intercept or collection of the trespasser communications will occur outside of the field office of the approving official, the SAC or ASAC of the field office

within which the interception will occur must be notified, and the notification must be documented in the investigative file.

18.6.2.5.1.6 ***(U) DURATION***

(U//F~~OUO~~) The request for approval (FD-759) must state the length of time needed for the interception. Unless otherwise warranted, approval may be granted for the duration of the investigation, subject to a substantial change of circumstances, as described in DIOG Section 18.6.2.6, below.

18.6.2.5.1.7 ***(U) LEGAL REVIEW***

(U//~~FOUO~~) Prior to conducting the interception, the CDC or OGC must review the request and determine that, given the facts of the investigation, the interception appears to be lawful under the computer trespasser exception. Whenever the factors surrounding the use of the approved technique change substantially, a new FD-759 must be executed. The newly executed FD-759 must include new legal review by the CDC or OGC. (AGG-Dom, Part V.A.4.) The following are examples of substantial changes in the circumstances of the interception that require a new FD-759: a change in owner or operator, a change in the method of collection, or the change or addition of a protected computer system. On the other hand, technical changes in the collection system for the purpose of improving or refining the interception are usually not substantial changes to the circumstances of the interception.

18.6.2.5.1.8 ***(U) JOINT INVESTIGATIONS***

(U//~~FOUO~~) In joint investigations, if the FBI is the lead investigating agency, FBI policies and guidance regarding the interception of computer trespasser communications must be followed. If the FBI is not the lead investigating agency, the policies of the lead investigating agency must be followed and documented to the appropriate FBI investigative file.

18.6.2.5.1.9 ***(U) EXTRATERRITORIAL CONSIDERATIONS***

(U//~~FOUO~~) b7E

18.6.2.6 (U) DURATION OF APPROVAL FOR INTERCEPTING THE COMMUNICATIONS OF A COMPUTER TRESPASSER

(U//F~~OUO~~) The interception and collection of computer trespasser communications under the computer trespasser exception may be approved for a specified length of time or for the duration of the particular investigation.

18.6.2.7 (U) SPECIFIC PROCEDURES FOR INTERCEPTING THE COMMUNICATIONS OF A COMPUTER TRESPASSER

(U//F~~OUO~~) The following procedures apply when obtaining authorization.

18.6.2.7.1 *(U) DOCUMENTING AUTHORIZATION TO INTERCEPT*

(U//~~FOUO~~) Whenever possible, written authorization must be obtained from the owner or operator of the protected computer and documented on an FD-1070, "Authorization to Intercept the Communications of a Computer Trespasser," or any subsequent form as appropriate. If the authorization from the owner or operator is provided orally, at least one FBI agent and another law enforcement or intelligence officer should witness the authorization, and the authorization must be memorialized in an FD-302. The fact that the authorizing party has declined or was unable to give written authorization must also be recorded on the FD-1070. This form should then be completed with the exception of the authorizing party's signature.

(U//~~FOUO~~) The case agent must document to the file (i.e., FD-302 or EC) the facts that establish that the person providing the authorization is a proper party to provide authorization for the anticipated interception.

(U//~~FOUO~~) The FD-1070 signed by the owner/operator must be maintained in the 1A section of the appropriate investigative file. If the consenting party is a CHS, the CHS must sign the FD-1070 in his/her payment name and the original FD-1070 must be maintained in the 1A section of the appropriate investigative file, with a separate copy filed in the CHS file in Delta. The FD-1070 is case specific and will remain valid until such time as the consenting or authorizing party revokes the consent or authorization, either orally or in writing, to an FBI agent or TFO, or the FBI terminates the investigation.

(U//~~FOUO~~) If the case agent is seeking approval for the FBI to engage in both consensual monitoring and an interception of the computer trespasser on the same computer system, separate forms --

b7E

18.6.2.7.2 *(U) ACQUIRING ONLY THE TRESPASSER COMMUNICATIONS*

(U//F~~OUO~~) The computer trespasser exception permits the FBI to intercept only trespasser communications. Prior to seeking approval to intercept computer trespasser communications, the case agent must coordinate the use of the method with the Field Office Technical Advisor by submission of an Electronic Technical Request (ETR). On receipt of the ETR, the Technical Advisor must ensure that the technical equipment and expertise necessary to lawfully implement the interception are timely provided following approval to use this investigative method.

(U//F~~OUO~~) Many of the technical challenges and risks associated with accurately isolating the trespasser communications can be mitigated by also obtaining consent to monitor the computer or a court order. The possibility of using the authority to intercept trespasser communications in conjunction with consent should be raised at the time of the ETR submission or as soon thereafter as the case agent determines that the authorized users of the protected computer will consent to FBI monitoring.

(U//~~FOUO~~) When intercepting trespasser communications, the case agent must prepare an FD-302 or EC detailing the steps taken to identify trespasser communications and to isolate such communications from those of authorized users. For example: "reviewed system logs provided by the system administrator and identified a trespasser accessing the system at the

following dates and times via IP address xxx or port xxx." Additionally, any subsequent review or revision of the steps needed to identify and isolate the trespasser's communications must also be documented to the investigative file by an EC or FD-302, as appropriate.

18.6.2.7.3 *(U) REVIEWING THE ACCURACY OF THE INTERCEPTION*

(U//~~FOUO~~) At the initiation of the interception and collection of computer trespasser communications, the Technical Advisor or designated technically trained agent (TTA) coordinating the implementation of the interception and collection device shall ensure that appropriate collection parameters are implemented as required by OTD policy and procedures.

(U//~~FOUO~~) The case agent shall ensure a timely initial review of the collected information to verify that the interception and collection are limited to communications authorized for interception and collection under the trespass authority or other lawful exception. Following this initial review, the case agent shall ensure that a similar review and evaluation is repeated at appropriate intervals throughout the duration of the interception to ensure that the interception and collection remain within the scope of the trespasser or other lawful exceptions. Factors that may impact the frequency of reviews include, but are not limited to: volume of data to be reviewed, complexity and nature of data collected, and complexity of the trespassed system.

(U//~~FOUO~~) Any FBI employee who identifies interception and collection of communications that may be outside the scope of the trespasser or other lawful exception shall immediately notify the case agent and the operational SSA of the possible unauthorized interception and collection of communications. Upon the determination that communications have been unlawfully intercepted or collected, the interceptions and collection must be halted immediately. The case agent must consult with a TTA to determine whether collection may be resumed in a manner that assures further unlawful collections will not occur. If the SSA determines that unlawful collection can be reliably prevented, that determination must be documented to the file before lawful interceptions and collection may resume.

(U//~~FOUO~~) The content of communications determined to have been unlawfully collected cannot be used in any manner and shall be removed promptly from all FBI systems and destroyed. A memorandum documenting the removal and destruction shall be filed in the main investigation file and the appropriate investigative ELSUR sub-file.

18.6.2.7.4 *(U) REVIEWING THE RELEVANCY OF THE INTERCEPTION*

(U//F~~OUO~~) The trespasser exception requires the FBI to have a reasonable belief that the contents of the trespasser's communications will be relevant to the investigation. Following the initiation of the interception and collection of the trespasser communication, the case agent must ensure that the collected communications are reviewed, at appropriate intervals throughout the duration of the interception, to determine whether the interception is and continues to be relevant to the authorized investigation. Factors that may impact the frequency of reviews include, but are not limited to: volume of data to be reviewed, complexity and nature of data collected, and complexity of the trespassed system.

18.6.2.7.5 *(U) DURATION OF APPROVAL*

(U//~~FOUO~~) Authorization to intercept trespasser communications remains valid until such time as the authorizing party, orally or in writing, revokes the authorization or on the termination date of the authorization, whichever comes first.

18.6.2.7.6 *(U) ELSUR REQUIREMENTS*

(U//F~~OUO~~) The information obtained from the collection must be retained in conformity with the ELSUR Policies located in the OGC Main Law Library) or other applicable policies.

(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 Sentinel.

18.6.2.7.7 *(U) MULTIPLE COMMUNICATIONS.*

(U//~~FOUO~~) In investigations in which various modes of communication may be intercepted (e.g., telephonic, non-telephonic, electronic communications, etc., or the use of consensual computer monitoring in conjunction with the interception of trespasser communications), one FD-759 may be used to document approval, provided that each mode of communication to be monitored is being used in the same investigative file and all facts required on the FD-759 are the same. If the material facts on the FD-759 vary (e.g., different periods of authority, etc.), separate FD-759s must be executed.

18.6.2.7.8 *(U) INVESTIGATION SPECIFIC APPROVAL*

(U//~~FOUO~~) Approval for intercepting a computer trespasser's communications is investigation specific and is not transferable to any other investigation, unless the investigative file under which the authority was granted is consolidated or reclassified. Investigation specific approval must be obtained for any spin-off investigation(s) that arises out of the original investigation.

18.6.2.8 (U) COMPLIANCE AND MONITORING

(U//~~FOUO~~) Case agents must regularly monitor the use of this method to ensure that the continued interception of trespasser communications is warranted and being lawfully conducted. Such monitoring shall include a review of the investigative file to ensure that consent and authorization forms have been properly executed and filed. ELSUR program personnel must review all submitted FD-759 and FD-1070, "Authorization to Intercept the Communications of a Computer Trespasser" forms to ensure proper approval has been documented for the interception of computer trespasser communications.

18.6.2.9 (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 Sentinel.

This Page is Intentionally Blank.

18.6.3 *(U//~~FOUO~~) INVESTIGATIVE METHOD: [redacted] CLOSED-CIRCUIT TELEVISION/VIDEO SURVEILLANCE, DIRECTION FINDERS, AND OTHER MONITORING DEVICES* b7E

18.6.3.1 (U) SUMMARY

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

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

18.6.3.2 (U) APPLICATION

(U//~~FOUO~~) [redacted] b7E

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

18.6.3.3 (U) LEGAL AUTHORITY

A) (U) AGG-Dom, Part V

B) (U) Rule 41 Federal Rules of Criminal Procedure

C) (U) Fourth Amendment to the United States Constitution

18.6.3.4 (U) DEFINITION OF INVESTIGATIVE METHOD

A) (U//~~FOUO~~) Closed circuit television / video surveillance (CCTV / video surveillance): a fixed-location video camera / device that is typically concealed from view or that is placed on or operated by a consenting party. See *License Plate Reader Policy Directive (0917D)* for guidance on the use of FBI LPR systems.

B) (U//~~FOUO~~) Electronic tracking devices: See OGC's guidance for use of electronic tracking devices and also OTD's *Technology-Based Tagging, Tracking and Locating Program Policy Directive and Policy Guide* (0643DPG).

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

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

(U//F~~OUO~~) Except for a hand-held video as described above, CDC or OGC review and SSA approval is required for the use of CCTV/Video Surveillance. CDC review and SSA approval must be documented using the FD-759. SSA approval may be granted if the following criteria have been met:

A) (U//~~FOUO~~) Legal review from the CDC or OGC that a court order is not required for installation or use of the device because there has been lawful consent, no reasonable expectation of privacy exists, or no physical trespass is necessary to install the device. Whenever circumstances change in either installation or monitoring, a new legal review must be obtained to determine whether a separate authorization is necessary;

B) (U//~~FOUO~~) Use of the method is reasonably likely to achieve investigative objectives;

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

b7E

18.6.3.6 (U) DURATION OF APPROVAL

(U//F~~OUO~~)

18.6.3.7 (U) SPECIFIC PROCEDURES

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

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

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

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

b7E

D) (U//~~FOUO~~) [redacted] b7E

18.6.3.8 **(U) CCTV/VIDEO SURVEILLANCE WHERE THERE IS A REASONABLE EXPECTATION OF PRIVACY IN THE AREA TO BE VIEWED OR FOR THE INSTALLATION OF THE EQUIPMENT.**

18.6.3.8.1 ***(U) WARRANT OR COURT ORDER***

(U//~~FOUO~~) A warrant/court order is required for the use of CCTV/Video Surveillance when a reasonable expectation of privacy exists in either the area to be viewed or the location where the equipment will be installed, unless the installation and monitoring is being conducted pursuant to consent. See DIOG Section 18.6.3.8.2 below for the required consultation with the Technical Advisor (TA) or technically Trained Agent (TTA).

A) (U//FO~~UO~~) ***Criminal Investigations:*** When there is a reasonable expectation of privacy in the area to be viewed and no consenting party, prior DOJ/OEO approval is required before seeking a warrant/order. When there is a reasonable expectation of privacy only in the location where the CCTV/Video Surveillance equipment will be installed, but not in the area to be viewed, prior DOJ/OEO authorization is not required to seek a warrant/order for the installation. In an emergency situation where CCTV usage is desired and a warrant/court order would be required, but cannot be obtained within the time required, an AUSA must be contacted to seek DOJ/OEO's guidance on how to proceed.

B) (U//~~FOUO~~) ***National Security Investigations:*** The use of CCTV/Video Surveillance in national security investigations under the Foreign Intelligence Surveillance Act of 1978 (FISA) requires the filing of an appropriate FISA court order because the use of CCTV/Video Surveillance falls within the definition of "electronic surveillance" under FISA. See DIOG Section 18.7.3.

C) (U//~~FOUO~~) ***Where a warrant is required and the request is included with a Title III or is a FISA request:*** Where the CCTV/video surveillance request is made pursuant to FISA or in conjunction with a Title III request, the required supervisory approvals and CDC or OGC review will take place as part of the larger FISA or Title III review and approval process. No additional reviews or approvals for the CCTV/video surveillance are required.

D) (U//~~FOUO~~) ***Where a warrant is required and the request is NOT coupled with a Title III request or made pursuant to FISA:*** As the FD-759 is not used when a court order is needed, the required SSA approval and CDC or OGC review must be documented in an EC. Maintain the original SAC approved EC in the appropriate investigative ELSUR sub-file.

18.6.3.8.2 ***(U//~~FOUO~~) REQUIRED CONSULTATION WITH TECHNICAL ADVISOR (TA) OR TECHNICALLY TRAINED AGENT (TTA)***

(U//~~FOUO~~) Prior to filing an application and affidavit for a warrant/court order under Rule 41/All Writs Act (in criminal law-based investigations) or under FISA (in national security-based investigations), the case agent/special agent must consult with the field office TA/TTA to:

A) (U//F~~OUO~~) consider any potential technical issues; and

B) (U//~~FOUO~~) review any "technical" or "technique" language used in the application and affidavit.

(U//~~FOUO~~) This review ensures that the language used therein is accurate and does not disclose classified/sensitive methods and techniques.

18.6.3.9 **(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 Sentinel.

18.6.3.10 **(U)**

(U//~~FOUO~~)

b7E

(U//~~FOUO~~)

18.6.3.11 **(U) CCTV/VIDEO SURVEILLANCE EQUIPMENT – TYPES, AVAILABILITY, REPAIR AND DISPOSAL**

18.6.3.11.1 ***(U) EQUIPMENT TYPES***

(U//~~FOUO~~) Listed below are categories of CCTV/Video Surveillance equipment and related methods. Since CCTV/Video Surveillance tools change with some frequency, available equipment and methods can be accessed via the VSU BuNET page.

b7E

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

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

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

18.6.3.11.1.1 **(U//FOUO)**

(U//~~FOUO~~) is an approved, unclassified system that supports FBI special agents and tactical groups using CCTV/Video Surveillance methods that

18.6.3.11.2 *(U) EQUIPMENT AVAILABILITY*

(U//~~FOUO~~) If CCTV/Video Surveillance equipment is not available from the existing field office inventory, the TA/TTA must use the Technical Management Database (TMD) to forward requests to the appropriate VSU program manager (PM).

18.6.3.11.2.1 (U) SURVEY SHEET

(U//~~FOUO~~) The TA or TTA should contact the case agent/special agent requesting the CCTV/video surveillance to determine his/her objective and expectations of the CCTV/Video Surveillance. The [redacted] is designed to capture the information needed to maximize investigative *and technical success when using CCTV/Video Surveillance equipment.* b7E

18.6.3.11.3 *(U) EQUIPMENT REPAIR*

(U//~~FOUO~~) Field office TAs/TTAs must consult with the appropriate VSU PM and obtain approval prior to sending any CCTV/Video Surveillance equipment to VSU for repairs.

18.6.3.11.4 *(U) EQUIPMENT DISPOSAL*

(U//~~FOUO~~) Field office TAs/TTAs must determine the appropriate disposition of non-repairable equipment. Surplus property will be disposed of by field offices for equipment under its cost code.

18.6.3.12 (U) COMPLIANCE AND MONITORING

(U//~~FOUO~~) Authorization documents regarding the use of the CCTV/Video must be documented in the appropriate investigative ELSUR sub-file and will be available for compliance and monitoring review. See this Section and DIOG Section 18.6.1.9 (consensual CCTV/video surveillance use) for the requirements for using CCTV/Video Surveillance. See OTD's [redacted] b7E

This Page Is Intentionally Blank.

18.6.4 *(U) INVESTIGATIVE METHOD: ADMINISTRATIVE SUBPOENAS (COMPULSORY PROCESS)*

18.6.4.1 (U) OVERVIEW OF COMPULSORY PROCESS

(U//~~FOUO~~)

b7E

(U)

18.6.4.2 (U) APPLICATION

(U//~~FOUO~~)

b7E

18.6.4.3 (U) ADMINISTRATIVE SUBPOENAS

18.6.4.3.1 *(U) SUMMARY*

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

(U//FOUO) Within the FBI, the authority to issue administrative subpoenas is limited to positions authorized by the Attorney General; that authority may not be further redelegated.

b7E

18.6.4.3.2 ***(U) LEGAL AUTHORITY AND DELEGATION***

18.6.4.3.2.1 **(U) INVESTIGATIONS INVOLVING THE SALE, TRANSFER, MANUFACTURE OR IMPORTATION OF UNLAWFUL DRUGS**

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

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

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

(U//F~~OUO~~) ***Delegated authority to issue:*** By DOJ regulation, the Attorney General's delegation includes SACs, ASACs, SSRAs and "those FBI Special Agent Squad Supervisors who have management responsibilities over Organized Crime/Drug Program investigations."

(U//F~~OUO~~) ***Multi-offense investigations:***

b7E

(U//F~~OUO~~) ***Confidentiality:***

18.6.4.3.2.2 **(U) INVESTIGATIONS INVOLVING THE SEXUAL EXPLOITATION AND ABUSE OF CHILDREN**

(U) ***Authority:*** 18 U.S.C. § 3486(a) and Attorney General Order 4227-2018.

(U) ***May be issued to:***

i) (U//F~~OUO~~) Any individual or business holding records or things relevant to the investigation of a federal offense involving the sexual exploitation or abuse of children. The subpoena may require production as soon as possible, but in no event less than 24 hours after service of the subpoena.

ii) (U//F~~OUO~~) A "provider of an electronic communication service" or a "remote computer service" (both terms are defined in DIOG subsection 18.6.4.3.4.2.1) and only for the production of basic subscriber or customer information. The subpoena may require production as soon as possible, but in no event less than 24 hours after service of the subpoena.

(U) ***Records to be obtained:***

i) (U) For administrative subpoenas issued to individuals or businesses:

(U//~~FOUO~~) Any records relevant to an investigation of a federal offense involving the sexual exploitation or abuse of children.

ii) (U) For administrative subpoenas issued to providers of electronic communication services or remote computer services:

(U)

b7E

(U) ***Delegated authority to issue:***

(U//~~FOUO~~)

(U) ***Violations to which this authority applies:***

(U//~~FOUO~~) These administrative subpoenas may only be issued in investigations that involve violations of 18 U.S.C. §§ 1201, 1591, 2241(c), 2242, 2243, 2251, 2251A, 2252, 2252A, 2260, 2421, 2422, or 2423 in which the victim is less than 18 years old

b7E

18.6.4.3.2.3 **(U) INVESTIGATIONS INVOLVING FEDERAL HEALTH CARE FRAUD OFFENSES**

(U) ***Authority:*** 18 U.S.C. § 3486(a)

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

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

(U//~~FOUO~~) ***Delegated authority to issue:*** The Attorney General has not delegated signature authority to the FBI. AG authority is delegated only to personnel within DOJ's Criminal Division and to United States Attorneys, who may redelegate the authority to

AUSAs. FBI employees must request an AUSA to issue administrative subpoenas in health care fraud investigations.

(U) ***Limitations:*** The Right to Financial Privacy Act (RFPA) limitations described in 18.6.4.3.4 of this section apply. The provisions in ECPA govern, as discussed in 18.6.4.3.4 of this section, if the request for records is addressed to a "provider of electronic communication service" or a "remote computing service." The subpoena may not require the production of records at a place more than 500 miles from the place the subpoena is served.

(U) [redacted] b7E

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

18.6.4.3.3 ***(U) APPROVAL REQUIREMENTS***

18.6.4.3.3.1 **(U) REQUIRED FORM**

A) (U) An administrative subpoena, in accordance with DIOG subsections 18.6.4.3.2.1 and 18.6.4.3.2.2 above, must be prepared and issued using the electronic FD-1035, "Administrative Subpoena" [redacted] The electronic form is designed to ensure an administrative subpoena is: (1) issued only in investigations where its use is permitted; (2) used to demand information that can be obtained within the applicable legal and policy limitations; and (3) approved by an individual with proper authority. The FD-1035 must be electronically placed into the (administrative subpoena) SBP sub-file in the relevant investigative case from which it is issued. An electronic copy of the subpoena will automatically be saved in the FD-1035 data base when it is electronically placed into Sentinel.

B) (U) The [redacted] allows for the generation of an administrative subpoena for any need specified in DIOG subsections 18.6.4.3.2.1 and 18.6.4.3.2.2 above. For administrative subpoenas served to participating providers, it also provides the ability to receive expedited returns, as well as a means to review and ingest the return information into [redacted] for storage, processing, and analysis. b7E

C) (U) An FD-1035 addressed to an electronic communication service provider contains an attachment explaining the meaning of various terms used in the demand for information [redacted] issued by the FBI or proposed by the FBI for issuance by a DOJ attorney without approval from OGC or the CDC. That approval must be documented to the SBP sub-file.

18.6.4.3.3.2 **(U) APPROVAL AUTHORITY**

(U//~~FOUO~~) Use of an administrative subpoena requires SSA approval. The subpoena may be issued by the SSA if that SSA is among those with delegated authority to do so. See DIOG Sections 18.6.4.3.2.1 – 18.6.4.3.2.3 above) Otherwise, the subpoena must be forwarded to an individual with the proper delegated authority. Further review and approval may be required depending on the delegation. Review by the CDC is appropriate if legal questions arise in preparing and issuing the subpoena.

(U//~~FOUO~~) b7E

18.6.4.3.3.3 **(U) REIMBURSEMENT FOR THE PRODUCTION OF TOLL RECORDS**

A) (U//~~FOUO~~) Reimbursement to a telecommunications provider (electronic communications service) for toll, and other records produced, pursuant to the issuance of an administrative subpoena is governed by statutory requirements and exceptions to those provisions.

B) (U//~~FOUO~~) An individual designated by proper authority to issue an administrative subpoena is permitted to sign and issue a "no payment" response letter to a provider upon determination that an invoice received from the telecommunications provider falls within the statutory exceptions to reimbursement. Consultation with, and review of the letter by, the CDC is appropriate if legal questions arise in preparing and issuing the response letter.

18.6.4.3.4 ***(U) LIMITATIONS ON USE OF ADMINISTRATIVE SUBPOENAS***

18.6.4.3.4.1 **(U) FINANCIAL PRIVACY LIMITATIONS**

18.6.4.3.4.1.1 ***(U) OBTAINING RECORDS FROM A FINANCIAL INSTITUTION***

(U//~~FOUO~~) "Financial records" are those records that pertain to a customer's relationship with a financial institution. The term "financial institution" is broadly defined as a bank, savings bank, card issuer, industrial loan company, trust company, savings association, building and loan or homestead association, credit union, or consumer finance institution, located in any state, territory, or the District of Columbia. See 12 U.S.C. § 3401. (*Note:* The scope of the RFPA's definition of financial institution for this purpose, which limits the restrictions the RFPA places on federal law enforcement in using an administrative subpoena, is narrower than the definition of financial institution that is used in connection with NSLs. For that purpose, the RFPA refers to the broader definition found in the Bank Secrecy Act (BSA). Among the entities included in the BSA definition are money transmitting businesses, car dealers, travel agencies, and persons involved in real estate closings. See 12 U.S.C. § 3414(d) and 31 U.S.C. § 5312 (a) (2) and (c) (1).) When seeking financial records from a financial institution, the FBI must send a certificate of compliance required by 12 U.S.C. § 3403 to the financial institution. The certificate must indicate, among other things, that notice has been provided by the FBI to the individual customer whose financial records are to be obtained. The content of the notice is set out in 12 U.S.C. § 3405. A court order may be obtained that allows for delayed notice

pursuant to 12 U.S.C. § 3409. Notice is not required if the administrative subpoena is issued to obtain the financial records of a corporation or for records not pertaining to a customer. Notice is also not required if the administrative subpoena seeks only basic account information, defined as name, address, type of account, and account number. See 12 U.S.C. § 3413(g).

18.6.4.3.4.1.2 *(U) OBTAINING RECORDS FROM A CREDIT BUREAU*

(U//~~FOUO~~) A credit bureau or consumer reporting agency may only provide name, address, former addresses, place of employment and former place of employment in response to an administrative subpoena. See 15 U.S.C. § 1681f. A credit bureau or consumer reporting agency may not release financial information in a credit report or consumer report, or the names and locations of financial institutions at which the consumer has accounts pursuant to an administrative subpoena. A court order, a grand jury subpoena, or, in an appropriate investigation, a national security letter may be used to obtain this information. 15 U.S.C. § 1681b. Notice of disclosure will be provided by the credit bureau or consumer reporting agency to the consumer if the consumer requests this information.

18.6.4.3.4.2 (U) ELECTRONIC COMMUNICATION PRIVACY ACT

(U//~~FOUO~~) The ability to gather subscriber information and the content of electronic communications using an administrative subpoena is governed by ECPA. In investigations involving the sexual exploitation or abuse of children, only basic subscriber or customer information may be obtained with an administrative subpoena under the terms of the Attorney General's delegation, as described above. No content information may be obtained. In drug and health care fraud investigations, an administrative subpoena may be used to obtain basic subscriber or customer information and certain stored communications, under limited circumstances, from entities that provide electronic communication services to the public.

18.6.4.3.4.2.1 *(U) SCOPE*

(U//~~FOUO~~) ECPA applies to two types of entities that provide electronic communications to the public. They are:

A) (U//~~FOUO~~) "Electronic Communication Service" is defined as "any service that provides the user thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15)

B) (U//~~FOUO~~) "Remote Computing Service" is defined as the "provision to the public of computer storage or processing service by means of an electronic communication system." 18 U.S.C. § 2711(12)

18.6.4.3.4.2.2 *(U) SUBSCRIBER INFORMATION*

(U//~~FOUO~~) b7E

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

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

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

b7E

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

E) (U//~~FOUO~~)

F) (U//~~FOUO~~)

(U//~~FOUO~~)

(U//~~FOUO~~)

18.6.4.3.4.2.3 ***(U) SECOND GENERATION CONNECTION RECORDS***

(U//~~FOUO~~)

b7E

18.6.4.3.4.2.4 ***(U) RECORDS OR OTHER INFORMATION PERTAINING TO A SUBSCRIBER***

(U//~~FOUO~~)

b7E

18.6.4.3.4.2.5 ***(U) CONTENT***

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

A) (U) Unopened e-mail held in storage for 180 days or less may not be obtained using an administrative subpoena. A search warrant is required.

B) (U) Unopened e-mail that has been held in electronic storage for more than 180 days may be obtained with an administrative subpoena. (In the Ninth Circuit, the opened e-mail and un-opened e-mail must have been in storage for 180 days before it can be obtained with an administrative subpoena. See Theofel v. Farey-Jones, 359 F.3d 1066.) The government must provide notice to the subscriber or customer prior to obtaining such content. A limited exception to the notice requirement is provided in 18 U.S.C. § 2705.

C) (U) E-mail that has been opened and the content of other electronically stored files held in storage by an entity that provides storage services to the public (i.e., a remote computing service, as defined in 18 U.S.C. § 2711), may be obtained using an administrative subpoena with notice to the customer or subscriber, unless notice is delayed in accordance with 18 U.S.C. § 2705.

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

(U) The FD-1035 is not configured to obtain e-mail content because of developing case law in this area. This information may be obtained using an order issued under 18 U.S.C. § 2703(d). See DIOG Section 18.6.8.3.

18.6.4.3.4.3 (U) MEMBERS OF THE NEWS MEDIA[69]

(U//~~FOUO~~) ***Approval Requirements:*** An administrative subpoena directed to a provider of electronic communication services or any other entity seeking to obtain local and long distance connection records, or records of session times of calls, made by a member of the news media may only be issued with the specific approval of the Attorney General. Before proposing such a subpoena, an agent should review 28 CFR § 50.10. Requests for AG approval must be made by the AUSA involved in the investigation consistent with the DOJ policies set forth in 28 CFR § 50.10. Guidance on the DOJ policy may be obtained from the Investigative Law Unit and/or the Privacy and Civil Liberties Unit, OGC.

(U) 28 CFR § 50.10(b)(1)(ii) provides guidance on categories of individuals and entities not covered under the requirements set out above.

18.6.4.3.5 *(U) COMPLIANCE/MONITORING*

18.6.4.3.5.1 (U) LIMITS ON USE

(U//~~FOUO~~) [redacted] b7E

[redacted]

[69] Note: Due to an administrative error, the version of the DIOG released on September 17, 2021, prematurely included new requirements pertaining to the use of compulsory processes to obtain information from, or records of, members of the news media. As of October 25, 2021, those changes (including some that erroneously appeared on this page) have been reverted to the previous release of the DIOG, dated March 31, 2020. Additional updates about this topic are coming soon. Questions should be directed to CDCs or IPO.

b7E

18.6.4.3.5.2 (U) OVERPRODUCTION

(U//~~FOUO~~) If any of the information that is obtained with an administrative subpoena is subject to statutory privacy protections (e.g., records subject to the Electronic Communications Privacy Act (ECPA), Right to Financial Privacy Act (RFPA), the Fair Credit Reporting Act (FCRA), Health Insurance Portability and Accountability Act (HIPAA), or the Buckley Amendment), it must be reviewed at the time it is received by the employee who requested the issuance of an administrative subpoena to ensure that the information received from the third party provider is within the scope of the request. Any information received from a third party provider that is beyond the scope of the administrative subpoena and is subject to statutory protections must be treated as an overproduction. If it is determined that the overproduced material is subject to statutory protection, then all of the produced material must be sequestered with the employee's supervisor and may not be electronically placed into any FBI database or used in the investigation until one the following methods of disposition have been completed at the discretion of the field office or FBIHQ division that issued the administrative subpoena:

A) (U) The employee redacts the overproduced material. The employee's supervisor must approve the scope of the redaction. If there is any question whether the information provided is within the scope of the administrative subpoena, the CDC or OGC must be consulted. The method of redaction is left to the discretion of the employee, but redacted information must not be visible, used in the investigation, or electronically placed into any FBI database. The method of redaction will vary depending on whether the information was provided in hard copy or electronically. After the overproduced information has been redacted, the remainder of properly produced information may be electronically placed into any database and used in the investigation;

B) (U)

b7E

C) (U) The records are returned to the entity that produced them; or

D) (U) The records are destroyed.

(U) Whichever disposition is selected for the overproduction, it must be documented in the investigative SBP sub-file for administrative subpoenas.

(U) Any questions concerning this process, including the review or disposition of the responsive records, or the statutes which cover such records, should be discussed with the CDC or OGC.

18.6.4.3.5.3 (U) FACTORS FOR COMPLIANCE

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

A) (U//~~FOUO~~) The administrative subpoena must relate to a type of investigation for which the subpoena is authorized;

B) (U//~~FOUO~~) The administrative subpoena must be directed to a recipient to whom an administrative subpoena is authorized;

C) (U//~~FOUO~~) The administrative subpoena may request only records that are authorized under the pertinent law;

D) (U//~~FOUO~~) The administrative subpoena must be approved by an authorized official;

E) (U//~~FOUO~~) The administrative subpoena must be electronically uploaded into the investigation's [redacted] in Sentinel for recordkeeping purposes [redacted] b7E

[redacted]

F) (U//~~FOUO~~) The return of service information must be completed on the back of the original administrative subpoena. Typed signature blocks do not affect current practices for completing the return of service information. For electronically served subpoenas [redacted] satisfies the "return of service" upon the review of [redacted] thus no paper copy is required. For non-electronically served subpoenas, users must complete the [redacted]

process to satisfy the return of service requirement. This copy of the subpoena must be placed in the SBP sub-file or uploaded as a 1A to the case file, following your office practices;

G) (U//~~FOUO~~) The original administrative subpoena and completed return of service must be maintained in a SBP sub-file of the investigation. Provided a copy of the approved subpoena and a copy of the completed return of service are electronically placed to the case file in Sentinel, the SBP sub-file is not mandated. This only applies to those administrative subpoenas which are created through the [redacted] and

H) (U//~~FOUO~~) If the records provided in response to the administrative subpoena are subject to statutory privacy protections, they must be reviewed to ensure that they are within the scope of the request (i.e., that there is no overproduction). If an over-production has occurred, the procedures outlined above must be followed.

18.6.5 *(U) INVESTIGATIVE METHOD: GRAND JURY SUBPOENAS (COMPULSORY PROCESS)*

18.6.5.1 (U) OVERVIEW OF COMPULSORY PROCESS[70]

(U//~~FOUO~~) b7E

18.6.5.2 (U) APPLICATION

(U) An FGJ is an independent panel charged with determining whether there is probable cause to believe one or more persons committed a particular federal offense. The FGJ makes its determination based on evidence presented by the prosecuting attorney in an ex parte proceeding. If the FGJ believes probable cause exists, it will vote to return a "true bill" and the person will be indicted. An indictment is the most typical way a person is charged with a felony in federal court. The FGJ operates under the direction and guidance of the United States District Court. Generally, only witnesses for the prosecution testify before the grand jury.

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

18.6.5.3 (U) LEGAL AUTHORITIES

(U) An FGJ can collect evidence through the use of an FGJ subpoena, which is governed by Rule 6 of the FRCP. FRCP 6(e) controls the release of information obtained as part of the FGJ proceeding. FRCP 6(e) allows federal prosecutors to share foreign intelligence, counterintelligence, and terrorism-related threat information, and it is the DOJ's policy that such information must be shared to the fullest extent permissible by law and in a manner consistent with the rule. See also the Attorney General *Guidelines for the Disclosure and Use of Grand Jury Information under Rule 6(e)(3)(D)* (April 2008) (hereinafter FGJ Guidelines).

b7E

18.6.5.4 **(U) SCOPE**

(U//F~~OUO~~) This policy applies to all FBI employees engaged in a FGJ-related investigation who have access to FGJ information defined as "matters occurring before the grand jury" and are involved in operational activity. This includes FBI personnel such as task force officers (TFOs), task force members (TFMs), and task force participants (TFPs) (see DIOG subsection 3.3.2), and other government agency (OGA) personnel detailed to the FBI. FGJ subpoenas can be used to demand documents, records, testimony of witnesses, or any other evidence deemed relevant by a sitting grand jury. The FBI can request the issuance of an FGJ subpoena in coordination with the responsible USAO in all criminal investigative matters. In Type 1 & 2 Assessments the issuance of an FGJ subpoena for the purpose of obtaining limited subscriber or customer information from providers of electronic communication services or remote computing services (including telephone and electronic mail providers, as set forth in section 18.5.9, may be obtained from the USAO. The USAO must determine whether there is sufficient connection between the Assessment and possible criminal conduct to warrant issuance of an FGJ subpoena. FGJ subpoenas may not be sought during Type 3, 4, 5, or 6 Assessments. An FGJ subpoena may not be used in a positive foreign intelligence investigation. FGJ subpoenas are part of the investigative process. Thus, when an individual is indicted, further FGJ subpoenas may not be issued that are related to those offenses. Additional FGJ subpoenas pertaining to this individual could be issued, however, only for crimes which continue to be investigated and have not yet been indicted. FGJ subpoenas cannot be used to gather evidence for trial; trial subpoenas must be used for that purpose (see Rule 17 FRCP). See DIOG subsection 18.6.5.14 for guidance on the use of a FGJ subpoena in fugitive investigations.

18.6.5.4.1 ***(U) SCOPE OF FGJ POLICY ON ADMINISTRATIVE PERSONNEL***

(U)

b7E

(U//F~~OUO~~) FBI employees who are preparing a response to a Freedom of Information Act or Privacy Act request may properly access FGJ material because they are considered to be assisting the FGJ attorney by ensuring against any improper disclosure.

18.6.5.5 **(U) APPROVAL REQUIREMENTS**

(U) There are no FBI supervisory approval requirements associated with issuing a FGJ subpoena, but all FGJ subpoenas must be issued by the USAO that is handling the [redacted] Assessment or predicated investigation to which the subpoenaed materials or witnesses are relevant. b7E

18.6.5.6 **(U) DURATION OF APPROVAL**

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

18.6.5.7 **(U) MEMBERS OF THE NEWS MEDIA**[71]

(U) ***Approval Requirements:*** A FGJ subpoena directed to a provider of electronic communication services or any other entity seeking to obtain local and long distance connection records, or for records of session times of calls, that were made by a member of the news media may only be issued with the specific approval of the Attorney General. Before proposing such a subpoena, an agent should review 28 CFR § 50.10. Requests for AG approval must be made by the AUSA involved in the investigation consistent with the DOJ policies set forth in 28 CFR § 50.10, and AG Memorandum "Updated Policy Regarding Obtaining Information From, or Records Of, Members of the News Media; and Regarding Questioning, Arresting, or Charging Member of the News Media" (February 2014) and AG Memoranudm "Updated Policy Regarding Obtaining Information From, or Records Of, Members of the News Media; and Regarding Questioning, Arressting, Or Charging Member of the News Media" (January 2015).

(U//~~FOUO~~) [redacted] b7E

[redacted]

(U) 28 CFR § 50.10(b)(1)(ii) provides guidance on categories of individuals and entities not covered under the requirements set out above.

(U) Additional guidance on the DOJ policy may be obtained from the field office CDC, the Investigative Law Unit and the Privacy and Civil Liberties Unit, OGC.

[71] Note: Due to an administrative error, the version of the DIOG released on September 17, 2021, prematurely included new requirements pertaining to the use of compulsory processes to obtain information from, or records of, members of the news media. As of October 25, 2021, those changes (including some that erroneously appeared on this page) have been reverted to the previous release of the DIOG, dated March 31, 2020. Additional updates about this topic are coming soon. Questions should be directed to CDCs or IPO.

18.6.5.8 (U) NOTICE AND REPORTING REQUIREMENTS

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

18.6.5.9 (U) DEFINITION OF MATTERS OCCURRING BEFORE THE GRAND JURY

(U) b7E

18.6.5.9.1 *(U) EXAMPLES OF MATTERS OCCURRING BEFORE THE GRAND JURY*

(U) As a general rule, the following constitute "matters occurring before the grand jury:" (1) the names of targets of the FGJ; (2) witnesses scheduled to be called by the FGJ; (3) the original FGJ subpoenas with any and all attachments; (4) FGJ testimony (including any and all transcripts of such testimony); and (5) documents that reveal the intentions or direction of the b7E

(U)

18.6.5.9.2 *(U) FEDERAL GRAND JURY PHYSICAL EVIDENCE AND STATEMENTS OF WITNESSES*

(U) Physical evidence provided to the government in response to an FGJ subpoena is subject to the secrecy rule regardless of whether such evidence is presented to the grand jury. Physical evidence provided voluntarily or obtained by means other than grand jury process (such as by consent or a search warrant) is not considered a matter occurring before the grand jury regardless of whether such evidence was previously or is thereafter presented to the grand jury. The fact that the physical evidence was presented to the grand jury is, however, subject to the grand jury secrecy rules. For example, a witness voluntarily provides documentation to the agent who later presents the documentation to the grand jury. The fact the material was presented to the grand jury does not cause the documents to be identified as matters occurring before the grand jury; however, since the documents were presented, they may be subject to the grand jury secrecy rules.

(U) Statements of witnesses obtained as a result of grand jury process including FGJ subpoena, such as a statement given in lieu of grand jury testimony, are matters occurring before the grand jury irrespective of whether such witnesses testified before the grand jury or were not required to testify. Voluntary statements of witnesses made outside of the grand jury context (not pursuant to any grand jury process including an FGJ grand jury subpoena), including statements made outside the grand jury by a witness who is being prepared for grand jury testimony, are not matters occurring before the grand jury irrespective of whether the witness previously testified or will thereafter testify before the grand jury.

18.6.5.9.3 *(U) Documents Created Independent of Grand Jury but Obtained by Grand Jury Subpoena*

(U) As described earlier, Rule 6(e) generally prohibits disclosing matters occurring before the FGJ. The rule, however, does not define that phrase. The issue of whether preexisting documents fall within that prohibition has never been settled conclusively by the Supreme Court, although many lower courts have discussed it at length. Courts generally agree that this prohibition does not cover all information developed in the course of an FGJ investigation; rather, the secrecy rule applies only to information that would reveal the existence, strategy, or direction of the FGJ investigation; the nature of the evidence produced before the FGJ; the views expressed by members of the FGJ; or anything else that actually occurred before the FGJ. In addition, many courts have held that Rule 6(e) does not automatically protect third-party documents from disclosure simply because they were subpoenaed by the government. Those courts have focused on whether the disclosure of the subpoenaed documents or their contents may tend to reveal the direction or strategy of the FGJ's investigation. Due to developing law on this issue, FBI personnel must consult with the responsible AUSA to determine how to best handle such documents.

18.6.5.9.4 *(U//~~FOUO~~) Data Extracted from Records Obtained by Grand Jury Subpoena*

(U//~~FOUO~~) Information extracted from business records that were obtained by grand jury subpoena is often used to facilitate investigations. Some of this type of data is, by statute or case law, subject to grand jury secrecy rules. In other investigations, determination of whether data must be considered subject to grand jury secrecy rules depends on the case law and local practice in the federal district. Information extracted from grand jury subpoenaed financial records subject to the Right to Financial Privacy Act of 1978 (12 U.S.C. § 3420) must be treated as matters occurring before a federal grand jury "unless such record has been used in the prosecution of a crime for which the grand jury issued an indictment or presentment or for a purpose authorized by rule 6(e) of the Federal Rules of Criminal Procedure" (emphasis added).

18.6.5.10 (U) Restrictions on Disclosure

(U) As a general rule, no one other than a grand jury witness may disclose matters occurring before the grand jury. Government agents, even if called as witnesses, may not disclose matters occurring before the grand jury. To determine if disclosure is permitted under certain circumstances, or if the disclosure restrictions are not applicable because the materials are not matters occurring before the grand jury, see DIOG subsection 18.6.5.9, above, and relevant subsections of 18.6.5.12 below.

(U//~~FOUO~~) b7E

18.6.5.11 (U) Disclosures by the Government Requiring the Court's Permission

(U//~~FOUO~~) The government, through its attorney, may disclose matters occurring before the grand jury under certain listed conditions and with permission of the court. Petitions to make these disclosures are generally, but not always, filed with the court that impaneled the grand jury. Unless the hearing on the government's petition is an ex parte hearing, the petition must be served on all parties to the proceeding and the parties must be afforded a reasonable period of time to respond.

A) (U) An attorney for the government may petition for disclosure to a foreign court or prosecutor for use in an official criminal investigation.

B) (U) An attorney for the government may petition for disclosure to a state, local, tribal, or foreign government official, if the government attorney can show that the matter may disclose a violation of state, tribal, or foreign criminal law, and the purpose of the disclosure is to enforce that law.

C) (U) An attorney for the government may petition for disclosure to an appropriate military official if the government attorney can show the matter may disclose a violation of military criminal law under the Uniform Code of Military Justice, and the purpose of the disclosure is to enforce that law.

18.6.5.11.1 *(U) Disclosures by the Government Not Requiring the Court's Permission*

(U//~~FOUO~~) The government, through its attorney, may disclose matters occurring before the grand jury without prior permission of the court under the following conditions:

A) (U) Under Rule 6(e)(3)(A), the government may disclose matters occurring before the federal grand jury to certain persons in certain situations provided the government does not disclose the grand jury's deliberations or any grand juror's vote and the government provides the court that impaneled the grand jury with the names of all persons to whom disclosure was made and certifies that the government has advised the receiving party of the obligation of secrecy under this rule, as set forth below in B - D.

B) (U) Also under Rule 6(e)(3)(A), persons eligible to receive matters occurring before the grand jury under this subsection are: 1) an attorney for the government for use in performing that attorney's duty; 2) any government personnel, including state, local,

[72] (U//~~FOUO~~) b7E

tribal, or foreign government personnel that an attorney for the government considers necessary to assist in performing that attorney's duty to enforce federal law; and 3) a person authorized under 18 U.S.C. § 3322.

C) (U) For Rule 6(e)(3)(A) purposes, OGC attorneys and CDCs are not "attorneys for the government." For purposes of the FRCP, it defines "attorney for the government" as "the Attorney General, an authorized assistant of the Attorney General, a United States Attorney, [and] an authorized assistant of the United States Attorney."

D) (U) Rule 6(e)(3)(B) authorizes grand jury material to be used "to assist an attorney for the government in performing that attorney's duty to enforce federal criminal law." With the approval of the USAO, information from subpoenaed telephone records may be disclosed for use in unrelated federal criminal investigations in those districts where such material is not considered a matter occurring before a grand jury. If the USAO approves generally of this procedure, such information may be used in unrelated criminal investigations without authorization from a government attorney in each instance.

E) (U) Under Rule 6(e)(3)(c), an attorney for the government may disclose any matter occurring before the grand jury to another federal grand jury.

18.6.5.11.2 *(U) RULE 6(E) EXCEPTIONS PERMITTING DISCLOSURE OF FGJ MATERIAL*

(U) Rule 6(e) allows certain exceptions permitting disclosure of matters occurring before the grand jury, which are discussed in the following sections. Rule 6(e)(3)(B) requires a federal prosecutor who discloses grand jury material to government investigators and other persons supporting the grand jury investigation to promptly provide the court that impaneled the grand jury the names of the persons to whom such disclosure has been made and to certify that he/she has advised such persons of their obligation of secrecy under the Rule. In order to document the certification required by the Rule, government attorneys often execute and deliver to the court a form, normally referred to as a "Certification" or "Rule 6(e) letter." A copy of this document must be maintained with the grand jury material held in the FBI's custody. The list of individuals authorized to access matters occurring before the grand jury, referred to as the "6(e) list," is drawn from the Rule 6(e) letter. See also DIOG subsection 18.6.5.4.1 above for Rule 6(e) exceptions involving administrative personnel.

18.6.5.11.3 *(U) RULE 6(E)(3)(D) DISCLOSURE EXCEPTION FOR INTELLIGENCE OR NATIONAL SECURITY PURPOSES*

(U) An attorney for the government may disclose any matter occurring before the grand jury involving foreign intelligence, counterintelligence, or foreign intelligence information to any federal law enforcement, intelligence, protective, immigration, national defense, or national security official to assist the official receiving the information in the performance of that official's duties. The government attorney must file, under seal, with the court that impaneled the grand jury, a notice that such information was disclosed and the agencies or departments that received the information. As used in Rule 6(e), foreign intelligence information is information that relates to the ability of the United States to protect against actual or potential attack or grave hostile acts by a foreign power or its agents; sabotage or international terrorism by a foreign power or its agents or clandestine intelligence activities by an intelligence service or network of a foreign power or its agents; or information with respect to a foreign power or foreign territory that relates to the national defense or security of the

United States or the United States conduct of foreign affairs. An attorney for the government may disclose any grand jury matter involving, either in the United States or elsewhere, a threat of attack or other grave hostile acts of a foreign power or its agent, a threat of domestic or international sabotage, or clandestine intelligence gathering activities by an intelligence service or network of a foreign power or by its agent to any appropriate federal, state, local, tribal, or foreign government official for the purpose of preventing or responding to such threat or activities.

(U//FOUO) FRCP 6(e)(3)(D) allows federal prosecutors to share foreign intelligence, counterintelligence, and terrorism-related threat information, and it is the DOJ's policy that such information must be shared to the fullest extent permissible by law and in a manner consistent with the rule. The Attorney General has issued FGJ practice guidelines for USAOs, and the FGJ Guidelines provides amplifying guidance.

18.6.5.11.4 *(U) FBI'S CONDUIT RULE*

(U//~~FOUO)~~ Only the federal prosecutor is authorized to make an initial disclosure of Rule 6(e)(3)(D) foreign intelligence information. As a practical matter, such disclosures are ordinarily accomplished through the FBI, which may have existing information-sharing mechanisms with authorized receiving officials. If the prosecutor intends to share information directly with another official, consultation with the FBI is required to ensure that disclosures will be consistent with the existing policy of intelligence community agencies and to ensure appropriate handling of sensitive or classified information [redacted] b7E

[redacted]

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

18.6.5.11.5 *(U) OTHER STATUTORY DISCLOSURE RESTRICTIONS NOT AFFECTED*

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

18.6.5.11.6 *(U) RULE 6(E)(3)(D) RECEIVING OFFICIAL RULES AND RESTRICTIONS*

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

B) (U//~~FOUO~~) If dissemination is necessary to the performance of his or her official duties, a receiving official may disseminate Rule 6(e)(3)(D) information outside of that official's agency to other government officials.

C) (U) A receiving official, other than a foreign government official, must consult with the attorney for the government before disseminating Rule 6(e)(3)(D) information publicly (including through its use in a court proceeding that is open to or accessible to the public), unless prior dissemination is necessary to prevent harm to life or property. In such instances, the receiving official must notify the attorney for the government of the dissemination as soon as practicable.

D) (U) A foreign government receiving official must obtain prior consent from the disclosing official where possible, or if the disclosing official is unavailable, from the agency that disseminated the information to that foreign official before dissemination of the information to a third government or publicly. Public dissemination includes using the information in a court proceeding that is open to or accessible by the public.

E) (U) A receiving official must take appropriate measures to restrict access to this information to individuals who require access for the performance of official duties.

F) (U) A receiving official must immediately report to the disclosing attorney for the government: any unauthorized dissemination of Rule 6(e)(3)(D) information; or any loss, compromise, or suspected compromise of Rule 6(e)(3)(D) information.

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

H) (U//F~~OUO~~) The FGJ Guidelines do not require the receiving official to notify the federal prosecutor of subsequent disclosures, except for consultation concerning public disclosures and consent for certain disclosures by foreign officials. The receiving official is bound by whatever restrictions govern his or her use and disclosure of the information as part of his official duties. Of note, per Rule 6(e)(3)(D)(ii), if the FBI is included in the initial 6(e)(3)(D) letter as an entity receiving disclosure, subsequent dissemination by the FBI is permitted and no additional permission or notification to the court is required. (The FGJ Guidelines provides additional guidance.)

18.6.5.11.6.1 (U//~~FOUO~~) DOCUMENTATION OF INTERNAL DISCLOSURE OF GRAND JURY MATERIAL

(U) Grand jury material must be kept in such as fashion as to maintain the integrity of the material. Upon taking custody of grand jury material, the FBI employee must categorize it in a manner to identify its production source and how it was obtained, to include the identity of a custodian of record for documentary evidence. In lieu of a Rule 6(e) letter from the USAO containing an exhaustive list of names of FBI personnel, an FBI record of additional internal disclosures must be maintained by the case agent in order to establish accountability. Use of this "internal certification" procedure must be authorized by the appropriate USAO. The internal certification document (e.g. EC) must record the date of disclosure as well as the identity and position of the recipient. Such internal disclosures may be made only in support of the same investigation in which a federal

prosecutor has previously issued a Rule 6(e) letter. In addition, the internal certification document must reflect that all recipients of matters occurring before the grand jury were advised of the secrecy requirements of Rule 6(e). Whenever practicable, recipients must be listed on this internal certification prior to disclosure. Local Rule 6(e) customs must govern the internal certification process used. See also DIOG subsection 18.6.5.4.1 above for Rule 6(e) exceptions involving administrative personnel.

18.6.5.11.7 ***(U) VIOLATIONS***

A) (U) A receiving official who knowingly violates Rule 6(e)(3)(D) by using the disclosed information outside the conduct of his or her official duties, or by failing to adhere to any limitations on the dissemination of such information, may be subject to contempt of court proceedings and to restriction on future receipt of Rule 6(e)(3)(D) information.

B) (U) A state, local, tribal, or foreign government official who receives Rule 6(e)(3)(D) information, and who knowingly violates these guidelines, may be subject to contempt of court proceedings.

C) (U) An attorney for the government who knowingly violates Rule 6(e)(3)(D) may be subject to contempt of court proceedings.

18.6.5.12 **(U) LIMITATION OF USE**

A) (U) Rule 6(e)(3)(D) does not require notice to the court of subsequent dissemination of the information by receiving officials.

B) (U//F~~OUO~~) Disclosure of material considered matters occurring before the grand jury cannot be made within the FBI for unrelated investigations unless a government attorney has determined that such disclosure to a particular investigator is needed to assist that attorney in a specific criminal investigation. The ability of government attorneys to freely share grand jury material with other government attorneys for related or unrelated criminal investigations does not extend to investigators without investigation specific authorization from the government attorney and notice to the court. Therefore, [redacted] b7E

[redacted]

C) (U//F~~OUO~~) If a government attorney authorizes the disclosure of material considered matters occurring before the grand jury in the possession of the FBI for use in an unrelated federal criminal matter, such approval must be documented in the "GJ" sub-file of both the initiated investigation file and the subsequent investigation file. That documentation will be in addition to any necessary supplementation to the government attorney's Rule 6(e) disclosure letter and/or to the internal certification disclosure list.

D) (U//F~~OUO~~) The USAO must be consulted immediately for precautionary instructions if material considered matters occurring before the grand jury will have application to civil law enforcement functions (e.g., civil RICO or civil forfeiture). There are very limited exceptions that allow government attorneys to use grand jury material or information in civil matters (e.g., civil penalty proceedings concerning banking law violations). These exceptions do not automatically apply to investigative personnel. Therefore, any similar use of FGJ information by the FBI must be approved in advance by the government attorney.

E) (U//~~FOUO~~) Disclosure cannot be made without a court order for use in non-criminal investigations, such as background investigations or name checks.

F) (U//~~FOUO~~) Government personnel who are preparing a response to a Freedom of Information Act or Privacy Act request may properly access grand jury material under the Rule because they are considered to be assisting the grand jury attorney by ensuring against any improper disclosure.

G) (U) Rule 6(e)(3)(B) requires a federal prosecutor who discloses material considered matters occurring before the grand jury to government investigators and other persons supporting the grand jury investigation to promptly provide the court that impaneled the grand jury the names of the persons to whom such disclosure has been made and to certify that he/she has advised such persons of their obligation of secrecy under the Rule. In order to document the certification required by the Rule, government attorneys often execute and deliver to the court a form, normally referred to as a "Certification" or "Rule 6(e) letter." A copy of this document must be maintained with the grand jury material held in the FBI's custody.

18.6.5.13 (U//~~FOUO~~) MARKING, PHYSICAL STORAGE, AND MAILING OF GRAND JURY MATERIAL

(U//~~FOUO~~) The FBI cannot make or allow unauthorized disclosure of matters occurring before the grand jury. If material and records obtained pursuant to the FGJ process are stored in FBI space, [redacted] b7E

[redacted]

process are frequently stored in FBI space, FBI employees must report any unauthorized disclosure to the appropriate government attorney who, in turn, must notify the court. In order to protect against unauthorized disclosure, grand jury material must be secured in the following manner:

1) (U//~~FOUO~~) The page cover, envelope, or container holding grand jury materials or records that have been identified as a "matter occurring before a grand jury" must be marked with the warning: "MATTERS OCCURING BEFORE THE FEDERAL GRAND JURY - DISSEMINATE ONLY PURSUANT TO RULE 6(e)." No grand jury stamp or mark should be affixed to the original material. Agents, analysts and other authorized parties should work from copies of such FGJ material whenever possible to ensure the original material retains its integrity [redacted] b7E

[redacted]

2) (U//~~FOUO~~) Access to [redacted] must be limited to authorized persons (e.g., those assisting an attorney for the government in a specific criminal investigation). All necessary precautions must be taken to protect

[redacted] to include maintaining the material in a secure location when not in use. The material must be appropriately [redacted] in Guardian or another FBI system. [redacted] is entered into a computer database, the data must be marked with the 6(e) warning and [redacted] restricted within the system. b7E

3) (U//~~FOUO~~) Registered mail or other traceable courier (such as Federal Express) approved by the Chief Security Officer (CSO) must be used to mail or transmit to other field offices any documents containing grand jury material. Couriers and other personnel employed in these services will not be aware of the contents of the material transmitted because of the wrapping procedures specified below, and therefore, do not require a background investigation for this purpose. The names of persons who transport the material need not be placed on a 6(e) disclosure list.

4) (U//~~FOUO~~) Material considered matters occurring before the grand jury that is to be mailed or transmitted by traceable courier outside a facility must be enclosed in opaque inner and outer covers. The inner cover must be a sealed wrapper or envelope that contains the addresses of the sender and the addressee, who must be authorized to have access to the grand jury material. The inner cover must be conspicuously marked "Grand Jury Information To Be Opened By Addressee Only." The outer cover must be sealed, addressed, return addressed, and bear no indication that the envelope contains grand jury material. When the size, weight, or nature of the grand jury material precludes the use of envelopes or standard packaging, the material used for packaging or covering must be of sufficient strength and durability to protect the information from unauthorized disclosure or accidental exposure.

5) (U//~~FOUO~~) If the government attorney determines that the sensitivity of, or threats to, such grand jury material necessitates a more secure transmission method, the material may be transmitted by an express mail service approved for the transmission of national security information or be hand carried by the assigned government attorney or his or her designated representative.

6) (U//~~FOUO~~) Material considered matters occurring before the grand jury containing classified national security information must be handled, processed, and stored according to 28 CFR Part 17. Such FGJ material containing other types of sensitive information, such as federal tax return information, witness security information, and other types of highly sensitive information that have more stringent security requirements than that usually required for matters occurring before the grand jury must be stored and protected pursuant to the security regulations governing such information and any special dissemination requirements provided by the organization that originated the information.

18.6.5.13.1 *(U//~~FOUO~~) PHYSICAL STORAGE OF FGJ MATERIAL*

(U//~~FOUO~~) [redacted] b7E

[redacted]

[redacted]

b7E

(U//F~~OUO~~)

(U//F~~OUO~~)

b7E

(U//F~~OUO~~)

(U//F~~OUO~~)

b7E

(U//F~~OUO~~)

(U//F~~OUO~~)

b7E

18.6.5.13.2 ***(U//~~FOUO~~) ELECTRONIC STORAGE OF FGJ MATERIAL***

(U//~~FOUO~~) If information identified as matters occurring before the grand jury is entered into a computer database, the data must be marked with the 6(e) warning and access must be restricted within the system

18.6.5.13.3 ***(U//~~FOUO~~) HANDLING AND STORAGE OF FGJ MATERIAL AFTER THE CLOSURE OF A CASE***

(U)

(U//~~FOUO~~)

b7E

(U//~~FOUO~~)

(U//~~FOUO~~)

18.6.5.13.4 ***(U//F~~OUO~~) DELETION OF ELECTRONICALLY STORED MATERIAL IDENTIFIED AS MATTERS OCCURRING BEFORE THE GRAND JURY***

(U//F~~OUO~~)

b7E

(U//F~~OUO~~)

18.6.5.13.5 ***(U//FOUO) FGJ MATERIAL CONTAINING CLASSIFIED OR OTHER SENSITIVE INFORMATION***

(U//F~~OUO~~)

b7E

18.6.5.14 **(U) REQUESTS FOR FGJ SUBPOENAS IN FUGITIVE INVESTIGATIONS**

(U//F~~OUO~~) The function of the grand jury is to decide whether a person should be charged with a federal crime. Locating a person who has been charged is a task that is ancillary to, rather than a part of, that function. As such, grand jury subpoenas cannot be used as an investigative aid in the search for a fugitive in whose testimony the grand jury has no interest. Absent one of the exceptions discussed below being applicable, grand jury subpoenas for testimony or records related to a fugitive's whereabouts may not be requested in FBI fugitive investigations.

(U//F~~OUO~~) If the grand jury has a legitimate interest in the testimony of a fugitive regarding another federal ongoing investigation, it may subpoena other witnesses and records in an

effort to locate the fugitive. In this situation, the responsible Assistant Attorney General must approve a "target" subpoena for the fugitive before the grand jury may subpoena witnesses and records to locate the fugitive.

(U//~~FOUO~~) When a fugitive's present location is relevant to an offense under investigation, the grand jury may legitimately inquire as to the fugitive's whereabouts. Offenses such as harboring, misprision of a felony, and accessory after the fact are examples of crimes as to which the fugitive's location may be relevant evidence. If, however, the person who is suspected of harboring the fugitive or being an accessory after the fact has been immunized and compelled to testify regarding the location of the fugitive, this will likely be viewed as improper subterfuge.

(U//F~~OUO~~) DOJ policy generally forbids the use of grand jury subpoenas to locate a defendant charged in a federal criminal complaint with unlawful flight to avoid prosecution (UFAP). UFAP investigations are, as a general rule, not prosecuted. Use of the grand jury in the investigation of a UFAP matter requires prior consultation with DOJ and written authorization to prosecute from the Assistant Attorney General in charge of the Criminal Division. Federal indictments for UFAP require prior written approval of the Attorney General, Deputy Attorney General, or an Assistant Attorney General.

18.6.5.15 (U) FGJ OVERPRODUCTION

(U) If any of the information received in response to an FGJ subpoena is subject to statutory privacy protections (e.g., records subject to the Electronic Communications Privacy Act (ECPA), Right to Financial Privacy Act (RFPA), the Fair Credit Reporting Act (FCRA), Health Insurance Portability and Accountability Act (HIPAA), or the Buckley Amendment), it must be reviewed at the time it is received by the employee who requested the issuance of the FGJ subpoena to ensure that the information received is within the scope of the subpoena's demand. Any information received from a third party provider that is beyond the scope of the FGJ subpoena and is subject to statutory protections must be treated as an overproduction. Overproduced material must not be electronically placed into any FBI application, database or used in any manner. Instead, the FBI employee must promptly notify the AUSA who authorized the issuance of the FGJ subpoena of the potential overproduction. The AUSA, in coordination with the FBI employee, must determine whether the information exceeds the scope of the FGJ subpoena, and if so, how to dispose of the overproduced material. The method of disposition for the overproduction must be documented in the investigation's GJ sub-file.

18.6.5.16 (U) FGJ MATERIAL COMPLIANCE AND MONITORING

(U//F~~OUO~~) [redacted] every field office must designate [redacted] to be responsible for overseeing the FBI's compliance on handling, storage and labeling of FGJ material meeting the definition of matters occurring before the federal grand jury. As part of these duties, the designee must review the field office practices for handling, storage and labeling such material at least once per fiscal year. This review must encompass the policy standards set out in this section and along with any local "standing" judicial requirements. The results of the review(s) must be reported to the field office Division Compliance Council (DCC), and through the DCC, to the Office of Integrity and Compliance using file number 380D-HQ-A3616616-(field office designator). The field office may set its own unique

b7E

inaugural fiscal year review date and use that date thereafter as its basis for the annual review period.

(U//~~FOUO~~) All field office specific local "standing" judicial guidance must be made available to employees assigned to that office.

This Page is Intentionally Blank.

18.6.6 *(U) INVESTIGATIVE METHOD: NATIONAL SECURITY LETTER (COMPULSORY PROCESS)*

18.6.6.1 (U) OVERVIEW OF COMPULSORY PROCESS

(U//~~FOUO~~) [redacted] b7E

[redacted]

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

[redacted]

18.6.6.2 (U) APPLICATION

(U//F~~OUO~~) NSLs may be used in a national security predicated investigation. This method may not be used for assistance to other government agencies, unless the information sought is relevant to an open FBI predicated investigation.

18.6.6.3 (U) NATIONAL SECURITY LETTERS

18.6.6.3.1 *(U) LEGAL AUTHORITY*

A) (U) 12 U.S.C. § 3414(a)(5)(A);

B) (U) 15 U.S.C. §§ 1681u and 1681v;

C) (U) 18 U.S.C. § 2709;

D) (U) 50 U.S.C. § 3162;

E) (U) AGG-Dom, Part V; and

F) (U) An NSL may be used only to request:

1) (U) Financial Records: The *Right to Financial Privacy Act (RFPA)*, 12 U.S.C. § 3414(a)(5);

2) (U) Identity of Financial Institutions: *Fair Credit Reporting Act (FCRA)*, 15 U.S.C. § 1681u(a);

3) (U) Consumer Identifying Information: FCRA, 15 U.S.C. § 1681u(b);

4) (U) Full Credit Reports in International Terrorism Investigations: FCRA, 15 U.S.C. § 1681v; and

5) (U) Telephone Subscriber Information, Toll Billing Records, Electronic Communication Subscriber Information, and Electronic Communication

Transactional Records: *Electronic Communications Privacy Act (ECPA)*, 18 U.S.C. § 2709.

18.6.6.3.2 ***(U) DEFINITION OF METHOD***

(U) An NSL is an administrative demand for documents or records that are relevant to a predicated investigation to protect against international terrorism or clandestine intelligence activities [redacted] b7E

18.6.6.3.3 ***(U) REVIEW AND APPROVAL REQUIREMENTS***

(U//~~FOUO~~) Those who review and approve NSLs are responsible for ensuring that all NSL investigative and procedural requirements have been met. The reviewers must ensure and the approver (an SAC, an ADIC, or a higher-ranking official) must certify that the information sought by the NSL is relevant to an open, predicated national security investigation. For an NSL to include a nondisclosure provision, the approver must determine that disclosure of the NSL "may result in– (i) a danger to the national security of the United States; (ii) interference with a criminal, counterterrorism, or counterintelligence investigation; (iii) interference with diplomatic relations; or (iv) danger to the life or physical safety of any person." 18 U.S.C. § 2709(c)(1)(B), 15 U.S.C. § 1681v(c)(1)(B), and 12 U.S.C. § 3414(c)(1)(B). Those who review or approve NSLs and those designated as acting officials who review or approve NSLs must have completed the Virtual Academy course on NSLs, reviewed DIOG subsection 18.6.6 ("National Security Letter").

(U//~~FOUO~~) The process for creating an NSL involves two documents: the NSL itself and the EC approving the issuance of the NSL. The Director has delegated the authority to sign NSLs to the DD; the NSB EAD and Associate EAD; the ADs and all DADs for the Counterterrorism, Counterintelligence, and Cyber Divisions and the Weapons of Mass Destruction Directorate; the GC and the deputy GC for the NSCLB; the ADICs in the New York, Washington, and Los Angeles Field Offices; and the SACs in all remaining field offices. See EC 333-HQ-A1487720 serial 515 (May 15, 2012). No other *delegations* are permitted. [redacted] b7E

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

(U//~~FOUO~~) In addition to being signed by an SAC, the statutorily required approver, an NSL must be reviewed by a CDC, an ADC, an attorney acting as a CDC or as an ADC, or an NSCLB attorney.

18.6.6.3.4 ***(U) STANDARDS FOR ISSUING NSLS***

(U//~~FOUO~~)

b7E

(U//~~FOUO~~)

(U//~~FOUO~~)

b7E

(U//~~FOUO~~)

b7E

(U//~~FOUO~~)

b7E

18.6.6.3.5 ***(U) SPECIAL PROCEDURES FOR REQUESTING COMMUNICATION SUBSCRIBER INFORMATION***

(U//~~FOUO~~)

(U//~~FOUO~~)

b7E

(U//~~FOUO~~) the employee should consider whether an NSL is the least intrusive and reasonable means based upon the circumstances of the investigation to obtain the information

18.6.6.3.6 ***(U) DURATION OF APPROVAL***

(U//~~FOUO~~)

18.6.6.3.7 ***(U) SPECIFIC PROCEDURES FOR CREATING NSLS***

(U//~~FOUO~~)

b7E

(U//~~FOUO~~)

(U//~~FOUO~~)

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

b7E

B) (U//F~~OUO~~)

C) (U//F~~OUO~~) b7E

D) (U//F~~OUO~~)

b7E

E) (U//F~~OUO~~)

F) (U//F~~OUO~~)

b7E

G) (U//F~~OUO~~)

(U//~~FOUO~~)

b7E

(U//~~FOUO~~)

(U//~~FOUO~~)

(U//~~FOUO~~)

18.6.6.3.7.1 **(U) COVER EC APPROVING AN NSL**

(U//~~FOUO~~)

(U//~~FOUO~~)

b7E

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

b7E

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

b7E

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

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

E) (U//~~FOUO~~)

b7E

F) (U//~~FOUO~~)

G) (U//~~FOUO~~)

b7E

H) (U//~~FOUO~~)

I) (U//~~FOUO~~)

b7E

J) (U//~~FOUO~~)

K) (U//~~FOUO~~)

(U//~~FOUO~~) When a national security investigation reaches its three-year anniversary or when the investigation closes, all NSLs issued in the investigation must be reviewed to determine if any nondisclosure provision(s) should be continued or terminated. Subsection 18.6.6.3.17 discusses, in detail, the review of NSL nondisclosure provisions.

b7E

18.6.6.3.7.2 **(U) COPY OF THE NSL AND RELATED DOCUMENTS IN THE INVESTIGATIVE FILE**

(U//~~FOUO~~)

b7E

(U//~~FOUO~~)

b7E

(U//~~FOUO~~)

18.6.6.3.7.3 **(U) COMMUNITY OF INTEREST INFORMATION**

(U//~~FOUO~~)

b7E

18.6.6.3.7.4 **(U) CONTACT WITH MEMBERS OF THE NEWS MEDIA BY A** [redacted] b7E

[redacted]

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

[redacted]

18.6.6.3.8 **(U) NOTICE AND REPORTING REQUIREMENTS**

(U//~~FOUO~~) NSCLB compiles NSL statistics for reporting to Congress. The NSL subsystem [redacted] (or successor system) automatically records the information needed for Congressional reporting. If the NSL is created outside the subsystem, then the NSL's cover EC must include the information necessary for NSCLB to report NSL statistics accurately, i.e., delineate the number of targeted facilities/accounts in each NSL issued to an NSL recipient. b7E

(U//~~FOUO~~) NSCLB also reports to Congress the USPER status of the target (as opposed to the subject of the investigation) of all NSLs, other than NSLs that seek only subscriber information. While the subject of the investigation is often the target of the NSL, that is not always the case. The EC must record the USPER status of the target of the NSL – the person whose information the FBI is seeking. If the NSL is seeking information about more than one person, the EC must record the USPER status of each person.

18.6.6.3.9 **(U) RECEIPT OF NSL INFORMATION, REVIEW FOR OVERPRODUCTION, AND RELEASING THE INFORMATION**

(U//~~FOUO~~) [redacted] b7E

[redacted]

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

[redacted]

[74] Note: Due to an administrative error, the version of the DIOG released on September 17, 2021, prematurely included new requirements pertaining to the use of compulsory processes to obtain information from, or records of, members of the news media. As of October 25, 2021, those changes (including some that erroneously appeared on this page) have been reverted to the previous release of the DIOG, dated March 31, 2020. Additional updates about this topic are coming soon. Questions should be directed to CDCs or IPO.

(U//F~~OUO~~)

b7E

(U//F~~OUO~~)

(U//F~~OUO~~)

18.6.6.3.10 **(U) OVERPRODUCTION**

(U//~~FOUO~~)

(U//F~~OUO~~)

b7E

(U//~~FOUO~~)

(U//~~FOUO~~)

(U//~~FOUO~~)

b7E

(U//~~FOUO~~)

(U//~~FOUO~~)

18.6.6.3.11 **(U) RETENTION OF NSL INFORMATION**

(U//~~FOUO~~)

b7E

(U//~~FOUO~~)

(U//~~FOUO~~)

b7E

18.6.6.3.12 **(U) SERVICE AND RETURNS OF NSLS**

(U//~~FOUO~~)

b7E

18.6.6.3.12.1 **(U//~~FOUO~~) ELECTRONIC SERVICE AND RETURN**

(U//~~FOUO~~)

b7E

(U//~~FOUO~~)

(U//~~FOUO~~)

b7E

(U//~~FOUO~~)

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

B) (U//~~FOUO~~ b7E

(U//~~FOUO~~

(U//~~FOUO~~

18.6.6.3.12.2 **(U//~~FOUO~~) PERSONAL SERVICE AND RETURN**

(U//~~FOUO~~ b7E

18.6.6.3.12.3 **(U//~~FOUO~~) RESTRICTED MAIL SERVICE AND RETURN**

(U//~~FOUO~~

18.6.6.3.12.4 **(U//~~FOUO~~) FAX SERVICE AND RETURN**

(U//~~FOUO~~ b7E

A) (U//~~FOUO~~

B) (U//~~FOUO~~

C) (U//~~FOUO~~

D) (U//~~FOUO~~) b7E

(U//~~FOUO~~)

18.6.6.3.12.5 **(U//~~FOUO~~) COMBINATION SERVICE AND RETURN**

(U//~~FOUO~~) b7E

18.6.6.3.13 ***(U) DISSEMINATION OF NSL INFORMATION***

(U//~~FOUO~~) Subject to certain statutory limitations, information obtained in response to an NSL may be disseminated according to general dissemination standards in the AGG-Dom. The Electronic Communications Privacy Act (ECPA) (telephone and electronic communications transactional records) and the Right to Financial Privacy Act (RFPA) (financial records) permit dissemination if consistent with the AGG-Dom and the information is clearly relevant to the responsibilities of the recipient agency. The Fair Credit Reporting Act (FCRA) permits dissemination of the identity of financial institutions and consumer identifying information to other federal agencies as may be necessary for the approval or conduct of a foreign counterintelligence investigation. FCRA imposes no special rules for dissemination of full credit reports.

(U//~~FOUO~~) neither the NSL nor the return information is classified. b7E

18.6.6.3.14 ***(U) SPECIAL PROCEDURES FOR HANDLING RIGHT TO FINANCIAL PRIVACY ACT INFORMATION AND OTHER INFORMATION***

(U//~~FOUO~~) b7E

[redacted] b7E

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

[redacted]

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

[redacted] b7E

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

[redacted]

(U//~~FOUO~~ [redacted]

[redacted]

18.6.6.3.15 ***(U) PAYMENT FOR NSL-DERIVED INFORMATION***

(U//~~FOUO~~) No legal obligation exists for the FBI to compensate recipients of NSLs issued pursuant to ECPA (telephone and electronic communications transactional records) or FCRA, 15 U.S.C. § 1681v (full credit reports in international terrorism investigations), and therefore no payment should be made in connection with those NSLs. See [redacted] b7E for a form letter to be sent in response to demands for payment concerning these NSLs.

(U//~~FOUO~~) Compensation for responding to NSLs issued pursuant to RFPA (financial records) and FCRA § 1681u (identity of financial institutions and consumer identifying information) is covered by a fee schedule adopted under *DOJ's Cost Reimbursement Guidance under the ECPA*.

18.6.6.3.16 *(U) JUDICIAL REVIEW OF NSLS*

(U//~~FOUO~~) All NSLs must include the necessary legal notices. Specifically, an NSL issued by the FBI must inform the recipient of the right to judicial review of the NSL pursuant to 18 U.S.C. § 3511(a). See *Doe v. Mukasey*, 549 F.3d 861 (2d Cir. 2008). An NSL issued by the FBI must also inform the recipient of the right to judicial review of any nondisclosure requirement imposed in connection with the NSL (e.g., 18 U.S.C. § 2709(d)). An NSL must specifically advise that if the recipient wishes to have a court review a nondisclosure requirement imposed in connection with an NSL, the recipient may notify the government, which must then initiate judicial review proceedings [redacted] if it wants to maintain nondisclosure of the NSL. If the FBI determines that nondisclosure continues to be necessary (see below paragraph for statutory standard for nondisclosure), the government must demonstrate to a federal judge the need for continued nondisclosure and obtain a judicial order requiring such nondisclosure. The nondisclosure requirement will remain in effect unless and until there is a final court order holding that disclosure is permitted. b7E

(U//~~FOUO~~) In any judicial review proceeding regarding a nondisclosure requirement in connection with an NSL, the government will bear the burden of persuading the district court that there is good reason to believe that disclosure may result in at least one of the enumerated harms set forth in the NSL statutes (e.g., 18 U.S.C. § 2709(c)), which are: a danger to the national security of the United States; interference with a criminal, counterterrorism, or counterintelligence investigation; interference with diplomatic relations; or danger to the life or physical safety of any person who is related to an authorized investigation to protect against international terrorism or clandestine intelligence activities. Accordingly, the field office or FBIHQ division that issued the NSL, in conjunction with OGC, must coordinate with DOJ and the United States Attorney's Office to ensure that the government's certification is sufficient to meet the government's burden of proof.

18.6.6.3.17 *(U) REVIEW OF NONDISCLOSURE REQUIREMENT IN NSLS*

(U//~~FOUO~~) The USA FREEDOM Act of 2015 requires the FBI, pursuant to procedures adopted by the Attorney General (AG), to review, at certain intervals, all NSLs that included a nondisclosure provision. Pursuant to the *Attorney General Termination Procedures for National Security Letter Nondisclosure Requirement (Procedures),* issued November 24, 2015, the review is to determine whether the nondisclosure requirement of an NSL should continue or be terminated. Under these *Procedures,* the nondisclosure requirement of an NSL shall terminate upon the closing of any investigation in which an NSL containing a nondisclosure provision was issued except where the FBI determines that the absence of a nondisclosure requirement "may result in– (i) a danger to the national security of the United States; (ii) interference with a criminal, counterterrorism, or counterintelligence investigation; (iii) interference with diplomatic relations; or (iv) danger to the life or physical safety of any person." 18 U.S.C. § 2709(c)(1)(B), 15 U.S.C. § 1681v(c)(1)(B), and 12 U.S.C. § 3414(c)(1)(B). Pursuant to the *Procedures,* when (i) an open investigative file reaches its third-year anniversary (i.e., three years from the Sentinel case opening date) or (ii) an

investigative file has been closed, an NSL nondisclosure review must be conducted. If an investigation is closed before its three-year anniversary, then the NSL nondisclosure review will be conducted once, when the investigation closes. No NSL nondisclosure reviews are required beyond the three-year anniversary and/or once the investigative file has been closed.

(U//F~~OUO~~)

b7E

(U//F~~OUO~~)

b7E

(U//F~~OUO~~)

This Page Is Intentionally Blank.

18.6.7 *(U) INVESTIGATIVE METHOD: FISA ORDER FOR BUSINESS RECORDS (COMPULSORY PROCESS)*

18.6.7.1 (U) OVERVIEW OF COMPULSORY PROCESS

(U//~~FOUO~~)

b7E

(U)

18.6.7.2 (U) APPLICATION

(U//~~FOUO~~) FISA Business Records Orders may be used during authorized national security investigations. b7E When collecting positive foreign intelligence, if the subject is a non-USPER, a request for business records pursuant to 50 U.S.C. §§ 1861-63 is lawful.

18.6.7.3 (U) BUSINESS RECORDS UNDER FISA

18.6.7.3.1 *(U) LEGAL AUTHORITY*

(U) 50 U.S.C. §§ 1861-63

18.6.7.3.2 *(U) DEFINITION OF METHOD*

(U) A FISA order for business records, is an order for a third party to produce relevant to an authorized national security investigation.

b7E

(U)

18.6.7.3.3 ***(U) APPROVAL REQUIREMENTS***

(U//~~FOUO~~

b7E

(U//~~FOUO~~)

18.6.7.3.4 ***(U) DURATION OF COURT APPROVAL***

(U) Authority for a FISA business records order is established by court order.

18.6.7.3.5 ***(U) NOTICE AND REPORTING REQUIREMENTS***

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

18.6.7.3.6 ***(U) COMPLIANCE REQUIREMENTS***

(U//~~FOUO~~) The employee who receives material produced in response to a FISA business records order must handle the material as required by the Standard Minimization Procedures Adopted for Business Records Orders and

b7E

[redacted] b7E

18.6.7.3.7 ***(U) FISA OVERCOLLECTION AND STANDARD MINIMIZATION PROCEDURES***

(U//~~FOUO~~[redacted] b7E

[redacted]

This Page is Intentionally Blank.

18.6.8 *(U) INVESTIGATIVE METHOD: STORED WIRE OR ELECTRONIC COMMUNICATIONS AND TRANSACTIONAL RECORDS*

18.6.8.1 (U) SUMMARY

(U//F~~OUO~~) FBI employees may acquire the contents of stored wire or electronic communications and associated transactional records—including basic subscriber information—as provided in 18 U.S.C. §§ 2701-2712 (Electronic Communications Privacy Act (ECPA)).

(U//F~~OUO~~) All requests for information from electronic communication service providers (e.g., telephone companies, internet service providers) pertaining to a subscriber or customer must comply with ECPA. As used in ECPA, the term "information pertaining to a subscriber or customer" should be read broadly. It includes, for example, information regarding whether a particular individual has an account with a covered provider. Thus, unless done in accordance with ECPA, an FBI employee may not ask a telephone company or internet service provider whether John Smith has an account with the company (i.e., the FBI employee may not informally seek information that is statutorily protected prior to the issuance of appropriate process or the existence of an exception to ECPA). In addition, based on a November 5, 2008 interpretation of ECPA from the Office of Legal Counsel, the FBI may not ask a telephone company whether a given telephone number that the company services has been assigned to an individual. In short, in order to obtain any information specific to the subscriber from a telephone company or electronic communication service provider, the FBI must provide legal process pursuant to 18 U.S.C. §§ 2703 or 2709 or the request must fall within the limited exceptions established in 18 U.S.C. § 2702, and discussed below.

(U//F~~OUO~~)

18.6.8.2 (U) APPLICATION

(U//F~~OUO~~) b7E

18.6.8.2.1 *(U) STORED DATA*

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

(U) Records covered by ECPA include all records that are related to the subscriber, including buddy lists, "friend" lists (Facebook), and virtual property owned (Second Life). These other

sorts of records are not subscriber records and cannot be obtained with a subpoena under 18 U.S.C. § 2703(c)(2) or an NSL under 18 U.S.C. § 2709.

18.6.8.2.2 *(U) LEGAL PROCESS*

(U) The legal process for obtaining disclosure will vary depending on the type of information sought and whether the information is being voluntarily provided under 18 U.S.C. § 2702 (e.g., with consent or when emergency circumstances allow disclosure) or the provider is being compelled to provide the information under 18 U.S.C. § 2703, as outlined below. The process for compelling production under 18 U.S.C. § 2709 is discussed in the NSL section above.

18.6.8.2.3 *(U) RETRIEVAL*

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

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

(U) Title 18 U.S.C. § 2705 establishes the standard to delay notice for an initial period of up to 90 days. Records or other information pertaining to a subscriber to or customer of such services, including basic subscriber information, can be obtained with a search warrant or an 18 U.S.C. § 2703(d) order without notice.

18.6.8.2.4 *(U) BASIC SUBSCRIBER INFORMATION*

(U) Basic subscriber information, as described in 18 U.S.C. § 2703(c)(2), can be compelled by a grand jury or administrative subpoena without notice.

18.6.8.2.5 *(U) PRESERVATION OF STORED DATA*

(U) The government is authorized under 18 U.S.C. § 2703(f) to direct a provider to preserve records or other information (stored records or communications) in its possession for 90 days (which may be extended for an additional 90-days) pending issuance of applicable legal process for disclosure. To make a preservation request, the FBI must believe that the records will subsequently be sought by appropriate legal process.

18.6.8.2.6 *(U) COST REIMBURSEMENT*

(U) 18 U.S.C. § 2706 requires the government to reimburse for costs incurred in providing the contents of communications, records, or other information obtained under 18 U.S.C. §§ 2702, 2703, or 2704, except that reimbursement is not required for records or other information maintained by a communications common carrier that relate to telephone toll records and telephone listings obtained under 18 U.S.C. § 2703. In essence, the government does not have to reimburse for the cost of producing records that the provider maintains in the ordinary course of its business.

18.6.8.3 (U) LEGAL AUTHORITY

(U) 18 U.S.C. §§ 2701-2712

(U) AGG-Dom, Part V.9

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

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

(U) [redacted] b7E

18.6.8.4 (U) ECPA DISCLOSURES

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

18.6.8.4.1 *(U) DEFINITIONS*

A) (U) ***Electronic Storage:*** is "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof," or "any storage of such communication by an electronic communication service for purposes of backup protection of such communication." 18 U.S.C. § 2510(17). In short, "electronic storage" refers only to temporary storage, made in the course of transmission, by a provider of an electronic communication service.

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

C) (U) ***Electronic Communications System:*** is "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." 18 U.S.C. § 2510(14).

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

18.6.8.4.2 *(U) COMPELLED DISCLOSURE*

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

A) (U) Search warrant;

B) (U) 18 U.S.C. § 2703(d) court order with prior notice to the subscriber or customer;

C) (U) 18 U.S.C. § 2703(d) court order without prior notice to the subscriber or customer;

D) (U) Subpoena with prior notice to the subscriber or customer; and

E) (U) Subpoena without prior notice to the subscriber or customer.

(U)

b7E

(U)

18.6.8.4.2.1 (U//~~FOUO~~) COMPELLED DISCLOSURE REGARDING MEMBERS OF THE NEWS MEDIA[75]

(U//~~FOUO~~)

b7E

[75] Note: Due to an administrative error, the version of the DIOG released on September 17, 2021, prematurely included new requirements pertaining to the use of compulsory processes to obtain information from, or records of, members of the news media. As of October 25, 2021, those changes (including some that erroneously appeared on this page) have been reverted to the previous release of the DIOG, dated March 31, 2020. Additional updates about this topic are coming soon. Questions should be directed to CDCs or IPO.

b7E

(U) 28 CFR § 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 above.

18.6.8.4.2.2 (U//F~~OUO~~) NOTICE—ORDERS NOT TO DISCLOSE THE EXISTENCE OF A WARRANT, SUBPOENA, OR COURT ORDER

(U//F~~OUO~~) FBI employees may obtain a court order directing network service providers not to disclose the existence of compelled process if the government has no legal duty to notify the customer or subscriber of the process. If an 18 U.S.C. § 2703(d) order or 18 U.S.C. § 2703(a) warrant is being used, a request for a non-disclosure order can be included in the application and proposed order or warrant. If a subpoena is being used to obtain the information, a separate application to a court for a non-disclosure order must be made.

18.6.8.4.2.3 (U) LEGAL STANDARD

(U//~~FOUO~~) A court may order an electronic communications service provider or remote computing service not to disclose the existence of a warrant, subpoena, or court order for such period as the court deems appropriate. The court must enter such an order if it determines that there is reason to believe that notification of the existence of the warrant, subpoena, or court order will result in:

A) (U) Endangering the life or physical safety of an individual;

B) (U) Flight from prosecution;

C) (U) Destruction of or tampering with evidence;

D) (U) Intimidation of potential witnesses; or

E) (U) Otherwise seriously jeopardizing an investigation or unduly delaying a trial. 18 U.S.C. § 2705(b).

18.6.8.4.2.4 (U) SEARCH WARRANT

(U//~~FOUO~~) Investigators can obtain the full contents of a network account with a search warrant issued pursuant to FRCP Rule 41. However, FRCP Rule 41 search warrant may not be issued in Preliminary Investigations. See DIOG Section 18.7.1.3.4.4.

18.6.8.4.2.5 (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 an 18 U.S.C. § 2703(d) court order without notice.

(U)

(U)

b7E

18.6.8.4.2.5.1 ***(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.

18.6.8.4.2.5.2 ***(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 to18 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 an 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). These orders issued by state courts, however, do not have effect outside the jurisdiction of the issuing state. See 18 U.S.C. §§ 2711(3).

18.6.8.4.2.6 (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).

18.6.8.4.2.6.1 *(U) TYPES OF TRANSACTIONAL RECORDS*

(U) The broad category of transactional records includes all records held by a service provider that pertain to the subscriber beyond the specific records listed in 2703(c)(2)

b7E

(U//~~FOUO~~

18.6.8.4.2.6.2 *(U) CELL SITE AND SECTOR INFORMATION*

(U) Cell site and sector information is considered "a record or other information pertaining to a subscriber" and therefore, production of historical and prospective cell site and sector information may be compelled by a court order under 18 U.S.C. § 2703(d). Requests made pursuant to 18 U.S.C. § 2703(d) for disclosure of prospective cell site and sector information—which is delivered to law enforcement under Communications Assistance for Law Enforcement Act (CALEA) at the beginning and end of calls— must be combined with an application for pen register/trap and trace device. Some judicial districts will require a showing of probable cause before authorizing the disclosure of prospective cell site and sector information.

18.6.8.4.2.6.3 *(U)*

b7E

(U)

(U//~~FOUO~~)

b7E

(U)

(U)

18.6.8.4.2.6.4 ***(U) LEGAL STANDARD***

(U) A court order under 18 U.S.C. § 2703(d) is known as an "articulable facts" court order or simply a "d" order. This section imposes an intermediate standard to protect online transactional records. It is a standard higher than a subpoena, but not a probable cause warrant.

(U) In applying for an order pursuant to 18 U.S.C. § 2703 (d), the FBI must state sufficient specific and articulable facts for the court to find that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation.

18.6.8.4.2.7 **(U) SUBPOENA WITH PRIOR NOTICE TO THE SUBSCRIBER OR CUSTOMER**

b7E

(U//~~FOUO~~) Investigators can subpoena opened e-mail from a provider if they give prior notice to the subscriber or comply with the delayed notice provisions of 18 U.S.C. § 2705(a)— hat there is reason to believe notification of the existence of the subpoena may have an adverse result.

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

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

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

C) (U) Basic subscriber information listed in 18 U.S.C. § 2703(c)(2).

(U) As a practical matter, this means that b7E

(U)

(U) ***Legal standards for delaying notice:*** The supervisory official must certify in writing that "there is reason to believe that notification of the existence of the court order may... endanger[] the life or physical safety of an individual; [lead to] flight from prosecution; [lead to] destruction of or tampering with evidence; [lead to] intimidation of potential witnesses; or... otherwise seriously jeopardiz[e] an investigation or unduly delay[] a trial." 18 U.S.C. §§ 2705(a)(1)(A), 2705(a)(2). This standard must be satisfied anew every time an extension of the delayed notice is sought. This documentation must be placed with the subpoena in the appropriate investigative file.

18.6.8.4.2.8 (U) SUBPOENA WITHOUT PRIOR NOTICE TO THE SUBSCRIBER OR CUSTOMER

(U//~~FOUO~~) Without notice to the subscriber or customer, investigators can subpoena basic subscriber information:

> (U) "name; address; local and long distance telephone connection records, or records of session times and durations; length of service (including start date) and types of service used; telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and means and source of payment for such service (including any credit card or bank account number)[.]" 18 U.S.C. § 2703(c)(2).

(U b7E

b7E

A) (U) ***Legal Standard:*** The legal threshold for issuing a subpoena is relevance to the investigation. Courts are reluctant to review the "good faith" issuance of subpoenas as long as they satisfy the following factors[76]: (i) the investigation is conducted pursuant to a legitimate purpose; (ii) the information requested under the subpoena is relevant to that purpose; (iii) the agency does not already have the information it is seeking with the subpoena; and (iv) the agency has followed the necessary administrative steps in issuing the subpoena.

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

b7E

B) (U//F~~OUO~~)

C) (U) ***Members of the News Media:*** Approval of the Attorney General must be obtained prior to seeking telephone billing records of a member of the news media. (See DIOG Section 18.6.5.7)

18.6.8.4.3 ***(U) VOLUNTARY DISCLOSURE***

b7E

(U)

A) (U) ***Service NOT Available to the Public:*** ECPA does not apply to providers of services that are not available "to the public;" accordingly such providers may freely disclose both contents and other records relating to stored communications. Andersen Consulting v. UOP, 991 F. Supp. 1041 (N.D. Ill. 1998) (giving hired consulting firm employees access to UOP's e-mail system is not equivalent to providing e-mail to the public).

B) (U) ***Services That ARE Available to the Public:*** If the provider offers services to the public, then ECPA governs the disclosure of contents and other records.

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

D) (U) If a provider voluntarily discloses under the statute, there is no follow-up legal process required or available. If the provider, on the other hand, either may not or will not disclose the

[76] (U) United States v. Morton Salt Co., 338 U.S. 632, 642-43 (1950).

[77] Note: Due to an administrative error, the version of the DIOG released on September 17, 2021, prematurely included new requirements pertaining to the use of compulsory processes to obtain information from, or records of, members of the news media. As of October 25, 2021, those changes (including some that erroneously appeared on this page) have been reverted to the previous release of the DIOG, dated March 31, 2020. Additional updates about this topic are coming soon. Questions should be directed to CDCs or IPO.

information voluntarily, FBI employees must rely on compelled disclosure provisions and obtain the appropriate legal orders.

1) (U) **Voluntary Disclosure of Stored Contents** - ECPA authorizes the voluntary disclosure of stored contents when:

   a) (U) The originator, addressee, intended recipient, or the subscriber (in the case of opened e-mail) expressly or impliedly consents, 18 U.S.C. § 2702(b)(3);

   b) (U) The disclosure "may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service," 18 U.S.C. § 2702(b)(5);

   c) (U) The provider "in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of information relating to the emergency," 18 U.S.C. § 2702(b)(8);

   d) (U//~~FOUO~~) An emergency disclosure under this statutory exception is justified when the circumstances demand action without delay to prevent death or serious bodily injury; the statute does not depend on the immediacy of the risk of danger itself. For example [redacted] b7E

   [redacted]

   H.R Rep. No. 107-497 at 13-14 (2002) accompanying The Cyber Security Enhancement Act of 2002, H.R. 3482, which passed as part of the comprehensive Homeland Security Act of 2002, Pub. L. No. 107-296, § 225 116 Stat. 2135 (2002).

   e) (U) The disclosure is made to the National Center for Missing and Exploited Children, in connection with a report submitted thereto under Section 227 of the Victims of Child Abuse Act of 1990. (42 U.S.C. § 13032 and 18 U.S.C. § 2702[b][6]); or

   f) (U) The contents are inadvertently obtained by the service provider and appear to pertain to the commission of a crime. Such disclosures can only be made to a law enforcement agency. 18 U.S.C. § 2702(b)(7)

2) (U) **Voluntary Disclosure of Non-Content Customer Records** - ECPA permits a provider to voluntarily disclose non-content customer records to the government when:

   a) (U) The customer or subscriber expressly or impliedly consents, 18 U.S.C. § 2702(c)(2);

   b) (U) The disclosure "may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service," 18 U.S.C. § 2702(c)(3);

   c) (U) The provider "in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of information relating to the emergency," 18 U.S.C. § 2702(c)(4); or

   d) (U//~~FOUO~~) *Note:* An emergency disclosure under this statutory exception is justified when the circumstances demand immediate action (i.e., obtaining/disclosing information "without delay") to prevent death or serious bodily injury; the statute does not depend on the immediacy of the risk of danger itself. For example, an e-mail that discusses a planned terrorist attack but not the timing of the attack would constitute an emergency that threatens life or limb and requires immediate action, even though the

timing of the attack is unknown. It is the need for immediate action to prevent the serious harm threatened rather than the immediacy of the threat itself that provides the justification for voluntary disclosures under this exception. H.R Rep. No. 107-497 at 13-14 (2002) accompanying The Cyber Security Enhancement Act of 2002, H.R. 3482, which passed as part of the comprehensive Homeland Security Act of 2002, Pub. L. No. 107-296, § 225 116 Stat. 2135 (2002).

e) (U) The disclosure is to the National Center for Missing and Exploited Children, in connection with a report submitted thereto under Section 227 of the Victims of Child Abuse Act of 1990. (42 U.S.C. § 13032 and 18 U.S.C. § 2702[c][5])

3) (U) **Preservation of Evidence under 18 U.S.C. § 2703(f) -** FBI employees may direct providers to preserve existing records pending the issuance of compulsory legal process. Such requests, however, have no prospective effect.

a) (U) Because there is generally no law regulating how long a network service provider must retain account records, there is a risk that evidence might be destroyed or lost in the normal course of the provider's business before law enforcement can obtain legal process to compel disclosure. A governmental entity is authorized to direct providers to preserve stored records and communications pursuant to 18 U.S.C. § 2703(f). Once a preservation request is made, ECPA requires that the provider must retain the records for 90 days, renewable for another 90-day period upon a government request. See 18 U.S.C. § 2703 (f)(2).

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

c) (U) FBI employees who send 18 U.S.C. § 2703(f) letters to network service providers should be aware of two limitations. First, the authority to direct providers to preserve records and other evidence is not prospective. Thus, 18 U.S.C. § 2703(f) letters can order a provider to preserve records that have already been created but cannot order providers to preserve records not yet made. If FBI employees want providers to record information about future electronic communications, they must comply with the electronic surveillance statutes. A second limitation of 18 U.S.C. § 2703(f) is that some providers may be unable to comply effectively with 18 U.S.C. § 2703(f) requests b7E

4) (U) **Video Tape Rental or Sales Records -** 18 U.S.C. § 2710 makes the unauthorized disclosure of records by any person engaged in the rental, sale, or delivery of prerecorded video cassette tapes or similar audiovisual materials unlawful and provides an exclusionary rule to prohibit personally identifiable information otherwise obtained from being admissible as evidence in any court proceeding. Personally identifiable information is defined as "information that identifies a person as having requested or obtained specific video material or services . . . ."

a) (U) The disclosure to law enforcement of "personally identifiable information" is permitted only when the law enforcement agency:

(i) (U) Has the written consent of the customer;

(ii) (U) Obtains a search warrant issued under Rule 41, FRCP or equivalent state warrant; or

(iii) (U) Serves a grand jury subpoena;

b) (U) [redacted] b7E

[redacted]

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

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

18.6.8.5 (U) VOLUNTARY EMERGENCY DISCLOSURE

18.6.8.5.1 *(U) SUMMARY*

(U//~~FOUO~~) The Electronic Communication Privacy Act (ECPA) protects subscriber and transactional information regarding communications (and the contents of such communications) from disclosure by providers of remote computing services or telephone or other electronic communication services to the public. Remote computing services, telephone and other electronic communications services are hereafter collectively referred to as "electronic communications service providers" or "providers." Generally, an NSL, a subpoena, or another form of legal process must be used to compel the electronic communications service provider to disclose such information. [redacted]

[redacted] b7E

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

[redacted]

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

[redacted]

(U//~~FOUO~~) [redacted] is designed to capture all the information the FBI needs to satisfy statutory annual Congressional reporting requirements.

18.6.8.5.2 ***(U) APPLICATION***

(U//~~FOUO~~) b7E

18.6.8.5.3 ***(U) DURATION OF APPROVAL***

(U) The must be approved by the designated officials as set forth in the following subsection. The approval to use this statutory authority remains for as long as the emergency necessitating the usage exists, and only in those circumstances when it is impracticable to obtain another legal process, such as a subpoena or an NSL. b7E

18.6.8.5.4 ***(U) SPECIFIC PROCEDURES***

A) (U//~~FOUO~~) ***Required use of the***

(U//~~FOUO~~)

1. (U//~~FOUO~~) b7E

B) (U//~~FOUO~~) ***Use of the provider's form:***

(U//~~FOUO~~)

(U//~~FOUO~~) b7E

C) (U//~~FOUO~~) ***Filling Requirements:***

18.6.8.5.5 ***(U) COST REIMBURSEMENT***

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

A) (U) Standardized payment procedures may be found in the OGC law library.

B) (U) *DOJ's Cost Reimbursement Guidance under the ECPA* can also be found in 18 U.S.C. § 2706.

18.6.8.5.6 ***(U) CONGRESSIONAL REPORTING REQUIREMENTS***

18.6.8.5.6.1 **(U) ISSUING EMPLOYEE**

(U) The database system that hosts the form will, when necessary, generate e-mail requests to the issuing employees to ensure that the information necessary to be included in the report to DOJ, which is also used to prepare the required Congressional report, is current. It is the responsibility of the issuing employees to respond to these requests for information as directed. b7E

18.6.8.5.6.2 **(U) OGC AND OPERATIONAL DIVISIONS**

(U) To fulfill Congressional reporting requirements, OGC, working with the appropriate FBIHQ operational divisions, is responsible for completing a report containing the following information for the previous calendar year:

A) (U) A tabulation of the number of accounts from which the FBI received voluntary disclosures under the authority of 18 U.S.C. § 2702(b)(8).

B) (U) A summary of the basis for the disclosures received pursuant to 18 U.S.C. § 2702(b)(8) in those instances in which the relevant investigation was closed without the filing of criminal charges.

C) (U) A tabulation of the number of accounts from which the FBI received voluntary disclosures under the authority of 18 U.S.C. § 2702(c)(4).

(U) The report must be submitted to the General Counsel for review and submission to DOJ by January 31 each year.

This Page is Intentionally Blank.

18.6.9 *(U) INVESTIGATIVE METHOD: PEN REGISTERS AND TRAP/TRACE DEVICES (PR/TT)*

18.6.9.1 (U) SUMMARY

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

18.6.9.2 (U) APPLICATION

(U//~~FOUO~~ b7E

18.6.9.3 (U) LEGAL AUTHORITY

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

18.6.9.4 (U) DEFINITION OF INVESTIGATIVE METHOD

(U) A pen register device or process 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. See 18 U.S.C. § 3127(3).

(U) A trap and trace device or process 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. See 18 U.S.C. § 3127(4).

18.6.9.5 (U) STANDARDS FOR USE AND APPROVAL REQUIREMENTS FOR INVESTIGATIVE METHOD

18.6.9.5.1 *(U) PEN REGISTER/TRAP AND TRACE UNDER FISA*[78]

(U) Applications for authority to use a PR/TT device can be made to the FISC in national security investigations. See 50 U.S.C. § 1842.

[78] Note: Due to an administrative error, the version of the DIOG released on September 17, 2021, prematurely included new requirements pertaining to the use of compulsory processes to obtain information from, or records of, members of the news media. As of October 25, 2021, those changes (including some that erroneously *appeared on*

(U//~~FOUO~~) b7E

(U) 28 CFR § 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 above.

18.6.9.5.1.1 **(U) LEGAL STANDARD**

(U) Applications to the FISC are to be under oath and must include:

A) (U) The identity of the federal officer making the application; and

B) (U) A certification by the applicant that the information likely to be obtained is foreign intelligence information not concerning an USPER or is information that is relevant to an ongoing investigation to protect the United States against international terrorism or clandestine intelligence activities; and that such investigation, if of an USPER, is not conducted solely upon the basis of activities protected by the First Amendment to the Constitution.

18.6.9.5.1.2 **(U) PROCEDURES**

(U//~~FOUO~~) Requests for initiating or a renewal of FISA PR/TT must be made using b7E

Routing a paper copy for signatures is not required. See the *Foreign*

this page) have been reverted to the previous release of the DIOG, dated March 31, 2020. Additional updates about this topic are coming soon. Questions should be directed to CDCs or IPO.

Intelligence Surveillance Act and Standard Minimization Procedures Policy Guide, (1242PG), for additional guidance on FISA PR/TT requirements.

(U//~~FOUO~~) See the [redacted] b7E for additional guidance.

18.6.9.5.1.3 (U) EMERGENCY AUTHORITY—FISA: 50 U.S.C. § 1843

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

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

A) (U) The Attorney General may authorize the installation and use of a PR/TT upon a determination that an emergency exists and that the factual basis exists for a court order. The FISC must be informed at the time of the authorization and an application for a court order must be made to the court as soon as practicable, but no more than seven (7) days after the authorization. If the court does not issue an order approving the use of a PR/TT, an emergency-authorized PR/TT use must terminate at the earliest of when the information sought is obtained, when the FISC denies the application, or seven (7) days after the Attorney General authorization is given. b7E

B) (U) If the FISC denies the application after an emergency PR/TT device has been installed, no information collected as a result may be used in any manner, except with the approval of the Attorney General upon a showing that the information indicates a threat of death or serious bodily harm to any person.

(U) Notwithstanding the foregoing, the President, acting through the Attorney General, may authorize the use of a PR/TT, without a court order, for a period not to exceed 15 calendar days, following a declaration of war by Congress. See 50 U.S.C. § 1844.

(U//~~FOUO~~) For an emergency authorization to use a PR/TT surveillance [redacted] at any time.

18.6.9.5.1.4 (U) COMPLIANCE REQUIREMENTS

(U//~~FOUO~~) [redacted] b7E

b7E

18.6.9.5.1.5 **(U) FISA OVERCOLLECTION**

(U//~~FOUO~~) In accordance with Foreign Intelligence Surveillance Court (FISC) Rule of Procedure 15, information acquired outside of the scope of the FISA authorization ("FISA overcollection") will no longer be sequestered with the FISC, absent extraordinary circumstances. Contact NSCLB for further guidance regarding the handling of any FISA overcollection.

18.6.9.5.2 ***(U) CRIMINAL PEN REGISTER/TRAP AND TRACE UNDER TITLE 18***[79]

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

(U//~~FOUO~~)

b7E

(U) Note: 28 CFR § 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 above.

18.6.9.5.2.1 **(U) LEGAL STANDARD**

(U) Applications for authorization to install and use a PR/TT device must include:

A) (U) The identity of the attorney for the government or the state law enforcement or investigative officer making the application and the identity of the law enforcement agency conducting the investigation; and

B) (U) A certification by the applicant that the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by that agency.

[79] Note: Due to an administrative error, the version of the DIOG released on September 17, 2021, prematurely included new requirements pertaining to the use of compulsory processes to obtain information from, or records of, members of the news media. As of October 25, 2021, those changes (including some that erroneously appeared on this page) have been reverted to the previous release of the DIOG, dated March 31, 2020. Additional updates about this topic are coming soon. Questions should be directed to CDCs or IPO.

18.6.9.5.2.2 **(U//~~FOUO~~) PROCEDURES**

(U//~~FOUO~~) An SSA must approve a request for initiating or renewal of PR/TT use prior to submission of the request to an attorney for the government. Before approving such a request, the SSA should consider the following:

A) (U//~~FOUO~~) The use of resources based on the investigative purpose set forth;

B) (U//~~FOUO~~) Whether there is sufficient factual basis for the certification to be made in the application (i.e., is the information likely to be obtained relevant to an ongoing criminal investigation);

C) (U//~~FOUO~~) Whether the customer or subscriber has consented to the use of a PR/TT, see 18 U.S.C. § 3121(b)(3); or

D) (U//~~FOUO~~) Whether the use of a PR/TT is the least intrusive method if reasonable based upon the circumstances of the investigation.

(U//~~FOUO~~) A copy of the approving EC must be maintained in the pen register sub-file "PEN."

(U//~~FOUO~~) A PR/TT order is executable anywhere within the United States and, upon service, the order applies to any person or entity providing wire or electronic communication service in the United States whose assistance may facilitate the execution of the order.

(U//~~FOUO~~) See [redacted] for additional guidance. b7E

18.6.9.5.2.3 **(U) EMERGENCY AUTHORITY—CRIMINAL: 18 U.S.C. § 3125**

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

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

A) (U) Immediate danger of death or serious bodily injury to any person;

B) (U) Conspiratorial activities characteristic of organized crime;

C) (U) An immediate threat to a national security interest; or

D) (U) An ongoing attack on a protected computer (as defined in 18 U.S.C. § 1030) that constitutes a crime punishable by a term of imprisonment greater than one year.

(U) Only DOJ officials have the authority to authorize the emergency installation of a PR/TT. The FBI does not have this authority. If the DOJ authorizes the emergency installation of a PR/TT, the government has 48 hours after the installation to apply for and obtain a court order according to 18 U.S.C. § 3123. It is a violation of law to fail to apply for and obtain a court order within this 48 hour period. Use of the PR/TT shall immediately terminate when the information sought is obtained, when the application for

a court order is denied, or if no court order has been obtained 48 hours after the installation of the PR/TT device in emergency situations.

(U//FOUO) As with requesting authorization for an emergency Title III [redacted] b7E

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

(U//FOUO) If an emergency situation arises after regular business hours [redacted] b7E

[redacted] During regular business hours [redacted]

18.6.9.6 **(U) DURATION OF APPROVAL**

A) (U) ***FISA:*** The use of a PR/TT device may be authorized by the FISC for a period of time not to exceed 90 days in investigations targeting an USPER. Extensions may be granted for periods not to exceed 90 days upon re-application to the court. In investigations in which the applicant has certified that the information likely to be obtained is foreign intelligence information not concerning a U.S. person (USPER), an order or extension may be for a period of time not to exceed one year.

B) (U) ***Criminal:*** The installation and use of a PR/TT device may be authorized by court order under 18 U.S.C. § 3123 for a period not to exceed 60 days, which may be extended for additional 60-day periods.

18.6.9.7 **(U) SPECIFIC PROCEDURES**

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

A) (U//FOUO) [redacted] b7E

B) (U//FOUO) [redacted]

C) (U//FOUO) [redacted]

D) (U//~~FOUO~~) [redacted] b7E

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

18.6.9.8 (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 Questions concerning the FISA use policy or requests for assistance in obtaining FISA use authority from the AG should be directed to NSCLB's Classified Litigation Support Unit.

(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).

18.6.9.9 (U) CONGRESSIONAL NOTICE AND REPORTING REQUIREMENTS

18.6.9.9.1 *(U) CRIMINAL PEN REGISTER/TRAP AND TRACE- ANNUAL REPORT*

(U) The Attorney General is required to make an annual report to Congress on the number of criminal PR/TT orders applied for by DOJ law enforcement agencies. See 18 U.S.C. § 3126. The report must include the following information:

A) (U) The period of interceptions authorized by the order, the court order number, and duration of any extensions;

B) (U) The offense specified in the order or application, or extension;

C) (U) The number of investigations involved;

D) (U) The number and nature of the facilities affected; and

E) (U) The identity, including the district, of the applying agency making the application and the person authorizing the order.

(U//~~FOUO~~) DOJ, Criminal Division, OEO requires the FBI to provide annual reports on pen register usage. To satisfy DOJ data requirements and standardize and simplify field reporting, court-ordered pen register usage must be reported to FBIHQ [redacted] b7E

[redacted] within five (5) workdays after the expiration date of an original order and any extensions, or denial of an application for an order. For all criminal PR/TT orders or extensions issued on or after January 1, 2009, the [redacted] These reporting requirements do not apply to PR/TT authorized pursuant to consent or under the provisions of FISA. b7E

18.6.9.9.2 *(U) National Security Pen Registers and Trap and Trace – Semi-Annual Report*

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

A) (U) The total number of applications made for orders approving the use of PR/TT devices;

B) (U) The total number of such orders either granted, modified, or denied; and

C) (U) The total number of PR/TT devices whose installation and use was authorized by the Attorney General on an emergency basis and the total number of subsequent orders approving or denying the installation and use of such PR/TT devices.

18.6.9.10 (U) Post Cut-Through Dialed Digits (PCTDD)

18.6.9.10.1 *(U) Overview*

(U//~~FOUO~~) Telecommunication networks provide users the ability to engage in extended dialing and/or signaling (also known as "post cut-through dialed digits" or PCTDD), which in some circumstances are simply call-routing information and, in others, are call content. For example, non-content PCTDD may be generated when a party places a calling card, credit card, or collect call by first dialing a long-distance carrier access number and then, after the initial call is "cut through," dialing the telephone number of the destination party. In other instances, PCTDD may represent call content, such as when a party calls an automated banking service and enters an account number, calls a pharmacy's automated prescription refill service and enters prescription information, or enters a call-back number when prompted by a voice mail service. See United States Telecom Assn v. Federal Communications Commission, 227 F.3d 450, 462 (D.C. Cir. 2000). [redacted] b7E

(U//~~FOUO~~) The definition of both a pen register device and a trap and trace device provides that the information collected by these devices "shall not include the contents of any communication." See 18 U.S.C. § 3127(3) and (4). In addition, 18 U.S.C. § 3121(c) makes explicit the requirement to "use technology reasonably available" that restricts the collection of information "so as not to include the contents of any wire or electronic communications." "Content" includes any information concerning the substance, purport, or meaning of a communication. See 18 U.S.C. § 2510(8). When the pen register definition is read in conjunction with the limitation provision, however, it suggests that although a PR/TT device may not be used for the express purpose of collecting content, the incidental collection of content may occur despite the use of "reasonably available" technology to minimize, to the

extent feasible, any possible over collection of content while still allowing the device to collect all of the dialing and signaling information authorized.

(U//~~FOUO~~) ***DOJ Policy:*** In addition to this statutory obligation, DOJ has issued a directive in [redacted] to all DOJ agencies requiring that no affirmative investigative use may be made of PCTDD incidentally collected that constitutes content, except in cases of emergency—to prevent an immediate danger of death, serious physical injury, or harm to the national security. b7E

(U//~~FOUO~~) [redacted] b7E

[redacted]

18.6.9.10.2 ***(U) COLLECTION OF PCTDD***

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

[redacted]

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

[redacted] b7E

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

[redacted]

18.6.9.10.3 ***(U) USE OF PCTDD***

(U//~~FOUO~~) [redacted] b7E

[redacted]

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

[redacted]

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

[redacted]

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

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

4) (U//~~FOUO~~)

b7E

5) (U//~~FOUO~~)

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

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

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

18.6.9.10.4 ***(U) WHAT CONSTITUTES PCTDD CONTENT***

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

(U//~~FOUO~~)

b7E

b7E

18.6.9.11 **(U//~~FOUO~~)** b7E

(U//~~FOUO~~)

18.6.9.11.1 ***(U//~~FOUO~~) TO LOCATE A KNOWN PHONE NUMBER***

A) (U//~~FOUO~~) ***Authority:*** A standard PR/TT order issued pursuant to 18 U.S.C. § 3127 is adequate to authorize the use of this technology to determine the location of a known targeted phone, provided that the language authorizes FBI employees to install or cause to be installed and use a pen register device, without geographical limitation, at any time of day or night within (X) days from the date the order is signed, to record or decode dialing, routing, addressing, or signaling information transmitted by the "Subject Telephone." Due to varying and often changing court interpretations of the requirements for obtaining cell site location information, agents contemplating legal process to obtain such information should consult as necessary with their CDC and/or AUSA for the legal requirements in their particular jurisdiction. The application and order should generally also request authority to compel disclosure of cell site location data on an ongoing basis under 18 U.S.C. § 2703(d)—or probable cause, if such is required by the particular district court—as such information may assist in determining the general location of the targeted phone. b7E

B) (U//F~~OUO~~)

C) (U//F~~OUO~~)

[redacted]" Under Kyllo v. United States, 533 U.S. 27 (2001), the use of equipment not in general public use to acquire data that is not otherwise detectable that emanates from a private premise implicates the Fourth Amendment [redacted] b7E

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

[redacted]

18.6.9.11.2 ***(U//~~FOUO~~) TO IDENTIFY AN UNKNOWN TARGET PHONE NUMBER***

(U//~~FOUO~~) ***Authority:*** [redacted] b7E

[redacted]

(U//~~FOUO~~) [redacted] b7E

[redacted]

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

[redacted]

B) (U//F~~OUO~~)

b7E

18.6.9.11.3 ***(U) PR/TT ORDER LANGUAGE***

(U) The language in the order should state that "the pen register will be implemented unobtrusively and with minimum interference with the services accorded to customers of such service."

18.6.9.12 (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 Sentinel.

This Page is Intentionally Blank.

18.6.10 *(U) INVESTIGATIVE METHOD: MAIL COVERS*

18.6.10.1 (U) SUMMARY

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

(U)

(U)

b7E

18.6.10.2 (U) APPLICATION

(U//~~FOUO~~

b7E

18.6.10.3 (U) LEGAL AUTHORITY

A) (U) Postal Service Regulation 39 CFR § 233.3 is the sole authority and procedure for opening a mail cover and for processing, using and disclosing information obtained from a mail cover;

B) (U) There is no Fourth Amendment protection for information on the outside of a piece of mail. See, e.g., U.S. v. Choate, 576 F.2d 165, 174 (9th Cir., 1978); and U.S. v. Huie, 593 F.2d 14 (5th Cir., 1979); and

C) (U) AGG-Dom, Part V.A.2.

18.6.10.4 (U) DEFINITION OF INVESTIGATIVE METHOD

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

A) (U) Protect the national security;

B) (U) Locate a fugitive;

C) (U) Obtain evidence of commission or attempted commission of a federal crime;

D) (U) Obtain evidence of a violation or attempted violation of a postal statute; or

E) (U) Assist in the identification of property, proceeds or assets forfeitable under law. See 39 CFR § 233.3(c) (1).

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

18.6.10.5 (U) STANDARD FOR USE AND APPROVAL REQUIREMENTS FOR INVESTIGATIVE METHOD

(U)

b7E

(U//~~FOUO~~) ***National Security Mail Cover:***

(U//~~FOUO~~)

(U//~~FOUO~~) ***Required Form:***

(U//~~FOUO~~) ***Criminal Mail Cover:***

(U//~~FOUO~~) ***Required Form.*** b7E

(U//~~FOUO~~) ***Review and Approval of National Security or Criminal Mail Cover Requests:*** Approval of any mail cover request or extension is conditioned on the following criteria being met:

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

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

C) (U//~~FOUO~~) b7E

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

E) (U//~~FOUO~~)

F) (U//~~FOUO~~) Under postal regulations, a mail cover must not include matter mailed between the mail cover subject and the subject's attorney, unless the attorney is also a subject under the investigation.

G) (U//~~FOUO~~) b7E

H) (U//~~FOUO~~)

I) (U//~~FOUO~~)

b7E

(U) ***Emergency Requests:*** For exigent circumstances an email request may be sent to the address. Requests sent to this mailbox should use the b7E

(U) b7E

18.6.10.6 **(U) DURATION OF APPROVAL**

A) (U) ***National Security Mail Covers:*** No national security mail cover may remain in force for longer than 120 continuous days unless personally approved for further extension by the Chief Postal Inspector or his/her designees at National Headquarters. See 39 CFR § 233.3(g)(6).

B) (U) ***Criminal Mail Covers Except Fugitives:*** A mail cover in a criminal investigation is limited to no more than 30 days, unless adequate justification is provided by the requesting authority. See 39 CFR § 233.3(g)(5). Renewals may be granted for additional 30-day periods, up to the maximum of 120 days, under the same conditions and procedures applicable to the original request. The requesting authority must provide a statement of the investigative benefit of the mail cover and anticipated benefits to be derived from the extension.

C) (U) ***Fugitives:*** No mail cover instituted to locate a fugitive may remain in force for longer than 120 continuous days unless personally approved for further extension by the Chief Postal Inspector or his/her designees at National Headquarters. See 39 CFR § 233.3(g)(6).

D) (U) ***Exception for Indictments and Information:*** Except for fugitive investigations, no mail cover may remain in force when an information has been filed or the subject has been indicted for the matter for which the mail cover has been requested. If the subject is under investigation for further criminal violations, or a mail cover is required to assist in the identification of property, proceeds or assets forfeitable because of a violation of criminal law, a new mail cover order must be requested. See 39 CFR § 233.3(g)(7). b7E

18.6.10.7 **(U) MAIL COVER DOCUMENTATION**

(U//~~FOUO~~) United States Postal Service (USPS) regulations require that the physical storage of all reports issued pursuant to a mail cover request be "at the discretion of the Chief Postal Inspector" (see 39 CFR § 233.3(h)(1)). Accordingly, FBI employees must conduct timely reviews of mail cover documents received from the USPS. A copy of the signed mail cover

request for Criminal Mail Covers must be maintained in the investigative file. Other communications between the FBI and the USPS by subsection 18.6.10.8 b7E

(U//~~FOUO~~) b7E (see DIOG subsection 18.6.10.8 for more detailed information on handling procedures in criminal investigations).

18.6.10.8 **(U) STORAGE OF MAIL COVER RESPONSIVE RECORDS–SPECIAL PROCEDURES FOR CRIMINAL CASES**

(U//~~FOUO~~)

b7E

(U//~~FOUO~~)

(U//~~FOUO~~) **NOTE**

(U//~~FOUO~~)

18.6.10.9 **(U) COMPLIANCE AND MONITORING**

(U//~~FOUO~~) FBI employees must conduct a timely review of mail cover information received from the USPS for any potential production of data beyond the scope of the requested mail cover ("overproduction"). Overproduced information from a mail cover must not be serialized into any FBI database or used in any manner.

A) (U//~~FOUO~~) ***Criminal Mail Cover – Overproduction:*** b7E

B) (U//~~FOUO~~) ***National Security Mail Cover – Overproduction:***

b7E

18.6.11 *(U) INVESTIGATIVE METHOD: POLYGRAPH EXAMINATIONS*

18.6.11.1 (U) SUMMARY

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

(U//~~FOUO~~) b7E b7E

(U//F~~OUO~~) This policy does not limit other authorized uses of the polygraph method outside of Assessments or predicated investigations, such as the FBI's responsibilities to conduct background checks and inquiries concerning applicants and employees under federal personnel security programs.

18.6.11.2 (U) APPLICATION

(U//~~FOUO~~)

when it is not otherwise prohibited by AGG-Dom, Part III.B.2-3.

18.6.11.3 (U) LEGAL AUTHORITY

(U) AGG-Dom, Part V.A.6 and AGG-VWA, Article III, Part L.2.b.(2).

18.6.11.4 (U) STANDARDS FOR USE AND APPROVAL REQUIREMENTS FOR INVESTIGATIVE METHOD

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

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

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

C) (U//~~FOUO~~) b7E

(U)

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

E) (U//~~FOUO~~)

18.6.11.5 **(U) DURATION OF APPROVAL** b7E

(U//~~FOUO~~)

18.6.11.6 **(U) SPECIFIC PROCEDURES**

(U//~~FOUO~~) An EC requesting the appropriate approval for the polygraph must be prepared as outlined in 18.6.11.4. If an AUSA is assigned to the investigation, an FBI employee must confer with the USAO to discuss any prosecutorial issues prior to the administration of the polygraph.

18.6.11.7 **(U) COMPLIANCE AND MONITORING**

(U//~~FOUO~~) All polygraphs conducted in predicated investigations must be documented in the investigative file b7E

18.6.12 *(U) INVESTIGATIVE METHOD: SEARCHES THAT DO NOT REQUIRE A WARRANT OR COURT ORDER (TRASH COVER, ABANDONED PROPERTY FROM A PUBLIC RECEPTACLE, ADMINISTRATIVE INVENTORY SEARCH OF A LOST/MISPLACED ITEM) AND INVENTORY SEARCHES GENERALLY*

18.6.12.1 (U) SUMMARY

(U) The Fourth Amendment to the United States Constitution prevents the FBI from conducting unreasonable searches and seizures. It also generally requires a warrant be obtained if the search will intrude on a reasonable expectation of privacy. To qualify as a "reasonable expectation of privacy," the individual must have an actual subjective expectation of privacy and society must be prepared to recognize that expectation as objectively reasonable. See Katz v. United States, 389 U.S. at 361. If an individual has a reasonable expectation of privacy, a warrant or order issued by a court of competent jurisdiction or an exception to the requirement for such a warrant or order is required before a search may be conducted. Physical searches of personal or real property may be conducted without a search warrant or court order if there is no reasonable expectation of privacy in the property or area. As a general matter, there is no reasonable expectation of privacy in areas that are exposed to public view or that are otherwise available to the public.

(U) A reasonable expectation of privacy may be terminated by an individual abandoning property, setting trash at the edge of the curtilage or beyond for collection, or when a private party reveals the contents of a package (See DIOG subsection 18.6.12.4.2. However, the AGG-Dom and FBI policy have restricted the use of "trash covers" to predicated investigations [redacted] b7E

18.6.12.2 (U) APPLICATION

(U//~~FOUO~~ [redacted]

[redacted] b7E

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

(U//~~FOUO~~) *Note*: Consent Searches are authorized in Assessments, as well as in predicated investigations.

(U//~~FOUO~~) [redacted] b7E

[redacted] when not otherwise prohibited by AGG-Dom, Part III.B.2-3. See DIOG subsection 18.6.12.6 below for information on use of these methods.

18.6.12.3 (U) LEGAL AUTHORITY

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

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

18.6.12.4 (U) DEFINITION OF INVESTIGATIVE METHOD

18.6.12.4.1 *(U) DISTINCTION BETWEEN A TRASH COVER, A SEARCH OF ABANDONED PROPERTY IN A PUBLIC RECEPTACLE, AND ADMINISTRATIVE INVENTORY SEARCH[80] OF A LOST OR MISPLACED ITEM*

A) (U//F~~OUO~~) ***Trash Cover:*** b7E

A trash cover is a targeted effort to gather information regarding a particular person or entity by reviewing that person or entity's refuse. Generally, a trash cover is planned in advance based upon information indicating that a specific trash container will contain evidence or intelligence of an investigative interest within a specified period of time.

B) (U//F~~OUO~~) b7E

If, for example, an FBI employee

value in any public trash receptacle, the FBI employee may recover the item(s) without having an Assessment or predicated investigation open at that time.

C) (U//F~~OUO~~) b7E

D) (U) b7E

(U

b7E

b7E

(U)

See *Field Evidence Management Policy Guide*, 1209PG.

(U) b7E

(U) See DIOG subsection 19.7 for guidance on search incident to arrest. See DIOG subsection 19.7.3 for guidance on inventory of personal property following arrest.

18.6.12.4.2 *(U) DETERMINATION OF AN AREA OF CURTILAGE AROUND A HOME*

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

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

18.6.12.5 (U) STANDARDS FOR USE AND APPROVAL REQUIREMENTS FOR A TRASH COVER

(U//~~FOUO~~) SSA approval is required for the use of a trash cover. In Type 5 Assessments, prior to using a trash cover, the employee must also consult with the CDC or OGC to determine whether the search implicates a reasonable expectation of privacy and thus requires a search warrant. During predicated investigations, if there is a doubt as to whether a person has a reasonable expectation of privacy in the area to be searched, the employee must consult with the CDC or OGC to determine whether a search warrant is required. Use of this method must be documented in the investigative file.

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

See the *Abandonment of Unclaimed Property Policy Guide* (1169PG).

18.6.13 *(U) INVESTIGATIVE METHOD: UNDERCOVER OPERATIONS*

18.6.13.1 (U) SUMMARY

(U//~~FOUO~~) b7E

(U//F~~OUO~~) 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//F~~OUO~~) ***Application:*** 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//F~~OUO~~) ***Undercover Activity (UCA):*** An "undercover activity" is any investigative activity involving the use of an assumed name or cover identity by an employee of the FBI or another Federal, state, tribal or local law enforcement organization working with the FBI. An element of UCA is the conduct of investigative activity to seek information relevant to federal crimes or national security threats by means of interaction with a third party(ies).

(U//~~FOUO~~) b7E

B) (U//F~~OUO~~) The Covert Approach, which may be authorized in an approved Type 5 Assessment, pursuant to the procedures detailed in the *CHSPG* [links to SECRET//NOFORN document], is not undercover activity subject to the provisions of this section (DIOG subsection 18.6.13). The distinction between undercover activity and the Covert Approach lies in the authorized purpose of a Type 5 Assessment, which is to seek information to identify,

evaluate, and recruit an individual as a CHS, and not to seek information relevant to federal crimes or national security threats.

C) (U//~~FOUO~~) ***Undercover Employee (UCE):*** An employee of the FBI, or employee of federal, state, or local law enforcement agency, USIC entity, or foreign intelligence agency working under the direction and control of the FBI during a particular investigation or operation whose relationship with the FBI is concealed from third parties in the course of an investigative or intelligence collection operation by the maintenance of a cover or alias identity.

D) (U//F~~OUO~~) ***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 individual(s) under investigation [redacted] b7E

[redacted]

(U//~~FOUO~~) In the context of online or other electronic communications or contacts, multiple [redacted]

18.6.13.3.1 *(U) Distinction Between Sensitive Circumstance and Sensitive Investigative Matter*

(U//~~FOUO~~) The term "sensitive investigative matter" as used in the AGG-Dom should not be confused with the term "sensitive circumstance" as that term is used in undercover operations or ELSUR matters. The term sensitive circumstance relates to a circumstance that arises in an undercover operation that requires the UCO to obtain FBIHQ approval. A comprehensive list of sensitive circumstances for criminal activities is contained in the *AGG-UCO* and [redacted] The Criminal Undercover Operations Review Committee (CUORC) and the [redacted] b7E must review and approve undercover operations that involve sensitive circumstances. The detailed policy for undercover operations is described in this section of the DIOG, the [redacted] 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//F~~OUO)~~ The risk that individuals engaged in undercover operations may become involved in illegal conduct;

E) (U//F~~OUO~~) The suitability of government participation in the type of activity that is expected to occur during the operation (*AGG-UCO*, Part IV.A); and

F) (U//~~FOUO~~) 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~~)

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

B) (U//F~~OUO~~) b7E

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

D) (U//~~FOUO~~

(U//~~FOUO~~)

E) (U//~~FOUO~~)

F) (U//~~FOUO~~)

G) (U//~~FOUO~~)

b7E

H) (U//~~FOUO~~)

I) (U//~~FOUO~~)

18.6.13.4.3 ***(U//~~FOUO~~) APPROVAL REQUIREMENTS FOR UCOs***

(U//~~FOUO~~)

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

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

b7E

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

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

If the matter involves religious or political organizations, the review must include participation by a representative of the DOJ NSD. (AGG-Dom, Section V; and

E) (U//~~FOUO~~)

F) (U//~~FOUO~~)

18.6.13.5 (U) [redacted] OIA IN UNDERCOVER OPERATIONS

b7E

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

A) (U) [redacted]

B) (U) [redacted]

(U//~~FOUO~~) *Note:* [redacted]

b7E

C) (U) [redacted]

D) (U) [redacted]

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

E) (U) [redacted]

b7E

F) (U) [redacted]

G) (U) [redacted]

H) (U) [redacted]

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

[81] (U) [redacted]

b7E

[82] (U) [redacted]

b7E

(U//~~FOUO~~

(U//~~FOUO~~

18.6.13.5.1 ***(U//~~FOUO~~) WRITTEN OPERATIONS ORDERS FOR CONTROLLED FIREARMS TRANSACTIONS***

(U) The controlled purchase, receipt, delivery, or sale of firearms can quickly escalate into violent confrontations and result in the death of, or serious bodily injury to, law enforcement personnel, subjects, or the general public. In an effort to mitigate foreseeable risks and to plan for contingencies, an agent or task force officer (TFO) must prepare a written FD-888 "Law Enforcement Operations Order" (OPORDER) for each planned firearms transaction conducted pursuant to subsection 18.6.13.5.B. Each OPORDER must address the five "SMEAC" categories that comprise the "Five Paragraph Order:"

A) (U) Situation

B) (U) Mission

C) (U) Execution

D) (U) Administration (e.g., equipment)

E) (U) Command & Control (e.g., communication)

(U) When the OPORDER drafter has knowledge that children or disabled individuals may be encountered during a planned operation, their potential presence must be accounted for in the same way as any other operational contingency.

(U//~~FOUO~~) The safety of law enforcement personnel and sound tactical judgment should always be paramount considerations when preparing an OPORDER. When FBI employees know that a planned operation involves a higher-than-normal risk, they must consult with an FBI SWAT team or the Critical Incident Response Group's (CIRG) Tactical Section. These elements may deploy for the operation in accordance with the *National Tactical Program Policy Guide* (1235PG), which contains the criteria for high risk operations and the parameters for mandatory use of a SWAT team or CIRG's Tactical Section resources. SWAT

teams and CIRG's Tactical Section are responsible for their own OPORDERs (rather than using the FD-888 template).

(U//~~FOUO~~) SACs (nondelegable) are the final approvers for OPORDERs drafted by field office employees pursuant to subsection 18.6.13.5.B. Prior to granting approval, SACs must seek CDC (or OGC) review and diligently review each OPORDER to ensure that careful and thorough planning has been conducted for each operation. They also must ensure that plans are adapted for the specific situation and include relevant details to enhance the safety and effectiveness of the employees involved in the operation. If a planned firearms transaction involves a significant amount of risk, but does not meet the risk threshold for mandatory deployment of a SWAT team or resources from CIRG's Tactical Section, the SAC is encouraged to consult with the SWAT senior team leader (STL) or a certified tactical instructor before approving the OPORDER. SACs may also ask other relevant subject matter experts (e.g., a principal firearms instructor) to review OPORDERs prior to approval.

(U//~~FOUO~~) Before executing a planned operation, the written OPORDER must be presented in an oral briefing to all employees involved. The briefer should cover all of the SMEAC categories and remind participants that the operation may become dangerous. An SAC may also require the SWAT STL, a certified tactical instructor, or the CDC to brief participating employees on tactics or the use of force policy (see Appendix F).

(U//~~FOUO~~) If appropriate under the circumstances, an SSA should notify local authorities of the planned operation in advance of its execution. Although the method, manner, and timing of this notification is left to the discretion of the SSA, he or 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) As soon as practicable, but no later than five business days after executing a planned operation, the OPORDER must be uploaded and serialized to the associated case file.

(U) In the event of exigent circumstances (i.e., an emergent and pressing necessity that requires immediate action), an SAC (nondelegable) may permit an abbreviated written operational plan and/or an oral briefing in lieu of a formal OPORDER. However, the abbreviated written operational plan and/or oral briefing must address all of the topics outlined in the FD-888, including the SMEAC categories. As applicable, the briefer should also remind participants about the use of force policy. As soon as practicable, but no later than five business days after executing a planned firearms transaction under exigent circumstances, an agent or TFO must document the following information in the associated case file: (1) the details of the operation (e.g., subject); (2) anyone encountered on scene; (3) the participating employees; and (4) the SAC's approval. b7E

(U//~~FOUO~~) For policy on required OPORDERs for searches and arrests, see subsections 18.7.1.6.1.6 and 19.2.3, respectively. These requirements also appear in subsection 17.5.3.1 in the context of OIA that is not part o

18.6.13.6 **(U) DURATION OF APPROVAL**

(U//~~FOUO~~) b7E

18.6.13.7 **(U) ADDITIONAL GUIDANCE**

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

B) (U//~~FOUO~~) b7E

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

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

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

(U//~~FOUO~~) All UCOs must provide an to b7E

18.7 (U) AUTHORIZED INVESTIGATIVE METHODS IN FULL INVESTIGATIONS

(U) 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 18.5.3.1)
4) (U) Online 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)[83]
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)

[83] (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.

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

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//F~~OUO~~) ***Application:*** 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//F~~OUO~~) 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; E.O. 12333 § 2.5; 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.

18.7.1.3 (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 [redacted] b7E

[redacted]

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

[redacted]

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 to 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 an 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 an 18 U.S.C. § 2703(d) court order without notice.

(U) [redacted] b7E

(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 to18 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 an 18 U.S.C. § 2703[d] order); 18 U.S.C. § 2711(3) (court of competent jurisdiction includes any federal court having jurisdiction over the offense being investigated without geographic limitation).

(U) Title 18 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).

18.7.1.3.4.5 ***(U) NO KNOCK WARRANTS***

(U) Pursuant to 18 USC 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 a search 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) Subject to the below exceptions, Agents must "knock and announce" even when they have reason to believe that doing so could result in the destruction of evidence.

(U) First, an agent may seek judicial authorization to conduct a "no knock" entry only if that agent has reasonable grounds to believe at the time the warrant is sought that knocking and announcing the agent's presence would create an imminent threat of physical violence to the agent and/or another person. b7E

(U) Second, if an agent did not anticipate the need for a "no knock" entry at the time the warrant was sought, the agent may conduct a "no knock" entry only if exigent circumstances arise at the scene such that knocking and announcing the agent's presence would create an imminent threat of physical violence to the agent and/or another person. b7E

(U)

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 (or successor system). This form should be completed by the FISA-designated Case Agent (See DIOG subsection 18.7.1.6.2.1 for a definition). b7E

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~~) [redacted] b7E

[redacted]

(U) 28 CFR § 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 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.

---

[84] Note: Due to an administrative error, the version of the DIOG released on September 17, 2021, prematurely included new requirements pertaining to the use of compulsory processes to obtain information from, or records of, members of the news media. As of October 25, 2021, those changes (including some that erroneously appeared on this page) have been reverted to the previous release of the DIOG, dated March 31, 2020. Additional updates about this topic are coming soon. Questions should be directed to CDCs or IPO.

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 OPERATIONS ORDERS FOR SEARCHES

(U) Law enforcement operations, such as searches and arrests, are inherently risky. These activities can quickly escalate into violent confrontations and result in the death of, or serious bodily injury to, law enforcement personnel, subjects, or the general public. In an effort to mitigate foreseeable risks and to plan for contingencies, an agent or task force officer (TFO) must prepare a written FD-888 "Law Enforcement Operations Order" (OPORDER) for each search conducted pursuant to subsection 18.7.1. Each OPORDER must address the five "SMEAC" categories that comprise the "Five Paragraph Order:"

A) (U) Situation

B) (U) Mission

C) (U) Execution

D) (U) Administration (e.g., equipment)

E) (U) Command & Control (e.g., communication)

(U) When the OPORDER drafter has knowledge that children or disabled individuals may be encountered during a search, their potential presence must be accounted for in the same way as any other operational contingency.

(U//~~FOUO~~) The safety of law enforcement personnel and sound tactical judgment should always be paramount considerations when preparing an OPORDER. When FBI employees know that a search involves a higher-than-normal risk, they must consult with an FBI SWAT team or the Critical Incident Response Group's (CIRG) Tactical Section. These elements may deploy for the operation in accordance with the *National Tactical Program Policy Guide* (1235PG), which contains the criteria for high risk operations and the parameters for mandatory use of a SWAT team or CIRG's Tactical Section resources. SWAT teams and CIRG's Tactical Section are responsible for their own OPORDERs (rather than using the FD-888 template).

(U//~~FOUO~~) SACs are the final approvers for OPORDERs drafted by field office employees.[85] Prior to granting approval, SACs must diligently review each OPORDER to ensure that careful and thorough planning has been conducted for each search. They also must ensure that plans are adapted for the specific situation and include relevant details to enhance the safety and effectiveness of the employees involved in the search. If a search involves a significant amount of risk, but does not meet the risk threshold for mandatory deployment of a SWAT team or resources from CIRG's Tactical Section, the SAC is encouraged to consult with the SWAT senior team leader (STL) or a certified tactical instructor before approving the OPORDER. An SAC may also seek legal advice from the CDC (or OGC) or ask other relevant subject matter experts (e.g., special agent bomb technicians [SABT], the Hazardous Evidence Response Team) to review an OPORDER prior to approval.

[85] (U//~~FOUO~~) The SAC's authority, as described throughout this subsection, is delegable in accordance with subsection 3.5.3.

(U//~~FOUO~~) Before executing a search, the written OPORDER must be presented in an oral briefing to all employees involved. The briefer should cover all of the SMEAC categories and remind participants that the operation may become dangerous. An SAC may also require the SWAT STL, a certified tactical instructor, or the CDC to brief participating employees on tactics or the use of force policy (see Appendix F).

(U//~~FOUO~~) If appropriate under the circumstances, an SSA should notify local authorities of the planned search in advance of its execution. Although the method, manner, and timing of this notification is left to the discretion of the SSA, he or 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) As soon as practicable, but no later than five business days after executing a search, the OPORDER must be uploaded and serialized to the associated case file.

(U) In the event of exigent circumstances (i.e., an emergent and pressing necessity that requires immediate action), an SAC may permit an abbreviated written operational plan and/or an oral briefing in lieu of a formal OPORDER. However, the abbreviated written operational plan and/or oral briefing must address all of the topics outlined in the FD-888, including the SMEAC categories. As applicable, the briefer should also remind participants about the use of force policy. As soon as practicable, but no later than five business days after executing a search under exigent circumstances, an agent or TFO must document the following information in the associated case file: (1) the details of the search (e.g., location); (2) anyone encountered on scene; (3) the participating employees; (4) the legal authority for the search; and (5) the SAC's approval.

(U) If an agent or TFO plans to participate in a search led by another agency, the SAC must ensure that all five SMEAC categories have been considered and addressed before the agent or TFO is allowed to participate. The SAC may review a non-FBI OPORDER or confirm this information or consult with the other agency, orally or in writing, prior to the search. The SAC's approval for an agent or TFO to participate in a search led by another agency must be documented in the applicable case file. Consistent with subsection 3.5.2.2, an SAC may provide oral approval, which must be documented in the applicable case file as soon as practicable but no later than five calendar days thereafter.

(U//~~FOUO~~) In addition to searches, duly approved OPORDERs are required for other law enforcement operations, including planned arrests (see subsection 19.2.3) and OIA related to the controlled purchase, receipt, delivery, or sale of firearms (see subsections 17.5.3.B and 18.6.13.5.B). OPORDERs may also be required for investigative activity outside of the United States, pursuant to the [redacted] b7E
[redacted] Field office management may discretionarily require OPORDERs for other routine operations, as well. When multiple activities are planned as a concurrent operation (e.g., a search and arrest), only one OPORDER covering all of those activities is required.

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). The federal officer who serves as the declarant for the FISA application should be the FISA-designated Case Agent. See the *Foreign Intelligence Surveillance Act and Standard Minimization Procedures Policy Guide,* (1242PG), for additional guidance on specific roles and responsibilities.

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) Title 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, contact your assigned [redacted] b7E

[redacted]

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). In addition, queries of information acquired pursuant to a FISA order for physical search must comply with the appropriate query standard and other querying requirements, including any applicable pre-approval requirements for sensitive queries, such as for queries related to members of Congress or U.S.-based members of the news media. See the *Foreign Intelligence Surveillance Act and Standard Minimization Procedures Policy Guide* (1303PG) [links to a SECRET//NOFORN//LES document] for additional guidance on FISA physical search requirements.

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

[redacted]

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

[redacted]

A) (U//~~FOUO~~) Each investigative file for which an application is or has been prepared for submission to the FISC must include a FISA Accuracy "FISA ACCUR" sub-file [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~~)

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

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

b7E

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

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

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~~)** b7E

(U//F~~OUO~~)

A) (U//F~~OUO~~)

B) (U//F~~OUO~~)

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

(U//F~~OUO~~)

(U//F~~OUO~~) b7E

(U//F~~OUO~~)

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

(U//F~~OUO~~)

b7E

18.7.1.6.2.11 **(U) COMPLIANCE AND MONITORING FOR FISA**

(U//F~~OUO~~)

18.7.1.6.2.12 **(U) FISA OVERCOLLECTION**

(U//~~FOUO~~ [redacted] b7E

[redacted] or contact NSCLB 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; (iii) consultation with the Technical Advisor (TA) or a designated TTA to determine feasibility, applicability, and use of the appropriate equipment and (iv) if there is a reasonable likelihood of collecting non-English language material, consult with the Foreign Language Program Coordinator to determine if sufficient foreign language translation capability is available to process the collection.

(U//F~~OUO~~) ***Application*** [redacted] b7E
[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) Based upon the U.S. Supreme Court decision, *Dahda v. United States*, DOJ policy requires the Title III order(s) be obtained only in the district where the wireroom/monitoring room is located, per 18 USC 2518(3). This is to ensure the interceptions occur within the authorizing court's jurisdiction.

(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~~) A special agent in charge (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. The SAC's approval for the use of a nonsensitive Title III must be documented with an EC and serialized into the appropriate investigative ELSUR subfile. Any delegation of SAC approval authority to an ASAC under this section must be in writing (See DIOG Section 3.5.3).

(U//~~FOUO~~) CDC 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. 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[86]

(U//F~~OUO~~) 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. As with nonsensitive Title IIIs, an SAC must approve the use of this investigative method to ensure that field office managers will allocate the resources necessary and that approval must be documented with an EC and serialized into the appropriate investigative ELSUR subfile. As part of that process, 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.

[86] Note: Due to an administrative error, the version of the DIOG released on September 17, 2021, prematurely included new requirements pertaining to the use of compulsory processes to obtain information from, or records of, members of the news media. As of October 25, 2021, those changes (including some that erroneously appeared on this page) have been reverted to the previous release of the DIOG, dated March 31, 2020. Additional updates about this topic are coming soon. Questions should be directed to CDCs or IPO.

(U//~~FOUO~~) The field office must include a copy of the completed FD-926 "Chief Division Counsel (CDC) Title III Checklist" 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//F~~OUO~~) "Emergency" Title III interceptions (i.e., interceptions conducted prior to judicial approval under 18 U.S.C. § 2518(7)); or

B) (U//F~~OUO~~) 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) Title 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.

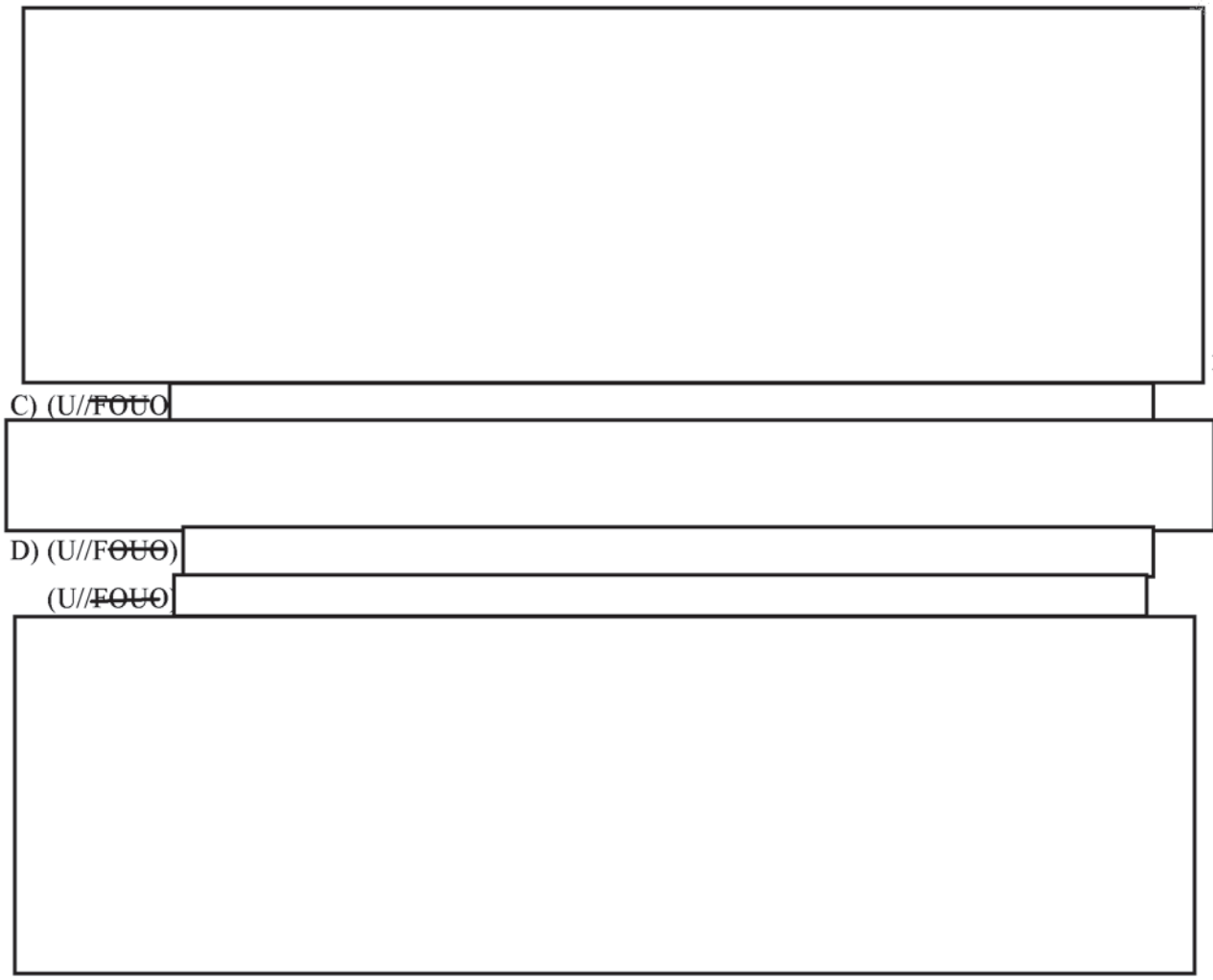
(U//~~FOUO~~) In all but the most unusual circumstances, the only situations likely to constitute an emergency by the Department of Justice (DOJ) are those involving an imminent threat to life, e.g., a kidnapping, hostage taking, or imminent terrorist activity.

18.7.2.7.1 *(U) OBTAINING EMERGENCY AUTHORIZATION*

(U//~~FOUO~~)

A) (U//~~FOUO~~) b7E

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



b7E

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

D) (U//F~~OUO~~)

(U//~~FOUO~~)

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 which must reflect the date and time of the emergency authorization. b7E

(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~~) b7E

(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~~)

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

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

C) (U//~~FOUO~~) b7E

(U//~~FOUO~~)

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

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

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

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

(U//~~FOUO~~) Title 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.

(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 **o**f 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 ELSUR Data Application (EDA) system and the systems of other appropriate agencies, must be conducted in accordance with the requirements of Appendix H. 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.

(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 at least 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

[redacted]

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) Title III – Documenting, Reporting, and Notice Requirements

18.7.2.12.1 *(U//~~FOUO~~)* [redacted]

(U//~~FOUO~~) [redacted] b7E

[redacted]

18.7.2.12.2 *(U//~~FOUO~~) Serializing Title III Documents*

(U//~~FOUO~~) [redacted] b7E

[redacted]

b7E

(U//F~~OUO~~

(U//F~~OUO~~) The responsibilities set forth in this subsection also apply to joint Title III operations, as set forth in subsection 18.7.2.13.

18.7.2.12.3 ***(U//~~FOUO~~)***

(U//F~~OUO~~

18.7.2.12.4 ***(U//~~FOUO~~)***

b7E

(U//~~FOUO~~)

18.7.2.12.5 ***(U//~~FOUO~~)***

(U//F~~OUO~~)

b7E

(U//~~FOUO~~

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

(U//~~FOUO~~) The anticipated interception of conversations related to a SIM, as defined in DIOG Section 10, requires notice to the appropriate FBIHQ unit chief and section chief, and the DOJ Criminal Division. ***Note:*** A SIM is not the same as a "sensitive circumstance" described in DIOG subsection 18.7.2.6.

18.7.2.12.7 ***(U//F~~OUO~~)***

(U//F~~OUO~~)

b7E

(U//F~~OUO~~)

(U//F~~OUO~~)

18.7.2.12.8 ***(U//F~~OUO~~) TITLE III WIRETAP REPORT***

18.7.2.12.8.1 **(U//F~~OUO~~) REPORTING WIRETAP INFORMATION TO DOJ**

(U//F~~OUO~~) The DOJ is required to provide a report containing information regarding Title III orders and applications to the Administrative Office of the United States Courts (AOUSC), as delineated in 18 U.S.C. § 2519(2). Pursuant to 18 U.S.C. § 2519(3), the AOUSC transmits a full and complete report pertaining to applications for orders authorizing or approving the interception of wire, oral, or electronic communications to Congress.

(U//F~~OUO~~) In support of DOJ's statutory obligation

b7E

18.7.2.12.8.2 **(U//F~~OUO~~)**

(U//F~~OUO~~)

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

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

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

18.7.2.12.8.3 **(U//~~FOUO~~)** b7E

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

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

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

18.7.2.12.8.4 **(U//~~FOUO~~)** b7E

(U//~~FOUO~~)

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~~) Example: The FBI and DEA are jointly conducting an investigation into a drug trafficking organization, and a federal wiretap order is being sought for a phone used by a suspected drug trafficker. The affiant on the initial affidavit is a DEA agent, and the DEA will administer the wiretap. Because the FBI is a joint participant in the investigation and execution, a copy of the Title III pleadings must be provided to the FBI (i.e., items (i) – (iii) and (v) in DIOG section 18.7.2.12). After thirty days, an extension of interceptions is sought, and an FBI agent is the affiant for the extension affidavit. The DEA may continue to be the administering agency for purposes of the extension affidavit, and a copy of the pleadings must again be provided to the FBI. Similarly, where the installation is being administered by the FBI, the FBI may continue to serve as the administering agency even if a DEA agent serves as an affiant on an extension or other related application.

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 Sentinel.

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***

(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) Title 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] (or successor system). 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~~) b7E

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 (or successor system) on the NSCLB Resource BuNET Page. b7E

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

(U//~~FOUO~~)

(U//~~FOUO~~)

(U//~~FOUO~~) b7E

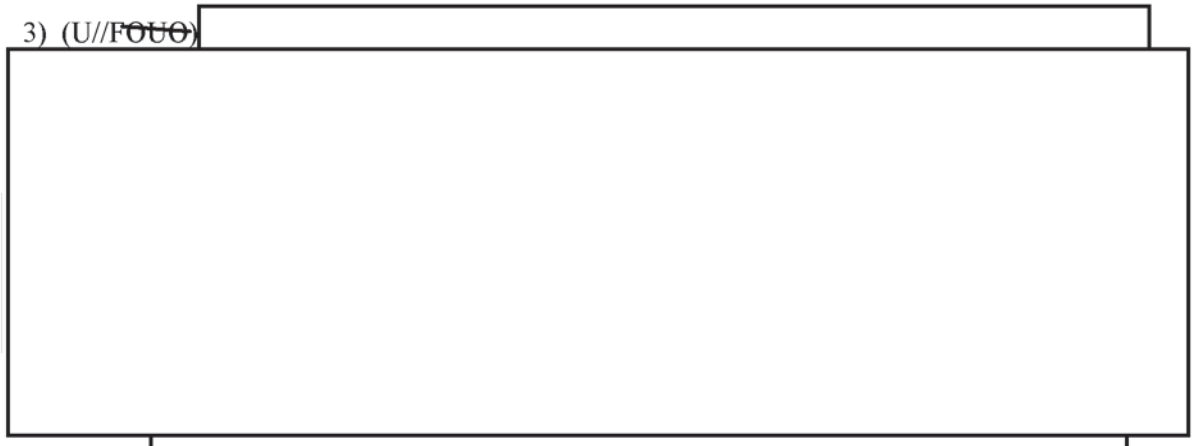
(U//~~FOUO~~)

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

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



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



b7E

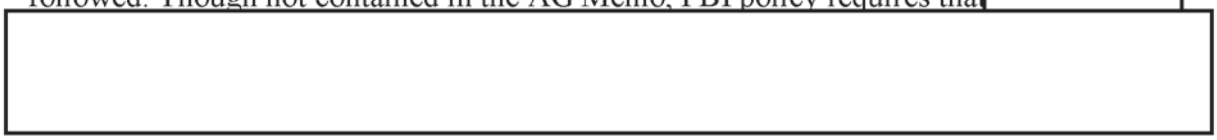
B) (U//~~FOUO~~



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

b7E



(U//F~~OUO~~) 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//F~~OUO~~)

b7E

A) (U//F~~OUO~~)

B) (U//F~~OUO~~)

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

(U//~~FOUO~~)

(U//F~~OUO~~)

b7E

(U//F~~OUO~~)

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

(U//~~FOUO~~)

b7E

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

(U//~~FOUO~~)

18.7.3.2.7 ***(U) COMPLIANCE AND MONITORING FOR FISA***

(U//~~FOUO~~ b7E

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~~

b7E

or contact NSCLB for guidance regarding the handling of any FISA overcollection.

18.7.3.2.10 ***(U) OTHER APPLICABLE POLICIES***

- (U//~~FOUO~~) *Counterintelligence Division Policy Directive and Policy Guide* (0717DPG) [~~links to SECRET//NOFORN/FISA document~~]
- (U//~~FOUO~~) *Counterterrorism Policy Guide* (1131DPG) [links to S~~ECRET//NOFORN//LES/SSI~~ document]

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 Sentinel.

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

(U//~~FOUO~~

b7E

(U//~~FOUO~~)

b7E

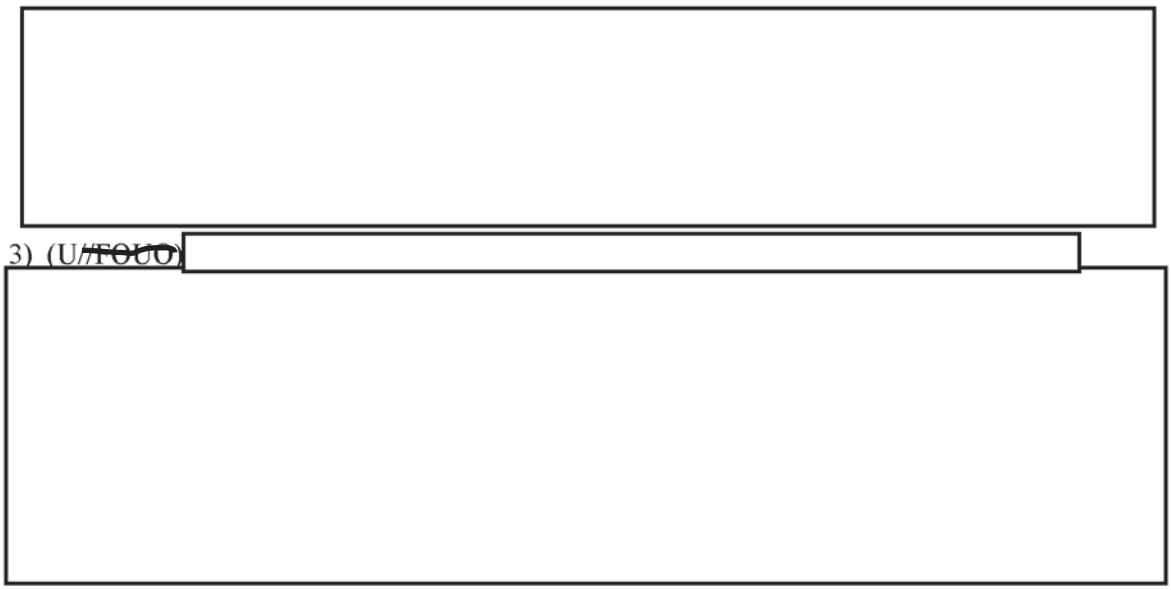
(U//~~FOUO~~)

(U//~~FOUO~~)

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

b7E

2) (U)



b7E

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. Note that any information obtained pursuant to an order under Title VII of FISA must be handled according to the minimization and querying procedures for such information, including the query standard and any applicable pre-approval requirements for sensitive queries, such as for queries related to members of Congress or U.S.-based members of the news media. See the *Foreign Intelligence Surveillance Act and Standard Minimization Procedures Policy Guide* (1303PG) [~~links to a SECRET//NOFORN//LES~~ document] for additional guidance.

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 agents[87] 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

[87] (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.

may have a significant impact on an investigation in another field office or when the arrest is 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 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) WRITTEN OPERATIONS ORDERS FOR PLANNED ARRESTS*

(U) Law enforcement operations, such as searches and arrests, are inherently risky. These activities can quickly escalate into violent confrontations and result in the death of, or serious bodily injury to, law enforcement personnel, subjects, or the general public. In an effort to mitigate foreseeable risks and to plan for contingencies, an agent or task force officer (TFO) must prepare a written FD-888 "Law Enforcement Operations Order" (OPORDER) for each planned arrest scenario. Each OPORDER must address the five "SMEAC" categories that comprise the "Five Paragraph Order:"

A) (U) Situation

B) (U) Mission

C) (U) Execution

D) (U) Administration (e.g., equipment)

E) (U) Command & Control (e.g., communication)

(U) When the OPORDER drafter has knowledge that children or disabled individuals may be encountered during a planned arrest, their potential presence must be accounted for in the same way as any other operational contingency.

(U//~~FOUO~~) The safety of law enforcement personnel and sound tactical judgment should always be paramount considerations when preparing an OPORDER. When FBI employees know that a planned arrest involves a higher-than-normal risk, they must consult with an FBI SWAT team or the Critical Incident Response Group's (CIRG) Tactical Section. These elements may deploy for the operation in accordance with the *National Tactical Program Policy Guide* (1235PG), which contains the criteria for high risk operations and the parameters for mandatory use of a SWAT team or CIRG's Tactical Section resources. SWAT teams and CIRG's Tactical Section are responsible for their own OPORDERs (rather than using the FD-888 template).

(U//~~FOUO~~) SACs are the final approvers for OPORDERs drafted by field office employees.[88] Prior to granting approval, SACs must diligently review each OPORDER to ensure that careful

[88] (U//~~FOUO~~) The SAC's authority, as described throughout this subsection, is delegable in accordance with subsection 3.5.3.

and thorough planning has been conducted for each planned arrest. They also must ensure that plans are adapted for the specific situation and include relevant details to enhance the safety and effectiveness of the employees involved in the arrest. If a planned arrest involves a significant amount of risk, but does not meet the risk threshold for mandatory deployment of a SWAT team or resources from CIRG's Tactical Section, the SAC is encouraged to consult with the SWAT senior team leader (STL) or a certified tactical instructor before approving the OPORDER. An SAC may also seek legal advice from the CDC (or OGC) or ask other relevant subject matter experts (e.g., special agent bomb technicians [SABT], the Hazardous Evidence Response Team) to review an OPORDER prior to approval.

(U//F~~OUO~~) Before executing a planned arrest, the written OPORDER must be presented in an oral briefing to all employees involved. The briefer should cover all of the SMEAC categories and remind participants that the operation may become dangerous. An SAC may also require the SWAT STL, a certified tactical instructor, or the CDC to brief participating employees on tactics or the use of force policy (see Appendix F).

(U) (U//~~FOUO~~) If appropriate under the circumstances, an SSA should notify local authorities of the planned arrest in advance of its execution. Although the method, manner, and timing of this notification is left to the discretion of the SSA, he or 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) (U) As soon as practicable, but no later than five business days after executing a planned arrest, the OPORDER must be uploaded and serialized to the associated case file.

(U) (U) In the event of exigent circumstances (i.e., an emergent and pressing necessity that requires immediate action), an SAC may permit an abbreviated written operational plan and/or an oral briefing in lieu of a formal OPORDER. However, the abbreviated written operational plan and/or oral briefing must address all of the topics outlined in the FD-888, including the SMEAC categories. As applicable, the briefer should also remind participants about the use of force policy. As soon as practicable, but no later than five business days after executing a planned arrest under exigent circumstances, an agent or TFO must document the following information in the associated case file: (1) the details of the arrest (e.g., subject); (2) anyone encountered on scene; (3) the participating employees; (4) the legal authority for the arrest; and (5) the SAC's approval. *Note*: this after-action documentation requirement for exigent circumstances applies to planned arrests with a warrant; for policy on arrests *without* warrants, see subsection 19.3.

(U) If an agent or TFO plans to participate in a planned arrest led by another agency, the SAC must ensure that all five SMEAC categories have been considered and addressed before the agent or TFO is allowed to participate. The SAC may review a non-FBI OPORDER or confirm this information or consult with the other agency, orally or in writing, prior to the planned arrest. The SAC's approval for an agent or TFO to participate in a planned arrest led by another agency must be documented in the applicable case file. Consistent with subsection 3.5.2.2, an SAC may provide oral approval, which must be documented in the applicable case file as soon as practicable but no later than five calendar days thereafter.

(U//F~~OUO~~) In addition to arrests, duly approved OPORDERs are required for other law enforcement operations, including searches (see subsection 18.7.1.6.1.6) and OIA related to the controlled purchase, receipt, delivery, or sale of firearms (see subsections 17.5.3.B and 18.6.13.5.B). OPORDERs may also be required for investigative activity outside of the United States, pursuant to the *International Operations Division Policy Guide* (1102PG) [links to a ~~SECRET//NOFORN~~ document]. Field office management may discretionarily require OPORDERs for other routine operations, as well. When multiple activities are planned as a concurrent operation (e.g., a search and arrest), only one OPORDER covering all of those activities is required.

19.2.4 *(U) ARREST TECHNIQUES – GENERAL*

(U) b7E

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

(U) b7E

b7E

(U)

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)

b7E

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)

b7E

b7E

(U) Search incident to arrest authority does not extend to digital information on a cell phone or other personal electronic device seized from an arrestee. See DIOG subsection 19.7.2 below for additional guidance on searches incident to arrest. The FBI vehicle should be searched both before and immediately after the transportation of any subject.

(U)

(U) When an agent knows or reasonably should know that the individual to be transported has a disability, the disability must be considered as a factor in employing reasonable judgement under the circumstances.

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

b7E

(U)

(U)

(U) When an agent knows or reasonably should know that the individual to be searched has a disability, the disability must be considered as a factor in employing reasonable judgement under the circumstances.

19.2.4.5 (U) TRANSPORTATION OF ARRESTED PERSONS

(U)

(U)

(U)

b7E

(U) When an agent knows or reasonably should know that the individual to be searched has a disability, the disability must be considered as a factor in employing reasonable judgement under the circumstances.

(U) For specific requirements to transport a federal prisoner from a detention facility in which he/she is housed, see DIOG Appendix C.7.

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 *Procedures for Eyewitness Identification of Suspects Policy Guide* (1047PG) for guidance on gathering eyewitness identifications of suspects during an investigation.

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 for a serious offense (felony or violent misdemeanor) and immediate action by the agent is necessary to prevent escape, serious bodily injury, or destruction of property.

(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 interviewed, when appropriate. If fingerprints are taken in the field office, the arresting agent(s) or TFO(s) must use the electronics JABS system or ARES application and enter all appropriate and known arrest information, including the Identity History Summary.

(U) Field offices are not required to submit the case disposition information to the CJIS Division; however, field offices may elect to submit case disposition information to CJIS by following the instructions on Form R-84. If the arresting agent(s) or TFO(s) cannot submit the arrestee's fingerprints electronically through JABS or ARES, the FD-249 "Criminal Fingerprint" card may be used as an alternative means to submit fingerprints to CJIS. The arresting agent(s) or TFO(s) must complete all known fields on the FD-249 card.

(U [redacted]
(See DIOG subsection 18.5.6.4.17 for guidance [redacted] 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. b7E

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 titled, "Authorization of DNA Collection from Arrestees and Detainees" (November 2009) (319T-HQ-A1487667-LAB serial 1458).

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) b7E

(U) See DOJ policy on the use of force *(DIOG* Appendix *F)*, and the *Less-Than-Lethal Devices Policy Guide* (1111PG).

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.

(U) When an agent knows or reasonably should know that the individual to be restrained has a disability, the disability must be considered as a factor in employing reasonable judgement under the circumstances in the use of restraining devices.

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 USC 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) Subject to the below exceptions, Agents must "knock and announce" even when they have reason to believe that doing so could result in the destruction of evidence.

(U) First, an agent may seek judicial authorization to conduct a "no knock" entry only if that agent has reasonable grounds to believe at the time the warrant is sought that knocking and announcing the agent's presence would create an imminent threat of physical violence to the agent and/or another person

b7E

(U) Second, if an agent did not anticipate the need for a "no knock" entry at the time the warrant was sought, the agent may conduct a "no knock" entry only if exigent circumstances arise at the scene such that knocking and announcing the agent's presence would create an imminent threat of physical violence to the agent and/or another person.

(U

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)

(U)

b7E

(U)

(U)

b7E

(U)

(U) See also DIOG subsection 18.6.12.4.1.D for guidance on inventory searches generally.

(U) The following two examples illustrate circumstances under which an inventory search could be conducted:

A) *Example:* (U)

b7E

B) *Example:* (U)

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

A) *Example:* (U)

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

(U) **Mandatory Notification Countries or Jurisdictions**

Antigua and Barbuda	Hong Kong[89]	Saint Vincent and the Grenadines
Armenia	Hungary	Seychelles
Azerbaijan	Jamaica	Sierra Leone
Bahamas	Kazakhstan	Singapore
Barbados	Kiribati	Slovakia
Belarus	Kuwait	Tajikistan
Belize	Kyrgyzstan	Tanzania
Brunei	Malaysia	Tonga
Bulgaria	Malta	Trinidad and Tobago
China[90]	Mauritius	Tunisia
Costa Rica	Moldova	Turkmenistan
Cyprus	Mongolia	Tuvalu
Czech Republic	Nigeria	Ukraine
Dominica	Philippines	United Kingdom[91]
Fiji	Poland (non-permanent residents only)	

[89] (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.

[90] (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.

[91] (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.

(U) **Mandatory Notification Countries or Jurisdictions**

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 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 CFR § 50.10.

(U) *Note:* 28 CFR § 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 CFR § 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

(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] is then responsible for seeking DAAG approval as set forth in 28 CFR 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] as soon as practicable [redacted] after the making the oral request. The [redacted] is responsible to prepare the appropriate written b7E

documentation to DOJ, including documenting the receipt of AG approval. This documentation must be electronically placed into the case file.

(U) See also the AG Memorandum "Updated Policy Regarding Obtaining Information From, or Records Of, Members of the News Media; and Regarding Questioning, Arresting, or Charging Member of the News Media" (February 2014), 28 CFR § 50.10, and the AG Memoranudm "Updated Policy Regarding Obtaining Information From, or Records Of, Members of the News Media; and Regarding Questioning, Arressting, Or Charging Member of the News Media" (January 2015).

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

(U) Arrests of juveniles for federal offenses are subject to the provisions of the Juvenile Delinquency Act.

19.12.1 *(U) DEFINITION OF JUVENILE DELINQUENCY*

(U) An act of juvenile delinquency is defined as a violation of 18 U.S.C. § 922(x)(2) or a violation of a federal law by an individual who has not attained his or her 18th birthday, which would have been a crime if committed by an adult. For the purpose of juvenile delinquency proceedings, a juvenile delinquent (or juvenile subject) is an individual who committed a crime before his or her 18th birthday who has not attained his or 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. See subsections 19.1-19.9. After arrest, however, the Federal Juvenile Delinquency Act requires strict compliance with the following procedures:

A) (U) **Advice of Rights and Interview**- 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 "Advice of Rights" meet this

requirement. As described in subsection 18.5.6.4.14, 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. See subsection 18.5.6.4.14 for complete policy requirements on interviewing juvenile subjects.

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. Absent exigent circumstances, FBI employees must allow a parent, guardian, or custodian access to the juvenile if requested by either party.

C) (U) **Initial Appearance before Magistrate Judge -** Subsequent to his/her arrest, the juvenile must be taken to a magistrate judge forthwith. If no magistrate judge is immediately available, the juvenile must be taken to a magistrate without undue delay.

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) **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.

F) (U) **DNA Collection** - Agents must not take DNA samples from juveniles at the time of arrest.

G) (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.

20 (U) OTHER INVESTIGATIVE RESOURCES

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~~)*

b3
b7E

(U) See Section 20.2 below.

20.1.2 *(U//~~FOUO~~)*

(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~~)

b3
b7E

(U//~~FOUO~~)

20.2.1 *(U) AUTHORIZED INVESTIGATIVE ACTIVITY*

(U//~~FOUO~~)

b3
b7E

(U) See

20.3 (U//~~FOUO~~)

(U//~~FOUO~~)

20.3.1 *(U) AUTHORIZED INVESTIGATIVE ACTIVITY*

(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), through its Behavior Analysis Units (BAUs), manages and directs the FBI's operational behavioral support across all investigative programs. In addition, the NCAVC's BAUs 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, cyber, 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 appropriate BAU. 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 [redacted] b7E

[redacted]

20.5.1 *(U) AUTHORIZED INVESTIGATIVE ACTIVITY*

(U[redacted]

[redacted] b7E

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

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

20.6 (U//~~FOUO~~) [redacted] b7E

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

20.6.1 *(U) AUTHORIZED INVESTIGATIVE ACTIVITY*

(U//~~FOUO~~)

b7E

This Page is Intentionally Blank.

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 a CEM that is responsive to a PFI, FBI, or IC collection requirement, but is not related to the topic, purpose or objective(s), of that specific investigation, Assessment, or CEM.

(U//~~FOUO~~) Incidentally collected information, responsive to the above-mentioned collection requirements, may also be derived from b7E

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

(U//~~FOUO~~) b7E

(U//~~FOUO~~)

(U//~~FOUO~~)

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//F~~OUO~~)

b7E

(U) For example:

A) (U//F~~OUO~~)

b7E

B) (U//F~~OUO~~)

C) (U//F~~OUO~~)

(U//F~~OUO~~) 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. The FBI is authorized to open an Assessment (or a Full Investigation) to collect on a USIC intelligence requirement only if it has been accepted and designated by FBIHQ DI as a PFI Collection Requirement, as specified in DIOG Section 9.

(U//F~~OUO~~)

b7E

(U//F~~OUO~~)

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 [redacted] b7E

[redacted]

This Page is Intentionally Blank.

A APPENDIX 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]

PREAMBLE

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

TABLE OF CONTENTS

INTRODUCTION 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

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

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

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

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,

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).)

> 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

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.

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

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.

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

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.

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

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.

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

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

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

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

A. ASSESSMENTS

1. Purposes

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

2. Approval

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

3. Authorized Activities

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

a. seeking information, proactively or in response to investigative leads, relating to:

   i. activities constituting violations of federal criminal law or threats to the national security,

   ii. the involvement or role of individuals, groups, or organizations in such activities; or

   iii. matters of foreign intelligence interest responsive to foreign intelligence requirements;

b. identifying and obtaining information about potential targets of or vulnerabilities to criminal activities in violation of federal law or threats to the national security;

c. seeking information to identify potential human sources, assess the suitability, credibility, or value of individuals as human sources, validate human sources, or maintain the cover or credibility of human sources, who may be able to provide or obtain information relating to criminal activities in violation of federal law, threats to the national security, or matters of foreign intelligence interest; and

d. obtaining information to inform or facilitate intelligence analysis and planning as described in Part IV of these Guidelines.

4. Authorized Methods

Only the following methods may be used in assessments:

a. Obtain publicly available information.

b. Access and examine FBI and other Department of Justice records, and obtain information from any FBI or other Department of Justice personnel.

c. Access and examine records maintained by, and request information from, other federal, state, local, or tribal, or foreign governmental entities or agencies.

d. Use online services and resources (whether nonprofit or commercial).

e. Use and recruit human sources in conformity with the Attorney General's Guidelines Regarding the Use of FBI Confidential Human Sources.

f. Interview or request information from members of the public and private entities.

g. Accept information voluntarily provided by governmental or private entities.

h. Engage in observation or surveillance not requiring a court order.

i. Grand jury subpoenas 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. PREDICATED INVESTIGATIONS

1. Purposes

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

2. Approval

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

3. Circumstances Warranting Investigation

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

a. An activity constituting a federal crime or a threat to the national security has or may have occurred, is or may be occurring, or will or may occur and the investigation may obtain information relating to the activity or the involvement or role of an individual, group, or organization in such activity.

b. An individual, group, organization, entity, information, property, or activity is or may be a target of attack, victimization, acquisition, infiltration, or recruitment in connection with criminal activity in violation of federal law or a threat to the national security and the investigation may obtain information that would help to protect against such activity or threat.

c. The investigation may obtain foreign intelligence that is responsive to a foreign intelligence requirement.

4. Preliminary and Full Investigations

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

a. Preliminary investigations

i. Predication Required for Preliminary Investigations

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

ii. Duration of Preliminary Investigations

A preliminary investigation must be concluded within six months of its initiation, which may be extended by up to six months by the Special Agent in Charge[1]. Extensions of preliminary investigations beyond a

[1] Special Agents in Charge may allow Assistant Special Agents in Charge to authorize extension of time for concluding preliminary investigations by up to six months consistent with FBI policy. 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.

year must be approved by FBI Headquarters.

iii. Methods Allowed in Preliminary Investigations

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

b. Full Investigations

i. Predication Required for Full Investigations

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

ii. Methods Allowed in Full Investigations

All lawful methods may be used in a full investigation.

5. Notice Requirements

a. An FBI field office shall notify FBI Headquarters and the United States Attorney or other appropriate Department of Justice official of the initiation by the field office of a predicated investigation involving a sensitive investigative matter. If the investigation is initiated by FBI Headquarters, FBI Headquarters shall notify the United States Attorney or other appropriate Department of Justice official of the initiation of such an investigation. If the investigation concerns a threat to the national security, an official of the National Security Division must be notified. The notice shall identify all sensitive investigative matters involved in the investigation.

b. The FBI shall notify the National Security Division of:

i. the initiation of any full investigation of a United States person relating to a threat to the national security; and

ii. the initiation of any full investigation that is based on paragraph 3.c. (relating to foreign intelligence).

c. The notifications under subparagraphs a. and b. shall be made as soon as practicable, but no later than 30 days after the initiation of an investigation.

d. The FBI shall notify the Deputy Attorney General if FBI Headquarters disapproves a field office's initiation of a predicated investigation relating to a threat to the

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

C. ENTERPRISE INVESTIGATIONS

1. Definition

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

a. a pattern of racketeering activity as defined in 18 U.S.C. 1961(5);

b. international terrorism or other threat to the national security;

c. domestic terrorism as defined in 18 U.S.C. 2331(5) involving a violation of federal criminal law;

d. furthering political or social goals wholly or in part through activities that involve force or violence and a violation of federal criminal law; or

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

2. Scope

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

3. Notice and Reporting Requirements

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

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.

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. fu 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

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.

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

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.

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.

V. AUTHORIZED METHODS

A. PARTICULAR METHODS

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

1. The methods described in Part II.A.4 of these Guidelines.

2. Mail covers.

3. Physical searches of personal or real property where a warrant or court order is not legally required because there is no reasonable expectation of privacy (e.g., trash covers).

4. Consensual monitoring of communications, including consensual computer monitoring, subject to legal review by the Chief Division Counsel or the FBI Office of the General Counsel. Where a sensitive monitoring circumstance is involved, the monitoring must be approved by the Criminal Division or, if the investigation concerns a threat to the national security or foreign intelligence, by the National Security Division.

5. Use of closed-circuit television, direction finders, and other monitoring devices, subject to legal review by the Chief Division Counsel or the FBI Office of the General Counsel. (The methods described in this paragraph usually do not require court orders or warrants unless they involve physical trespass or non-consensual monitoring of communications, but legal review is necessary to ensure compliance with all applicable legal requirements.)

6. Polygraph examinations.

7. Undercover operations. In investigations relating to activities in violation of federal criminal law that do not concern threats to the national security or foreign intelligence, undercover operations must be carried out in conformity with the Attorney General's Guidelines on Federal Bureau of Investigation Undercover Operations. In investigations that are not subject to the preceding sentence because they concern threats to the national security or foreign intelligence, undercover operations involving religious or political organizations must be reviewed and approved by FBI Headquarters, with participation by the National Security Division in the review process.

8. Compulsory process as authorized by law, including grand jury subpoenas and other subpoenas, National Security Letters (15 U.S.C. 1681u, 1681v; 18 U.S.C. 2709; 12

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

9. Accessing stored wire and electronic communications and transactional records in conformity with chapter 121 of title 18, United States Code (18 U.S.C. 2701- 2712).

10. Use of pen registers and trap and trace devices in conformity with chapter 206 of title 18, United States Code (18 U.S.C. 3121-3127), or the Foreign Intelligence Surveillance Act (50 U.S.C. 1841-1846).

11. Electronic surveillance in conformity with chapter 119 of title 18, United States Code (18 U.S.C. 2510-2522), the Foreign Intelligence Surveillance Act, or Executive Order 12333 § 2.5.

12. Physical searches, including mail openings, in conformity with Rule 41 of the Federal Rules of Criminal Procedure, the Foreign Intelligence Surveillance Act, or Executive Order 12333 § 2.5. A classified directive provides additional limitation on certain searches.

13. Acquisition of foreign intelligence information in conformity with title VII of the Foreign Intelligence Surveillance Act.

B. SPECIAL REQUIREMENTS

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

1. Contacts with Represented Persons

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

2. Use of Classified Investigative Technologies

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

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

C. OTHERWISE ILLEGAL ACTIVITY

1. Otherwise illegal activity by an FBI agent or employee in an undercover operation relating to activity in violation of federal criminal law that does not concern a threat to the national security or foreign intelligence must be approved in conformity with the Attorney General's Guidelines on Federal Bureau of Investigation Undercover Operations. Approval of otherwise illegal activity in conformity with those guidelines is sufficient and satisfies any approval requirement that would otherwise apply under these Guidelines.

2. Otherwise illegal activity by a human source must be approved in conformity with the Attorney General's Guidelines Regarding the Use of FBI Confidential Human Sources.

3. Otherwise illegal activity by an FBI agent or employee that is not within the scope of paragraph 1. must be approved by a United States Attorney's Office or a Department of Justice Division, except that (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 following:

   a. otherwise illegal activity that would not be a felony under federal, state, local, territorial, or tribal law;

   b. the controlled[2] 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 the true ownership of a proprietary, but not including sworn testimony;

   f. conducting money laundering transactions (including acting as an

[2] In a controlled transaction, the item(s) will be monitored by the FBI and retained or seized at the conclusion of the transaction.

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

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.

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

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.

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

specially 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

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

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.

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. 168lv 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. 168lu(f); 18 U.S.C. 2709(d); 50 U.S.C. 436(e).

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

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.

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

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

B APPENDIX B: (U) EXECUTIVE ORDER 12333

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

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

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

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

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;

(5) 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:

(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

originating Intelligence Community element or the head of the originating department, declassify, or direct the declassification of, information or 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 tradecraft 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

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

(B) Mission Managers shall serve as principal substantive advisors 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

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

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

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

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.

(e) 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

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

under the leadership of the Director, as specified in such 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;

(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(b)(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,

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

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 29, 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 directive;

(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

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

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;

(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(i) 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

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.

(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)(6), and 1.10(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

sections 1.3(b)(4), 1.7(a)(6), and 1.10(i) 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

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.

(i) 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.

(j) 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.

1.8 *The Department of State.* In addition to the authorities

exercised by the Bureau of Intelligence and Research under sections 1.4 and 1.7(i) 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(i) 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

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 (21) 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) though (i) above, and to support the Intelligence Community elements of the Department of

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 those 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;

(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,

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

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

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;

(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,

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

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

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

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

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 nonelectronic 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

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

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.

(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

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//F~~OUO~~) **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//F~~OUO~~) **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 (see DOJ Criminal Division memorandum *Use and Targeting of Federal Prisoners in Investigations* [January 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] See subsection C.4.1 for approval requirements. 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]

(U//~~FOUO~~) [redacted] The process is as follows:

A) (U//~~FOUO~~) The FBI field office employee must: b7E

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

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

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

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

5) (U//~~FOUO~~)

6) (U//~~FOUO~~)

b7E

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

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

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

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

4) (U//~~FOUO~~)

(U//~~FOUO~~) *Note*:

(U//~~FOUO~~)

(U//~~FOUO~~)

b7E

(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.

C.4.2 *(U) APPROVAL - INTERVIEW A FEDERAL PRISONER*

(U//~~FOUO~~) The FBI employee must:

b7E

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

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

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

C.5 (U) EXEMPTIONS TO DOJ APPROVAL REQUIREMENT

(U//~~FOUO~~)

b7E

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

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

1) (U//~~FOUO~~)
2) (U//~~FOUO~~)
3) (U//~~FOUO~~)
4) (U//~~FOUO~~)

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

b7E

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

(U) *Note:*

(U//~~FOUO~~)

A) (U//~~FOUO~~)
B) (U//~~FOUO~~)
C) (U//~~FOUO~~)
D) (U//~~FOUO~~)

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

C) (U//~~FOUO~~)
D) (U//~~FOUO~~)
E) (U//~~FOUO~~)

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,

A) (U//~~FOUO~~)
B) (U//~~FOUO~~)
C) (U//~~FOUO~~)
D) (U//~~FOUO~~)
E) (U//~~FOUO~~)
F) (U//~~FOUO~~)
G) (U//~~FOUO~~)
H) (U//~~FOUO~~)

b7E

This Page is Intentionally Blank.

D Appendix D: (U) DEPARTMENT OF JUSTICE MEMORANDA ON COMMUNICATIONS WITH THE WHITE HOUSE AND CONGRESS

(U) There are two DOJ Memoranda included in this appendix:

D.1 (U) COMMUNICATIONS WITH THE WHITE HOUSE

(U) Attorney General's Memorandum "Department of Justice Communications with the White House" dated July 21, 2021.

(U) This memorandum supersedes all clauses in the previous Memorandum (included in Appendix D.2) **pertaining to communications with the White House only**. See Appendix D.2 for DOJ policy on communications with Congress. Substantively new content (as compared to the 2009 memo in D.2) is highlighted in yellow.

D.2 (U) COMMUNICATIONS WITH CONGRESS

(U) Attorney General's Memorandum "Communications with the White House and Congress" dated May 11, 2009

(U) As of July 21, 2021, this Memorandum should only be consulted for DOJ policy on **communications with Congress** (all clauses pertaining to communications with the White House were superseded by a subsequent Memorandum, included in Appendix D.1).

D.1 (U) COMMUNICATIONS WITH THE WHITE HOUSE

Office of the Attorney General
Washington, D. C. 20530

July 21, 2021

MEMORANDUM FOR ALL DEPARTMENT PERSONNEL

FROM: THE ATTORNEY GENERAL

SUBJECT: DEPARTMENT OF JUSTICE COMMUNICATIONS WITH THE WHITE HOUSE

The success of the Department of Justice depends upon the trust of the American people. That trust must be earned every day. And we can do so only through our adherence to the longstanding Departmental norms of independence from inappropriate influences, the principled exercise of discretion, and the treatment of like cases alike.

Over the course of more than four decades, Attorneys General have issued policies governing communications between the Justice Department and the White House. The procedural safeguards that have long guided the Department's approach to such communications are designed to protect our criminal and civil law enforcement decisions, and our legal judgments, from partisan or other inappropriate influences, whether real or perceived, direct or indirect.

This memorandum sets out guidelines to govern all communications between Justice Department and White House personnel. (The "White House," for purposes of this memorandum, means all components within the Executive Office of the President.) As has traditionally been the case, these guidelines have been developed in consultation with, and have the full support of, the Counsel to the President.

A. Communications Concerning Pending or Contemplated Criminal or Civil Law Enforcement Investigations or Cases

1. In order to promote and protect the norms of Departmental independence and integrity in making decisions regarding criminal and civil law enforcement, while at the same time preserving the President's ability to perform his constitutional obligation to "take care that the laws be faithfully executed," the Justice Department will not advise the White House concerning pending or contemplated criminal or civil law enforcement investigations or cases unless doing so is important for the performance of the President's duties and appropriate from a law enforcement perspective.

2. The Assistant Attorneys General, the United States Attorneys, the heads of the investigative agencies, and their subordinates have the primary responsibility to initiate and supervise law enforcement investigations and cases. In order to insulate them from inappropriate influences, initial communications between the Department and the White House concerning

pending or contemplated law enforcement investigations or cases will involve only the Attorney General or Deputy Attorney General, and the Counsel or a Deputy Counsel to the President (or the President or Vice President). If the communications concern pending or contemplated civil law enforcement investigations or cases, the Associate Attorney General may also be involved. Communications about Department personnel regarding their handling of specific law enforcement investigations or cases are included within the requirements of this Part.

3. If further or continuing communications between the Department and the White House on a particular matter are required, the officials who participated in the initial communication may designate subordinates to carry on such communications. The designating officials must monitor subsequent communications, and the designated subordinates must keep their superiors regularly informed of any such communications.

4. This Part also applies to communications between the Justice Department and the White House concerning the Department's exercise of its adjudicatory authority, including within the Executive Office for Immigration Review.

5. This Part is not intended to interfere with the normal communications between the Department and other departments and agencies in their capacities as Department clients (including entities within the Executive Office of the President when they are Department clients) or any meetings or communications necessary to the proper conduct of investigations or litigation in that capacity. However, in matters where the Executive Office of the President is the Department client, Department personnel must keep the Office of the Attorney General or Deputy or Associate Attorney General advised of such communications.

6. This Part does not prevent officials in the communications, public affairs, or press offices of the Department and the White House from communicating with each other to coordinate communications efforts. However, the relevant offices (the Office of the Attorney General or Deputy or Associate Attorney General, and the Office of the White House Counsel) must be advised and approve of such coordination efforts in advance.

B. Communications Concerning National Security Matters

1. It is critically important to have frequent and expeditious communications between the Department and the White House in matters relating to foreign relations and national security, including counterterrorism and counterespionage. Therefore, communications from or to the Assistant to the President for National Security Affairs, the Principal Deputy National Security Advisor, the Deputy Counsel to the President for National Security Affairs, and the staff of the National Security Council that relate to such matters are not subject to the limitations set out in Part A above or Part F below. However, the Office of the Attorney General or Deputy Attorney General, and the Office of the White House Counsel, must be kept advised of such communications. Such communications may also be subject to further supervisory guidance designed by those Offices to safeguard both the Department's independence and national security responsibilities.

2. This exception for foreign relations and national security related matters does not extend to domestic matters unrelated to foreign actors or foreign influences when there are no exigent circumstances that would render infeasible the initial communication requirement of Part A. Nor does the exception extend to pending adversary cases in litigation that may have national security implications. Communications related to such domestic matters and pending cases are subject to the guidelines for pending or contemplated law enforcement investigations or cases described in Part A. If communications occur in the exigent circumstances described in this paragraph, the Office of the Attorney General or Deputy Attorney General, and the Office of the White House Counsel, must be notified as soon as feasible.

C. White House Requests for Legal Opinions

All requests from the White House for formal legal opinions will come from the Counsel or a Deputy Counsel to the President (or the President or Vice President), and will be directed to the Attorney General, Deputy Attorney General, or Assistant Attorney General for the Office of Legal Counsel. The Assistant Attorney General will advise the Attorney General and Deputy Attorney General of any such requests. If further or continuing communications on a particular matter are required, the Assistant Attorney General may designate subordinates to carry on such communications. The Assistant Attorney General will report to the Attorney General or Deputy Attorney General any communications that, in the Assistant Attorney General's view, constitute improper attempts to influence the Office of Legal Counsel's legal judgment. All other White House communications with Office of Legal Counsel personnel must be in accordance with the other parts of this memorandum. The Office of the Attorney General or Deputy Attorney General, and the Office of the White House Counsel, must be kept advised of such communications.

D. Communications with the Office of the Solicitor General

Communications between the White House and the Office of the Solicitor General concerning Supreme Court and appellate matters are often appropriate. Any initial such communication will involve only the Counsel or a Deputy Counsel to the President, and the Attorney General, Deputy Attorney General, or Solicitor General. If further or continuing communications on a particular matter are required, the officials who participated in the initial communication may designate subordinates from each side to carry on such communications. The Solicitor General must keep the Office of the Attorney General or Deputy Attorney General advised regarding such communications. All other White House communications with Office of the Solicitor General personnel must be in accordance with the other parts of this memorandum.

E. Communications with the Pardon Attorney

The Pardon Attorney may communicate directly with the Counsel and Deputy Counsels to the President concerning clemency matters. The Pardon Attorney and the Counsel to the President may designate additional subordinates to carry on further communications after the initial communication is made. The Pardon Attorney must keep the Office of the Deputy Attorney General informed of all such communications.

F. Communications Concerning Policy and Intergovernmental Relations

As a department within the Executive Branch, the Justice Department appropriately works to advance the Administration's policies and intergovernmental relations. Thus, communications between the Department and the White House that are limited to these subjects, and that do not relate to pending or contemplated law enforcement investigations or cases, are appropriate. In order to ensure that such communications do not touch upon the latter (which are the subject of Part A), initial communications between the Department and the White House concerning policies and intergovernmental relations will involve the Office of the Attorney General or Deputy or Associate Attorney General, and the Office of the Counsel to the President. If further or continuing communications are appropriate, the officials who participated in the initial communication may authorize other personnel to carry on such communications, who must keep those Offices advised.

G. Communications Concerning Procurement and Grantmaking

Communications between the White House and the Department regarding procurement and grantmaking policies and priorities are appropriate. However, the award of specific contracts and grants are subject to the norm of independence in decision-making.

In order to insulate the Department's procurement and grantmaking functions from potentially inappropriate influences, initial communications between the Department and the White House concerning procurement and grantmaking will involve only the Offices of the Attorney General or Deputy or Associate Attorney General, and the Office of the Counsel to the President. If further or continuing communications are appropriate, the officials who participated in the initial communication may authorize other personnel to carry on such communications, who must keep those Offices advised.

H. Other Communications Not Relating to Pending or Contemplated Investigations or Criminal or Civil Cases

Communications between the Department and the White House that are limited to legislation, budgeting, political appointments, public affairs, or administrative matters that do not relate to pending or contemplated law enforcement investigations or cases may be handled directly by the personnel concerned. Such communications are appropriate, but they must take place with the knowledge of the Department's lead point of contact regarding the subject, who must keep the Office of the Attorney General or Deputy or Associate Attorney General advised of such communications.

I. 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 actual or perceived partisan affiliation. Thus, although the Department regularly receives communications from the White House (as well as from Senators and Members of Congress and their staffs) concerning political appointments,

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 must be immediately reported to the Deputy Attorney General.

J. Redirection of Communications

Employees of Department components who receive communications outside of these guidelines must immediately redirect those communications to the appropriate official or office under these guidelines, and so advise the relevant official or office.

* * *

As Attorney General Benjamin Civiletti noted in issuing the Department's first White House communications memorandum in 1979, these guidelines are not intended to wall off the Department from legitimate communications with the Administration. Rather, they are intended to route communications to the appropriate officials so that the communications can be adequately reviewed and considered, free from the appearance or reality of inappropriate influence. As such, these guidelines are an essential element of the norms that ensure the Department's adherence to the rule of law.

This memorandum supersedes all previous Attorneys General memoranda regarding communications with the White House. The *Justice Manual* will be amended to incorporate these guidelines.

D.2 (U) COMMUNICATIONS WITH CONGRESS

Office of the Attorney General
Washington, D. C. 20530

May 11, 2009

MEMORANDUM FOR HEADS OF DEPARTMENT COMPONENTS
ALL UNITED STATES ATTORNEYS

FROM: 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.

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.

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

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*.

E Appendix E: (U//~~FOUO~~) ATTORNEY GENERAL MEMORANDUM – REVISED POLICY ON THE USE OR DISCLOSURE OF FISA INFORMATION, DATED JANUARY 10, 2008

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:

- [redacted] b7E

b7E

- [redacted]
- [redacted]
- [redacted]

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.

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 information[1] 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.

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] b7E [redacted] and shall comply with the following procedures in matters that involve the use or disclosure of FISA information:[3]

---

[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~~

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.
3.
4.

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] b7E To the extent that applications in such districts require the disclosure of additional FISA information beyond the disclosure o[redacted] advance authorization as provided for in Section II of this policy is required prior to such applications being made to the court.

~~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.

C. [redacted] b7E

1. Where such further consultation takes place because of particularly sensitive sources, methods, or collections, NSD shall provide notice of such consultation to ODNI.

D. This section does not permit the use or disclosure of FISA information obtained [redacted] b7E 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~~

~~**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

[redacted]

[redacted] Title 18, Chapter 119, United States Code;

[redacted] Title 18, Chapter 121, United States Code;

[redacted] Rule 41 of the Federal Rules of Criminal Procedure;

[redacted] 18 U.S.C. § 3144;

[redacted]

[redacted]

2. *Criminal Indictments and Post-Indictment Proceedings*

a. The use or disclosure of FISA information [redacted] b7E

[redacted] As a result, the advance authorization of the Assistant Attorney General for National Security is required before such use or disclosure.

b. This advance authorization requirement applies to [redacted] b7E

[redacted]

~~**FOR OFFICIAL USE ONLY**~~

3. Among the factors that will be considered with respect to granting use authority are:

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

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 NSD shall provide notice of such request to ODNI. b7E

III. Use or Disclosure of FISA Information In Non-Criminal Proceedings

A. Therefore, authorization of the Assistant Attorney General for National Security or his designee is required before such use or disclosure. b7E

1. b7E

~~FOR OFFICIAL USE ONLY~~

2. Among the factors that will be considered with respect to granting use authority are: [redacted] b7E

[redacted]

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 [redacted] b7E

[redacted]

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.

Classification:

NOTIFICATION OF USE OR DISCLOSURE OF FISA INFORMATION FORM

b7E

Classification:

Classification:

b7E

Classification:

This Page is Intentionally Blank.

F Appendix F: (U) DOJ POLICY ON USE OF FORCE

F.1 (U) DOJ POLICIES ON THE USE OF FORCE

- (U) Attorney General's Memorandum on "Department's Updated Use-of-Force Policy," dated 5/20/2022.
- (U) Deputy Attorney General's Memorandum on "Policy on the Use of Less-than-Lethal Devices," dated 4/21/2011.

F.2 (U) USE OF FORCE TRAINING AND INSTRUCTION

F.2.1 *(U) INTRODUCTION*

(U) The following general principles shall guide the interpretation and application of this policy:

A) (U) DOJ policies reflect the paramount value of human life and the commitment to take reasonable steps to minimize the need to use force through training and procedures.

B) (U) This policy shall not be construed to require officers to assume unreasonable risks to themselves.

C) (U) The reasonableness of an officer's decision to use force must be viewed from the perspective of a reasonable officer on the scene, at the moment force is applied, without the benefit of 20/20 hindsight. Allowance must be made for the fact that officers are often forced to make split-second decisions in circumstances that are tense, uncertain, and rapidly evolving.

D) (U) Even when deadly force is permissible, officers must assess whether its use creates a danger to third parties that outweighs the likely benefits of its use.

F.2.2 *(U) ASSESSING THE NEED FOR USING FORCE*

(U) In assessing the need to use force, officers should consider the facts and circumstances of each case, including:

1) (U) The severity of the crime at issue,

2) (U) Whether the suspect poses an immediate threat to the safety of the officers or others, and

3) (U) Whether he or she is actively resisting or attempting to evade arrest by flight.

F.2.3 *(U) DEFINITIONS*

(U) For the purposes of this Appendix, the following definitions apply:

A) (U) **Deadly Force**: Is force that is reasonably likely to cause death or serious physical injury.

B) (U) **Reasonable Belief**: Is synonymous with "probable cause." It is determined by a totality of the facts and circumstances known to officers at the time, and the logical inferences that may be drawn from them.

C) (U) **Necessary**: The necessity to use deadly force requires 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 officer or other persons.

D) (U) **Imminent Danger**: Does not mean "immediate" or "instantaneous" but that an action that reasonably appears to pose a danger of death or serious physical injury is pending. Thus, a subject may pose an imminent danger even if the subject is not at that very moment pointing a weapon at the officer.

(U) For example

1) (U)

2) (U) b7E

3) (U)

4) (U)

F.2.4 *(U) MOVING VEHICLES*

1) (U) Firearms may not be discharged solely to disable a moving vehicle.

2) (U) Officers may discharge their weapon at the driver or passenger of a moving vehicle if the subject of such force poses an imminent danger of death or serious physical injury to the officer or another person by means other than the vehicle.

3) (U) If the vehicle is being operated in a manner that poses an imminent danger to the officer or another person, firearms may not be discharged at the vehicle if the officer and others can safely move from the path of the vehicle. However, if the officer and others can all safely move from the path of the vehicle, discharging a weapon at the vehicle is not permitted solely to prevent the flight from this violent confrontation.

4) (U) b7E

F.2.5 *(U) THREAT SOLELY TO SELF OR PROPERTY*

1) (U) A person who poses a threat solely to themselves or to property does not pose an imminent danger under this policy.

2) (U) If an officer or another person is in close proximity (i.e., within an area where it is reasonable to believe there is a threat of death or serious physical injury to the officer or other person) to an individual who poses an imminent danger of death or serious physical injury, deadly force may be used.

F.2.6 *(U) ADDITIONAL POLICY REQUIREMENTS*

F.2.6.1 (U) DE-ESCALATION

(U) Officers should employ de-escalation tactics and techniques to gain voluntary compliance from a subject before using force if objectively reasonable and if to do so would not increase the danger to the officers or others.

(U) Summary Statement: Officers should seek to gain voluntary compliance before using force if feasible and if doing so would not increase the danger to the officers or others.

1) (U) The goal of these techniques is to seek voluntary compliance before using force. De-escalation is not required in all situations, only those in which it is feasible and if doing so does not increase the danger to the officers or others.

2) (U) [redacted]

F.2.6.2 (U) DUTY TO INTERVENE

(U) Officers have the affirmative duty to intervene to prevent or stop, as appropriate, any officer from engaging in excessive force or any other force that violates the Constitution, other federal laws, or Department policies on the reasonable use of force.

b7E

(U) Summary Statement: Officers must prevent or stop, as appropriate, another officer from engaging in excessive or unlawful force, or force that violates DOJ policy.

1) (U) Excessive force is force that is clearly and obviously unnecessary or that involves a degree or level of force that no reasonable officer would believe is necessary.

2) (U) Force that serves no legitimate law enforcement purpose is excessive and unnecessary. In general, force is necessary if it is used to effect or maintain an arrest or investigative detention, to protect against or prevent physical harm, or to obtain or maintain compliance with a lawful order.

3) (U) Force that may otherwise violate federal laws or DOJ policies may occur when an officer acts without the legal authority to use force (for example, [redacted] or when force that violates DOJ policy is used (for example, [redacted]

b7E

4) (U) Officers who observe another DOJ law enforcement officer clearly engaging in such conduct are required to take appropriate steps to prevent or stop this violation.

5) (U) This section does not require off-duty officers to intervene.

F.2.6.3 (U) MEDICAL AID

(U) Officers have the affirmative duty to request and/or render medical aid, as appropriate, when needed.

(U) Summary Statement: Officers must request and/or render medical aid as appropriate.

1) If aid is rendered, it should be limited to training received by the officer.

2) This section does not require off-duty officers to request and/or render medical aid.

F.2.7 *(U) PRACTICAL CONSIDERATIONS*

(U) In assessing the necessity to use deadly force, the following practical considerations are relevant to its proper application:

F.2.7.1 (U) INHERENT LIMITATION ON ABILITIES TO ASSESS THE THREAT AND RESPOND

b7E

F.2.7.2 (U) ACHIEVING INTENDED PURPOSE

(U) Deadly force may only be applied for the intended purpose of bringing an imminent danger of death or serious physical injury to a timely halt

(U) b7E

F.2.8 *(U) PERTINENT LANGUAGE ON USE OF FORCE*[92]

(U) Deadly Force

(U) 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) (U) Deadly force may not be used solely to prevent the escape of a fleeing suspect.

B) (U) Firearms may not be discharged solely to disable moving vehicles. Specifically, firearms may not be discharged at a moving vehicle unless:

1) (U) A person in the vehicle is threatening the officer or another person with deadly force by means other than the vehicle.

2) (U) The vehicle is operated in a manner that threatens to cause death or serious physical injury to the officer or others, and no other objectively reasonable means of defense appear to exist, which includes moving out of the path of the vehicle.

(U) Firearms may not be discharged from a moving vehicle except in exigent circumstances. In these situations, an officer must have an articulable reason for this use of deadly force.

C) (U) 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) (U) Warning shots are not permitted outside of the prison context.

E) (U) 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.

F) (U) Deadly force should not be used against persons whose actions are a threat solely to themselves or property unless an individual poses an imminent danger of death or serious physical injury to the officer or others in close proximity.

(U) Summary of Additional Use of Force Policy Requirements

[92] (U) Department of Justice Updated Use-of-Force Policy (05/20/2022), in pertinent part. The language in this subsection is to be used for training purposes and inclusion in FD-888 "Law Enforcement Operations Order."

1) (U) Officers should seek to gain voluntary compliance before using force if feasible and if doing so would not increase the danger to the officer or others.

2) (U) Officers must prevent or stop, as appropriate, another officer from engaging in excessive or unlawful force, or force that violates DOJ policy.

3) (U) Officers must request and/or render medical aid as appropriate.

G Appendix G: (U) CLASSIFIED PROVISIONS

(U) See the separate classified *DIOG Appendix G* [links to a ~~SECRET//NOFORN document~~].

This Page is Intentionally Blank.

H Appendix H: (U) PRE-TITLE III ELECTRONIC SURVEILLANCE (ELSUR) SEARCH POLICY

H.1 (U) SCOPE

(U) Title 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.

H.1.1 *(U) COMPLIANCE WITH THE PREVIOUS APPLICATION PROVISION*

(U) 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, the affiant and affiant's supervisor must ensure all pre-Title III electronic surveillance searches (hereinafter "ELSUR searches") of the ELSUR Data Application (EDA) system have been properly completed by an ELSUR Operations Technician (EOT) prior to submission of the Title III application and affidavit to the court.

H.1.1.1 (U) WHEN TO SEARCH

(U) Original Title III Application/Affidavit: For both sensitive and non-sensitive Title IIIs, ELSUR searches for all target subjects, facilities, and/or places must be completed within 45 calendar days prior to the date the application and affidavit are filed with the court. [93]

(U) Extension and Renewal Title III Applications/Affidavit: For both sensitive and non-sensitive Title IIIs, ELSUR searches for all target subjects, facilities, and/or places previously searched for the same investigation must be completed within 90 calendar days prior to the date the new application and affidavit are filed with the court.

(U) However, any newly identified person, facility, and/or place named in an extension/renewal must be searched within 45 calendar days prior to the date the new application and affidavit are filed with the court.

(U) If an individual named by an alias, 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 EDA must be searched for previously submitted Title III applications involving any of the persons, facilities, and/or places specified in the current Title III application. There is no obligation to search for prior interceptions.

[93] 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).

H.1.1.2.1 ***(U) PERSONS***

(U) In submitting an FD-940 "Pre-Title III ELSUR Search Request," 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.[94] 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 ELSUR 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 must 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 (e.g., 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 an 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) An ELSUR search 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.

H.1.1.2.2 ***(U) FACILITIES***

(U) In submitting the FD-940, 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).

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).

[94] (U) All individuals listed in the application and affidavit as being involved in the specified criminal activity should be searched in EDA.

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. 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 an ELSUR search.

H.1.1.2.3 *(U) PLACES*

(U) In submitting the FD-940, 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] 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 application and affidavit to the court.[95]

H.1.1.3 (U) WHERE TO SEARCH

(U) A search of the FBI's EDA 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) EDA 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 EDA of any other federal, state, or local law enforcement agency that is actively participating in a joint investigation with the FBI (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.

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.

---

[95] 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 EDA prior to submitting the application and affidavit to the court.

H.1.1.4 (U) How To Initiate A Search Request

(U) The FD-940 must be used for requesting pre-Title III ELSUR searches of the EDA 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. The requesting agent must submit a lead to the ELSUR Technology Support Unit (ETSU) and the field office EOT. Use of the form will ensure search requirements are met, and must be submitted with adequate time for the EOT to conduct the search and document the results.

(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 must conduct a search of the EDA for records of previous applications only as specified in the FD-940. Records retrieved as a result of the search must be furnished to the requesting agent, and documented in the appropriate investigative ELSUR subfile.

(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 ensure a review of the pertinent investigative file(s) was conducted 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 ELSUR searches must be electronically placed in the appropriate investigative ELSUR subfile.

H.1.1.5 (U) Affidavit Language Examples

A) (U) NO PREVIOUS APPLICATIONS:

(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:

(U) "John Doe was named in a previous application for an order authorizing the interception of wire and electronic communications. The order was [signed or denied] on [date], by U.S. District Judge [name], of the District of [Name of District], 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 PROVIDED TO EOT

(U) The EOT and the ELSUR supervisor must confirm 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 must verify 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 application and order. The EOT must email a copy of these documents to the ETSU. The ETSU must index and upload these documents into the EDA system. These requirements also apply to the joint Title III operations discussed in section 18.7.2.13.

H.1.1.7 ROLE OF SPECIAL OPERATIONS DIVISION (SOD) AND SEARCHES

(U//~~FOUO~~)

b7E

(U//~~FOUO~~)

This Page is Intentionally Blank.

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 CFR § 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 CFR § 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 CFR § 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 CFR § 99.31(a)(9) nor the recordation requirements at 34 CFR § 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.

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//F~~OUO~~) The residence, location or destination of the subject of the investigation;

B) (U//F~~OUO~~) 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//F~~OUO~~) 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//F~~OUO~~) 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//F~~OUO~~) 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//F~~OUO~~) 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 matters (263 classification).

(U//F~~OUO~~) 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 out of an open investigative file, including an:

A) (U) 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 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;

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

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 Action Required or Information Only 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.

(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 his or her supervisor and the prior concurrence of the relevant SSA in the other field office, 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 SSA approval and advance SSA concurrence before entering another field office's AOR, notification should be made as soon as practicable to the employee's SSA and relevant SSA 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.

J.1.4 *(U) INVESTIGATION AND OTHER FILES*

(U//F~~OUO~~) 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 Assessment files, 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 IMD 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.

(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), and the *Manual Restriction of Access to Data in FBI Case Files Policy Notice* (0758N).

(U//~~FOUO~~) The types of files are:

J.1.4.1 (U) ZERO "O" FILES

(U//F~~OUO~~) [redacted] b7E

[redacted]

J.1.4.2 (U) DOUBLE ZERO "OO" FILES

(U//F~~OUO~~) 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. b7E

J.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), Laboratory assistance, 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 (66A classification) and civil litigation or claim matters (197A-F classifications) 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.

(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.1.4.4 (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, analytic intelligence products[96] that are prepared for program management purposes, etc. Note: **Investigative activity must not be conducted[97] 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 b7E

[96] (U//~~FOUO~~) A copy of all analytic intelligence products that are directly related to an investigation must be placed in an INTELPRODS sub-file. See DIOG section 15.6.1.2.

[97] (U) Section 18 investigative methods may only be conducted out of investigative files.

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) TYPE 1 & 2 ASSESSMENT FILES**

(U//~~FOUO~~) Type 1 & 2 Assessments must be maintained in an applicable Assessment file. When completing the Guardian FD-71a or Assessment file lead for an Assessment [redacted] b7E

(U//~~FOUO~~) Action leads can be set when using an Assessment file. Guardian, the EC, and the Sentinel 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, an opening EC is required (DIOG Section 5.6.3.2 through 5.6.3.5 type Assessments and DIOG Section 5.7 as discussed above). [redacted] 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. [redacted] b7E

[redacted] A pending-inactive Full Investigation may be assigned to investigative personnel or a squad/unit. b7E

J.1.4.5.4 ***(U) NATIONAL INCIDENT-BASED REPORTING SYSTEM***

(U//~~FOUO~~) If prompted, all case agents must complete the National Incident-Based Reporting System (NIBRS) form in Sentinel prior to closing a case or placing a full investigation in pending-inactive status.

J.1.4.5.5 ***(U) UNADDRESSED WORK FILES***

(U//~~FOUO~~) [redacted] b7E

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

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

(U//~~FOUO~~) Guardian incidents cannot be placed in an Unaddressed Work status.

J.1.4.5.6 ***(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 in column one must be used when creating sub-files to document the investigative or administrative activity described in column two. However, employees may create and utilize unique sub-file names to document investigative or administrative activities not already listed in the below standardized sub-file name list. For instance, a sub-file may be opened named "John Doe" with its contents all related to the activities of John Doe.

(U) List of standardized sub-files:

Sub-file Name	Description of Sub-file Contents
ADMIN	Administrative Matters
AFF	Affidavits
BC	Background Information Re Subject (FD-160; FD-125)
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
---	**"the appropriate investigative ELSUR sub-file"** *(Note: field offices may continue to use the following listed ELSUR sub-files pending the creation of new sub-file names by OTD and IMD to be reflected in the next DIOG Update.)*
ELA	ELSUR Administrative (Criminal and National Security)
ELA1	Title III Administrative
ELA2 (Note: The DIOG requires sub-file "PEN")	Pen Registers (See DIOG required sub-file "PEN" below)
ELA3	Consensual Monitoring
EL1	ELSUR Original Logs (Criminal and National Security)
EL1A	ELSUR Copies of Logs (Criminal and National Security)
EL1B	ELSUR Transcripts (Criminal and National Security)

ELA	Intercepts / Overhears
EMAIL	E-Mail
FA	Financial Analysis
FF	Forfeiture
	b7E
FISUR	Physical Surveillance Logs
FTP	Federal Taxpayer Information
FUG	Fugitives
GJ	**Federal Grand Jury Subpoenas and Materials**
INTELPRODS	**Written Analytic Intelligence Products**
LAB	Laboratory / Latent Reports
LEADS	Leads
LEGAL	Legal Documents
LOC	Locations
MC	Mail Covers (Criminal and National Security)
MEDIA	Media Reports
MISC	Miscellaneous
NC	Newspaper Clippings and Press Releases
NSL	**National Security Letters**
OGA	Other Government Agencies - Information / Reports
OM	Other Matters
OPS	Operation Plans
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
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-1087s)
1C	Bulky, Non-Evidence (FD-1087s)
1D	ELSUR
FD302	FD-302s (and other testimonial 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//F~~OUO~~) The text of FBI-generated records (including, but not limited to, FD-65, FD-786, and nontransitory 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//F~~OUO~~) 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 IMD BuNET page.

K Appendix K: (U) REQUIREMENT FOR ALL FBI PERSONNEL TO REPORT SUSPECTED ABUSE

K.1 (U) MANDATORY REPORTING

(U) Consistent with the Attorney General Guidelines for Victim and Witness Assistance (AGG-VWA), all FBI personnel – regardless of job function, position, or title – are mandatory reporters of suspected abuse. Accordingly, FBI personnel who suspect that any of the following categories of individuals are being (or have been) subjected to abuse must report the allegations as described in this policy:

- (U) Children[98]
- (U) Elderly persons[99]
- (U) Otherwise vulnerable individuals[100]

(U) Unless an exception is approved in accordance with subsection K.5, all reports of suspected abuse must be made without delay. For the purposes of this policy, "without delay" means initiating the reporting requirements in subsection K.2 without unnecessary or unreasonable deviations and no later than 24 hours after learning of facts that lead the mandatory reporter to suspect that abuse is occurring (or has occurred).

(U) These mandatory reporting requirements apply to all FBI personnel (except when an exception to the prompt reporting is approved in accordance with subsection K.5. FBI personnel need not personally witness or observe (i.e., hear or see) specific activities in order to suspect active or historical abuse. Rather, FBI personnel are required to make reports pursuant to this policy any time that they learn of facts that give reason to suspect abuse – including when such activity inadvertently or incidentally comes to their attention.

(U) The requirements in this policy are consistent with federal law and DOJ policy, but FBI personnel are also subject to applicable state, local, tribal, and territorial (SLTT) laws governing mandatory reporting requirements and procedures in their specific areas of responsibility (AOR). Accordingly, FBI personnel should familiarize themselves with applicable SLTT laws and direct questions about the applicability of these statutory requirements to chief division counsels (CDC) or the Office of the General Counsel (OGC). If an SLTT jurisdiction has more stringent reporting requirements than those contained in this policy, FBI personnel are required to comply with the more stringent SLTT law.

(U) Consistent with DIOG subsection 2.5, this policy is not intended to, does 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 does it place any limitation on otherwise lawful investigative and litigative prerogatives of the DOJ and the FBI.

---

[98] (U) See AGG-VWA Art. III.L.1.c.
[99] (U) See AGG-VWA Art. III.L.3.b.
[100] (U) See AGG-VWA Art. III.L.3.b.

(U) Definitions of terms used in this policy are included below in subsection K.7. FBI personnel who are unsure if an activity qualifies as abuse (and is therefore subject to the reporting requirements in this policy) should contact their CDCs or OGC's Investigative Law Unit (ILU) for assistance. Generally, if the requirement to report suspected abuse is unclear, FBI personnel should err on the side of caution and complete the reporting procedures in this policy.

(U) Comprehensive requirements pertaining to other aspects of the victim services program are located in the Victim Services Policy Guide (1010PG).

K.2 (U) REPORTING TO APPLICABLE AGENCIES

(U) As mandatory reporters, all FBI personnel are required to report suspected abuse to the SLTT law enforcement (LE) agency with jurisdiction to investigate the allegations. Additionally, when applicable, all FBI personnel are required to report suspected abuse to the child protective services agency or adult protective services agency with jurisdiction to protect the allegedly abused individual. (These LE and social services agencies are collectively referred to hereafter as "the applicable SLTT agencies"). Generally, the applicable SLTT agencies are articulated in SLTT laws. FBI personnel who are unable to determine the applicable SLTT agencies for a report should consult a CDC or OGC's ILU for guidance.

(U) When working as part of a squad or multidisciplinary team (MDT), multiple FBI personnel may simultaneously learn of facts giving them reason to suspect abuse. In these circumstances, the individual with the most direct information regarding the allegations is required to make the report to the applicable SLTT agencies. Other personnel on the squad or MDT should not make duplicate reports unless they are augmenting the original report with new facts or distinguishable elements of the suspected abuse.

(U) FBI personnel may consult victim specialists (VS) or other victim services providers (VSP) for guidance on properly making reports to applicable SLTT agencies. However, FBI personnel cannot report allegations to a VS or a VSP in lieu of reporting allegations to applicable SLTT agencies or ask a VS or a VSP to make such a report on their behalf.

(U) Even when there is reason to believe that an incident was previously reported or is otherwise being investigated, FBI personnel should generally err on the side of caution and report the incident to the applicable SLTT agencies without delay. Specifically, FBI personnel are required to report any elements of suspected abuse (e.g., day, time, and place) that they reasonably know to be distinguishable from previous reports and/or investigations (due to the possibility of multiple offenses, unreported victims, or additional perpetrators). However, some allegations of abuse fall within the primary investigative jurisdiction of the FBI (e.g., certain Indian Country matters, special jurisdiction matters, and certain crimes against children matters). If a mandatory reporter definitively knows that suspected abuse is the subject of an FBI investigation, the suspected abuse does not need to be reported to other (i.e., SLTT) law enforcement agencies. FBI personnel still must report the abuse to the applicable child protective services agency or adult protective services agency if such reporting is necessary to further protect the allegedly abused individual. When considering if such reporting is necessary, FBI personnel should consider the nature of the suspected abuse and the likelihood of imminent criminal charges against the alleged abuser. FBI personnel should consult their FO/FBIHQ division heads, their CDCs, or OGC's ILU to determine whether an additional report is reasonably necessary.

(U) As mandatory reporters, FBI personnel are generally immune from civil and criminal liability arising from reports that they make in good faith.

K.2.1 *(U) REPORTING SUSPECTED CHILD ABUSE ON FEDERAL LAND/PROPERTY*

(U) The FBI does not have primary investigative jurisdiction for all U.S. government-owned land and property. Pursuant to Title 34 U.S.C. § 20341, the Attorney General (AG) designates specific agencies (including some non-federal entities) to receive and investigate reports of child abuse on federal property (as well as federally operated or contracted facilities in which children are cared for or reside). FBI personnel who suspect that child abuse is taking place (or has taken place) on federal land/property must report the allegations to the applicable AG-designated agencies. If the AG has not designated an agency to investigate child abuse reports in a specific area, FBI personnel must instead report the allegations to the FBI field office in the AOR. FBI personnel who are unable to determine if the AG has designated an agency to receive and investigate child abuse allegations in a specific area should consult their CDCs or OGC's ILU for guidance.

K.2.2 *(U) REPORTING SUSPECTED ABUSE IN FOREIGN JURISDICTIONS*

(U) FBI personnel assigned outside of the United States or on temporary duty (TDY) assignments in foreign jurisdictions are also required to report suspected abuse:

- (U) Suspected abuse involving United States government employees or dependents under the chief of mission of a U.S. embassy must be reported to the State Department regional security officer (RSO) and the FBI legal attaché (LEGAT) (non-delegable).
- (U) If the suspected activity involves foreign citizen perpetrators or victims, FBI personnel should consult with the LEGAT and/or the RSO regarding any reporting laws of the foreign country and act accordingly. FBI personnel may request that the LEGAT or RSO report the suspected activity to the host government on their behalf.

(U) FBI personnel outside of the United States on personal travel should also report suspected abuse to the agencies with jurisdiction to investigate such reports and/or to the social services agencies with jurisdiction to protect the allegedly abused individuals. FBI personnel may contact the applicable LEGAT for assistance.

K.3 (U) FBI INTERNAL NOTIFICATION AND DOCUMENTATION PROCEDURES FOR SUSPECTED CHILD ABUSE

(U//~~FOUO~~) In addition to the reporting requirements described in subsection K.2, FBI personnel who learn of facts during the course of their official duties giving them reason to suspect child abuse must also:

1. (U//~~FOUO~~) Notify their FO/FBIHQ division heads as soon as practicable but no later than 48 hours after learning of the facts giving them reason to suspect child abuse;[101] and

2. (U//~~FOUO~~) Serialize an electronic communication (EC) in case file number 188D-HQ-A2450935 as soon as practicable but no later than five calendar days after completing the reporting requirements in subsection K.2 (see subsection K.3.1 for complete EC requirements).

(U//~~FOUO~~) FBI personnel who suspect child abuse outside of their official duties (i.e., "off duty") may also notify their FO/FBIHQ division heads and consult relevant personnel (e.g., VSs) for guidance on properly filing reports pursuant to subsection K.2. However, FBI-specific notification and documentation is not required for "off duty" reports.[102]

(U//~~FOUO~~) Generally, FBI personnel should notify their FO/FBIHQ division heads (or their documented designees) after completing the reporting requirements in subsection K.2. However, if FBI personnel notify their FO/FBIHQ division heads (or their documented designees) before filing reports pursuant to subsection K.2, the FO/FBIHQ division heads (or their documented designees) must ensure that FBI personnel complete the reports. FBI personnel cannot report allegations to their FO/FBIHQ division heads (or their documented designees) in lieu of reporting allegations to applicable SLTT agencies or ask their FO/FBIHQ division heads (or their documented designees) to make such reports on their behalf. FO/FBIHQ division heads (or their documented designees) are also responsible for ensuring completion of the required EC (see subsection K.3.1).

K.3.1 *(U) Electronic Communications for Internal Documentation of Child Abuse Reports*

(U//~~FOUO~~) As described in subsection K.3, FBI personnel who learn of facts during the course of their official duties giving them reason to suspect child abuse must serialize an EC in case file number 188D-HQ-A2450935. The EC must be drafted as soon as practicable but no later than five calendar days after completing the reporting requirements in subsection K.2.

(U) The EC must include the following information (to the extent known and applicable):[103]

- (U//~~FOUO~~) [redacted] b7E
- (U//~~FOUO~~) [redacted]

[101] (U//~~FOUO~~) Each FO/FBIHQ division head may designate a secondary official to whom notifications may be made. For FOs, the designee must be no lower than an ASAC; for HQ divisions or offices, the designee must be no lower than an SC. The appointment of an FO/FBIHQ division head's designee must be documented in an EC to case file number 188D-HQ-A2450935.

[102] (U) For FBI policy on reporting misconduct (e.g., allegations of abuse committed by FBI personnel), see the *Office of Professional Responsibility Policy Guide* (1168PG) and the *Self-Reporting Requirements Policy Guide* (1037PG).

[103] (U) See the Victim Services Division's (VSD) BuNet site for a pony EC.

- (U//FOUO) b7E
- (U//FOUO)
- (U//FOUO)
- (U//FOUO)
- (U//FOUO)
- (U//FOUO)

(U//FOUO) FBI personnel must index and submit this EC for approval as soon as practicable but no later than five calendar days after completing the reporting requirements in subsection K.2.

(U//FOUO) When the above information is properly documented in an EC to case file number b7E

K.4 (U) SPECIAL NOTIFICATION REQUIREMENT FOR SUSPECTED HUMAN TRAFFICKING OF FOREIGN NATIONAL MINORS

(U//FOUO) In accordance with the Trafficking Victims Protection Act (TVPA),[105] FBI personnel are required to notify the U.S. Department of Health and Human Services (HHS) upon determining that a foreign national child may be the victim of human trafficking. Within 24 hours of making such a determination, FBI personnel must complete form FD-1181 "Notification to HHS of Suspected Trafficking of a Foreign National Child" and send it by UNet e-mail to HHS' Office on Trafficking in Persons (OTIP) (childtrafficking@acf.hhs.gov). After notifying HHS OTIP, FBI personnel must serialize the completed FD-1181 in the relevant investigative case file in Sentinel b7E In the event that FBI personnel are notifying HHS of multiple potential victims at one time, an LHM or a spreadsheet with consolidated victim information may be appended to one FD-1181 form (in lieu of completing multiple FD-1181 forms).

(U//FOUO) If operational circumstances preclude FBI personnel from completing an FD-1181 within 24 hours, the reporting individual may instead notify HHS OTIP by phone (202-205-4582) or by e-mail (without an attached form). In such circumstances, the reporting individual must serialize a completed FD-1181 (or otherwise consolidated victim information) to the

[104] (U//FOUO) Consistent with DIOG subsection 12.7.3, this provision establishes a limited exemption from DIOG subsections 12.6 and 12.7.1, which otherwise require the completion of an FD-999 form.
[105] (U) Including any subsequent reauthorizations of the TVPA.

investigative case file (or zero file, if appropriate) in Sentinel as soon as practicable but no later than five business days thereafter. When notifying HHS without an FD-1181, the reporting individual should provide the following information (to the extent known and applicable):

- (U)
- (U)
- (U)

b7E

(U//~~FOUO~~) When the above information is properly documented on an FD-1181 and serialized in Sentinel, FBI personnel are not required to complete an FD-999 form to document the dissemination of victim information to HHS.[106] Additionally, FBI personnel are not permitted to complete an FD-999 in lieu of completing an FD-1181.

(U) FBI personnel should contact VSD's Child Victim Services Unit (CVSU) with questions about this notification process.

K.5 (U//~~FOUO~~) AUTHORIZATION TO TEMPORARILY DELAY REPORTING

(U//~~FOUO~~) When FBI personnel suspect abuse based on information gathered during an investigation, they must make reasonable efforts to report the allegations to the applicable SLTT agencies in order to protect the safety of the allegedly abused individual. However, if it is not possible to report the allegations without significantly compromising the investigation, compromising a confidential source, disclosing protected information (e.g., classified information or law enforcement sensitive information), or endangering public safety, FBI personnel must, without delay, seek authorization from their FO/FBIHQ division heads to temporarily delay reporting. Only an FO/FBIHQ division head is authorized to make the determination to temporarily delay reporting (non-delegable). Whenever feasible, FO/FBIHQ division heads should make this determination within 48 hours of receiving a request to temporarily delay reporting.

(U//~~FOUO~~) Prior to requesting a delay in reporting, FBI personnel should consult relevant subject matter experts (e.g., a VS, a child and adolescent forensic interviewer [CAFI], or other VSD employee at FBIHQ) and must obtain a legal opinion from a CDC or ADC, OGC, or DOJ on the basis for the delay – including potential criminal and civil penalties. FBI personnel must include the legal opinion (and any relevant consultative information) in the requests to their FO/FBIHQ division heads. When approving and documenting their decisions to temporarily delay reporting, FO/FBIHQ division heads must include this legal opinion with an EC in case file FO/FBIHQ division heads must monitor the case, and no later than every 30 days, re-review the case to determine if the abuse can be reported without impacting the investigation. These reviews must be documented in a new EC to case file The instant that the basis for withholding the report no longer exists, FO/FBIHQ division heads must ensure that the suspected abuse is reported in accordance with subsection K.2 (and subsection K.4, if applicable).

b7E

[106] (U//~~FOUO~~) Consistent with DIOG subsection 12.7.3, this provision establishes a limited exemption from DIOG subsections 12.6 and 12.7.1, which otherwise require the completion of an FD-999 form.

K.6 (U) TRAINING

(U) On an annual basis, FBI personnel are required to complete training in the Virtual Academy (VA) system on child abuse reporting requirements and procedures. Based on completion reports generated by the Training Division (TD), FO/FBIHQ division heads (or their documented designees) are required to ensure compliance with this requirement.

K.7 (U) DEFINITIONS

(U) Many of the terms used in this appendix have different definitions depending on the context and applicable statutory or regulatory authorities. The following definitions should be used to read, interpret, and contextualize the requirements in this policy. Questions about the applicability of this policy should be directed to VSD, a CDC, or OGC's ILU. Generally, if the requirement to report suspected abuse is unclear, FBI personnel should err on the side of caution and complete the reporting procedures in subsection K.2.

K.7.1 *(U) GENERAL DEFINITIONS*

(U) **FBI personnel**: 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. In accordance with DIOG section 2.11., 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 CHS "when operating pursuant to the tasking or instructions of an FBI employee."

(U) **Otherwise vulnerable individuals** includes persons who are developmentally challenged, mentally ill, or physically disabled (see AGG-VWA Art.III.L.3.a and AGG-VWA Art.V.J.2). For example, persons with physical or mental limitations or disabilities that substantially impair their ability to adequately provide for their own care or protection of their person or property.

(U) **Severe form of trafficking**, as defined by the TPVA (22 U.S.C. § 7102(11)), is either of the following:

- (U) Sex trafficking (the recruitment, harboring, transportation, provision, obtaining, patronizing, or soliciting of a person for commercial sex) in which a commercial sex act is induced by force, fraud, or coercion, or in which the person induced to perform such acts has not attained 18 years of age.

- (U) The recruitment, harboring, transportation, provision, or obtaining of a person for labor or services, through the use of force, fraud, or coercion for the purpose of subjection to involuntary servitude, peonage, debt bondage, or slavery.

(U) **Suspected abuse**: The knowledge of facts leading a reasonable person to suspect that a child, elderly person, or otherwise vulnerable individual is subject to (or has been subjected to) actions that knowingly inflict physical or psychological harm or injury. This includes, but is not limited to physical abuse, mental abuse, exploitation (including sexual exploitation), sexual

abuse, and negligent treatment. See below for specific statutory definitions of child abuse and elder abuse.

(U) **Without delay**: initiating the reporting requirements in subsection K.2 without unnecessary or unreasonable deviations and no later than 24 hours after learning of facts that lead the mandatory reporter to suspect that abuse is occurring (or has occurred).

K.7.2 *(U) DEFINITIONS SPECIFIC TO CHILD ABUSE*

(U) **Child**: A person under the age of 18 years.

(U) **Child abuse**, as defined by 34 U.S.C. § 20341(c)(1): the physical or mental injury, sexual abuse or sexual exploitation, or negligent treatment of a child.[107]

(U) **Mental injury**, as defined by 34 U.S.C. § 20341(c)(3): harm to a child's psychological or intellectual functioning which may be exhibited by severe anxiety, depression, withdrawal or outward aggressive behavior, or a combination of those behaviors, which may be demonstrated by a change in behavior, emotional response or cognition.

(U) **Negligent treatment**, as defined by 34 U.S.C. § 20341(c)(7): the failure to provide (for reasons other than poverty) adequate food, clothing, shelter, or medical care so as to seriously endanger the physical health of a child.

(U) **Physical injury**, as defined by 34 U.S.C. § 20341(c)(2), includes but is not limited to lacerations, fractured bones, burns, internal injuries, severe bruising or serious bodily harm.

(U) **Sexual abuse**:

- (U) As defined by 34 U.S.C. § 20341(c)(4): the employment, use, persuasion, inducement, enticement, or coercion of a child to engage in, or assist another person to engage in, sexually explicit conduct or the rape, molestation, prostitution, or other form of sexual exploitation of children, or incest with children.

- (U) As defined by 42 U.S.C. § 5106g(a)(4):

  - (U) A. The employment, use, persuasion, inducement, enticement, or coercion of any child to engage in, or assist any other person to engage in, any sexually explicit conduct or simulation of such conduct for the purpose of producing a visual depiction of such conduct; or

  - (U) B. The rape, and in cases of caretaker or inter-familial relationships, statutory rape, molestation, prostitution, or other form of sexual exploitation of children, or incest with children.

(U) **Sexual exploitation**, as defined by Art.III.L.1.b.(2) of the AGG-VWA, is all of the following:

---

[107] (U) Pursuant to 34 U.S.C. § 20341(c)(8), child abuse does not include discipline administered by a parent or legal guardian to his or her child, provided that it is reasonable in manner and moderate in degree and otherwise does not constitute cruelty.

- (U) The production, distribution, receipt, possession, or access of child pornography [child sexual abuse material (CSAM)].
- (U) The commercial sexual exploitation of children (prostitution).
- (U) 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.7.3 *(U) DEFINITIONS SPECIFIC TO ELDER ABUSE*

(U) **Abuse**, as defined by 42 U.S.C. § 1397j(1): the knowing infliction of physical or psychological harm or the knowing deprivation of goods or services that are necessary to meet essential needs or to avoid physical or psychological harm.

(U) **Elder** (or elderly person), as defined by 42 U.S.C. § 1397j(5): an individual age 60 or older.

(U) **Elder abuse**, as defined by 34 U.S.C. § 12291(a)(11): any action against a person who is 50 years of age or older[108] that constitutes the willful —

(A) infliction of injury, unreasonable confinement, intimidation, or cruel punishment with resulting physical harm, pain, or mental anguish; or

(B) deprivation by a person, including a caregiver, of goods or services with intent to cause physical harm

(U) **Exploitation**, as defined by 42 U.S.C. § 1397j(8): the fraudulent or otherwise illegal, unauthorized, or improper act or process of an individual, including a caregiver or fiduciary, that uses the resources of an elder for monetary or personal benefit, profit, or gain, or that results in depriving an elder of rightful access to, or use of, benefits, resources, belongings, or assets.

[108] (U) Although the Elder Justice Act defines an "elder" as "an individual age 60 or older" (see 42 U.S.C. § 1397j(5)), the Violence Against Women Act's definition of "elder abuse" includes individuals age 50 or older (see 34 U.S.C. § 12291(a)(11)). FBI personnel who are unsure if an allegation constitutes abuse should generally err on the side of caution and complete the reporting procedures in subsection K.2 or consult a CDC or OGC's ILU for guidance.

This Page is Intentionally Blank.

L Appendix L: (U) ONLINE INVESTIGATIONS

(U) The policy for *Investigative Methods Conducted Online by FBI Employees* is ~~U//LES~~. Also see the Quick Reference Guide for Online Investigations.

This Page is Intentionally Blank.

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.

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.[109] 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 26 U.S.C. § 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 IRS[110] 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."[111] 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.[112]

(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.

---

[109] (U) *Tax Information Security Guidelines for Federal, State and Local Agencies and Entities* (August 24, 2010) (IRS Pub.1075).
[110] (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.
[111] (U) See § 1.1 of IRS Pub. 1075.
[112] (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.[113] 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.[114]

(U//~~FOUO~~) Tax information acquired directly from the IRS is considered FTI and is protected under the IRC's confidentiality protections. 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~~) b7E
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 b7E

[113] (U) IRS Publication 1075, § 2.2 ("Need and Use").
[114] (U) 26 U.S.C. § 6103(i)(A).

b7E

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//FO~~UO)~~ Taxpayer return information is information filed with, or furnished to, the IRS by, or on behalf of, a taxpayer.[115] (See N.3.3. above.)

b7E

(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 FTI.

b7E

(U//~~FOUO~~) **Example:**

[115] (U) See 26 U.S.C. § 6103(b)(3).

N.4 (U) Department Of Justice Requirements For Obtaining And Safeguarding Federal Taxpayer Information[116]

(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.[117] The notice should include all relevant details so that the IRS can assemble the requested information and make 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.

---

[116] (U) See DOJ Order 2620.5A, *Safeguarding Tax Returns and Tax Return Information* (February 23, 1981).
[117] (U) This responsibility would most likely rest with the United States Attorney's Office (USAO) prosecuting the case.

(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//F~~OUO~~)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:[118]

1. (U//~~FOUO~~) A specific crime has been committed.
2. (U//F~~OUO~~) The return or return information is or may be relevant to a matter relating to the commission of that crime.
3. (U//F~~OUO~~) The information is sought exclusively for use in a federal investigation, and the information cannot reasonably be obtained from another source.

(U//F~~OUO~~) 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. b7E

(U//F~~OUO~~) 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.[119] 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."[120] 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 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

[118] (U) 26 U.S.C. § 6103(i)(1)(B).
[119] (U//FOUO) This information is available in a Preliminary or Full Investigation.
[120] (U) 26 U.S.C. § 6103(i)(2)(A).

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 CIRCUMSTANCES*[121]

(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//F~~OUO~~) 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~~) [redacted] b7E

[redacted]

[121] (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~~)

b7E

(U//~~FOUO~~)

(U//~~FOUO~~)

(U//~~FOUO~~)

(U//~~FOUO~~)

b7E

(U//~~FOUO~~)

(U//~~FOUO~~)

b7E

N.5.2.2 (U) WRITTEN REQUEST RELATED TO TERRORIST ACTIVITIES

(U//~~FOUO~~)

(U//~~FOUO~~)

b7E

- (U)
- (U)
- (U)
- (U)
- (U)
- (U)
- (U)
- (U)

(U//~~FOUO~~)

[122] (U) 26 U.S.C. § 6103(i)(7(A).
[123] (U//~~FOUO~~) Case ID

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 theirs 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.[124] 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

b7E

(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).

b7E

(U//~~FOUO~~)

N.6.1 *(U) TRACKING FTI*

(U//~~FOUO~~)

b7E

(U//~~FOUO~~)

[124] (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 BuNET Page.

(U//F~~OUO~~) All original FTI received from the IRS, both electronic and hard copies, must be protected in accordance with the guidance referenced above. b7E

(U//F~~OUO~~)

(U//F~~OUO~~)

(U//F~~OUO~~)

N.6.2 *(U) MARKING FTI*

(U//F~~OUO~~) b7E

N.6.3 *(U) HANDLING AND TRANSPORTING OF FTI*

(U//F~~OUO~~) b7E

(U//F~~OUO~~)

N.7 (U) REMOVABLE ELECTRONIC MEDIA

(U//F~~OUO~~) b7E

(U//F~~OUO~~)

b7E

(U//~~FOUO~~)

(U//~~FOUO~~)

(U//~~FOUO~~)

N.8 (U) DISPOSAL OF MATERIAL UPON DISPOSITION OF CASE

(U//~~FOUO~~)

(U)

b7E

-
-
-

(U

(Note

N.8.1 *(U) RETURN OF FTI*

(U//~~FOUO~~)

b7E

1.

[125] (U) See IRS Publication 1075, subsection 8.3.

2.

3.

b7E

(U)

(U//~~FOUO~~)

(U//~~FOUO~~)

N.8.2 *(U) FINAL DISPOSITION OF FTI SERIALIZED INTO SENTINEL*

(U) Upon the closing of a case file, all records serialized utilizing the FTI caveat must be permanently charged out of Sentinel. Per current policy, only IMD has the authority to delete or permanently charge out a serialized record. Therefore, a permanent charge out (PCO) lead request must be sent to requesting that the serials identified be permanently charged out. See the *Permanent Charge Out (Deletion) of Records From All Electronic Recordkeeping Systems* (0861D) policy directive for additional guidance. Prior to submission of the PCO lead request,

b7E

These last steps must be accomplished to ensure the FBI is acting in accordance with National Archives and Records Administration (NARA) approved records disposition schedules established for investigative records/files.

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.

[126] (U) See Publication 1075, subsection 8.4.

(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.

This Page is Intentionally Blank.

O APPENDIX O: (U) RIGHT TO FINANCIAL PRIVACY ACT

O.1 (U) SUMMARY

(U//~~FOUO~~) The Right to Financial Privacy Act (RFPA), 12 U.S.C. § 3401, et seq., prohibits financial institutions from providing financial records to the government, unless access is authorized by one of the exceptions or methods that is outlined below. The RFPA applies when the government is seeking the "financial records" of a "customer" of a "financial institution." The RFPA only applies if all three elements are met (e.g., the FBI is obtaining customer financial account records from a bank).

(U//~~FOUO~~) This appendix outlines the general responsibilities of FBI personnel to comply with the statutory requirements of the RFPA when seeking to obtain financial records from financial institutions defined under the statute.

O.2 (U) DEFINITIONS

O.2.1 (U) FINANCIAL INSTITUTION (12 U.S.C. § 3401(1))

(U//~~FOUO~~) The definition focuses on offices of institutions "located in any State or territory of the United States, the District of Columbia, Puerto Rico, Guam, American Samoa, or the Virgin Islands." This includes all banking and banking-type institutions, as well as consumer finance companies, and companies that issue credit cards, even though such companies are often not banking-type institutions. The RFPA does not apply to records maintained by a bank in a foreign jurisdiction or a U.S. financial institution's office located in a foreign jurisdiction. The RFPA also does not apply to bonding companies, credit bureaus, brokerage houses, government lending agencies, small business investment companies, the United States Postal Service, and money-service businesses such as Western Union.

O.2.2 (U) FINANCIAL RECORDS

(U//~~FOUO~~) A "financial record" is any original, copy of, or information "knowingly derived from" a record pertaining to a present or past customer's relationship with a financial institution. Excluded from the RFPA are records or information not identifiable with a particular customer (12 U.S.C. § 3413(a)) or those records that reside in the account of a third party, such as a check endorsed and deposited into a third-party account or items drawn to an individual, then deposited by the individual into the account of a corporation if the item was obtained from the corporation's financial records. It also excludes forged or counterfeit financial instruments and records relating to fictitious account names.

(U//~~FOUO~~) Requests for basic account information are also excluded from the RFPA's protection (12 U.S.C. § 3413(g)), as are records relating to bank surveillance photographs; contents of a safe deposit box sought pursuant to a search warrant; or records pertaining to functions that do not involve an account relationship, such as the sale of stocks and other activities that do not constitute routine bank services. If the records are obtained by a formal written request, obtaining the basic account information requires the use of Department of Justice (DOJ) Form 475 "Formal Written Request for Account Information and Certificate of Compliance with RFPA". If a subpoena or other process is used to obtain this basic account

information, then the subpoena or other process is required, along with DOJ Form 461 "Certificate of Compliance with the Right to Financial Privacy Act of 1978".

(U) Under most circumstances, financial information relating to the accounts of individuals and partnerships of five or fewer individuals is protected under the RFPA (12 U.S.C. § 3401(2)).

O.2.3 (U) CUSTOMERS COVERED (12 U.S.C. § 3401(5))

(U//F~~OUO~~) To be considered a "customer" under the RFPA, the entity must meet the definition of a "person" under the statute. A "person" is defined as any natural person or partnership of five or fewer individuals (12 U.S.C. § 3401(4)) and includes any person for whom the financial institution is acting or has acted as a fiduciary in relation to an account maintained in the person's name at the institution. Corporations, associations, larger partnerships, pension funds, special interest nonprofit organizations, trusts, or other legal entities are not covered by the RFPA.

O.2.4 (U) GOVERNMENT AUTHORITY

(U//F~~OUO~~) The RFPA applies to all federal agencies, including the FBI or any officer, employee, or agent thereof, including TFOs.

O.2.5 (U) LAW ENFORCEMENT INQUIRY

(U) Any lawful investigation or official proceeding inquiring into a violation of, or a failure to comply with, any criminal or civil statute, regulation, rule, or order issued thereunder, is considered a law enforcement inquiry.

O.3 (U) METHODS FOR OBTAINING RECORDS

(U) Only the methods listed below may be used under the RFPA to obtain information from a financial institution.

O.3.1 (U) WRITTEN REQUEST

(U//F~~OUO~~) The FBI is authorized by 28 CFR § 47.3 to request financial records of any customer from a financial institution pursuant to a formal, written request (see 12 U.S.C. § 3408).

(U//F~~OUO~~) The FBI may request these records from the financial institutions; however, this method of access requires the cooperation of the financial institution, as well as notification (i.e., disclosure of the request using DOJ Form 464 "Customer Notice") to the customer, unless a delay of notice order (DOJ Form 468 "Order") is obtained.

(U//~~FOUO~~) The written request (DOJ Form 463 "Formal Written Request for Financial Records") must state the purpose of the investigation, without reference to the specific title and section of the U.S.C. Generic terms, such as fraud, bribery, extortion, and the like, may be used to describe the offense, similar to the character descriptions of cases the FBI now uses. If no delay of notice order is obtained, the customer notice provision within the request must state the name and business address of the FBI supervisory official to be served with copies of customer challenge papers, should the customer decide to challenge the production of records written

request. b7E

O.3.1.1 (U) FORMS REQUIRED FOR A WRITTEN REQUEST

(U) The following forms may be required when requesting a customer's financial records from a financial institution pursuant to a formal written request:

- (U) DOJ Form 461 "Certificate of Compliance with the Right to Financial Privacy Act of 1978"
- (U) DOJ Form 463 "Formal Written Request for Financial Records"
- (U) DOJ Form 464 "Customer Notice"
- (U) DOJ Form 465 "Motion for Order Pursuant to Customer Challenge Provisions of the Right to Financial Privacy Act of 1978"
- (U) DOJ Form 466 "Sworn Statement of Movant"

O.3.2 (U) JUDICIAL SUBPOENA

(U//~~FOUO~~) A judicial subpoena is any court order to produce records other than a grand jury subpoena—the most common of which is the trial subpoena directed at a party not involved in litigation. When used, a copy of the judicial subpoena, together with mandatory customer notice (i.e., DOJ Form 464), is served or mailed to the customer. The notice provisions for the judicial subpoena are the same as for the written request above (12 U.S.C. § 3407).

O.3.3 (U) ADMINISTRATIVE SUBPOENA

(U//~~FOUO~~) The statutory requirements of the RFPA provide that a government authority may have access to, or obtain copies of, the information contained in the financial records of any customer of a financial institution when such records are disclosed in response to an administrative subpoena or a summons meeting the requirements of 12 U.S.C. § 3405. The FBI may use administrative subpoenas to obtain bank records in Title 21 (Controlled Substance), sexual exploitation or abuse of children investigations, and healthcare fraud investigations. (**Note:** Healthcare fraud administrative subpoenas are issued by the relevant United States Attorney's Office [USAO]). See DIOG subsection 18.6.4, "Investigative Method: Administrative Subpoenas." For guidance on the use of administrative subpoenas and associated financial privacy limitations, see DIOG subsection 18.6.4.3.4.

O.3.4 (U) GRAND JURY SUBPOENA

(U//~~FOUO~~) The RFPA does not require notification to the customer when records are requested using a grand jury subpoena. However, the RFPA still places restrictions on the handling and use of customer financial records obtained in this manner. The RFPA record-handling requirements are consistent with the treatment of federal grand jury documents, b7E

b7E

(U) Financial records of a customer that were obtained from a financial institution by use of grand jury subpoena should be treated in accordance with guidance from the relevant USAO or DOJ component and marked as "Subject to RFPA." (See relevant DIOG subsection in 18.6.5, "Marking, Physical Storage, and Mailing of Grand Jury Material.")

(U//~~FOUO~~) Financial records (as defined by RFPA) obtained with a grand jury subpoena (see 12 U.S.C. § 3420) must be returned and actually presented to the grand jury unless the volume of such records makes it impractical. In that situation, the grand jury must be provided with a description of the content of the records. The records may only be used (1) for the purpose of considering whether to issue an indictment or presentment by that grand jury, (2) for prosecuting a crime for which the indictment or presentment has been issued, (3) for a purpose authorized by Rule 6(e) of the Federal Rules of Criminal Procedure (FRCP), or (4) for a purpose authorized under § 3412 of the RFPA.

(U//~~FOUO~~) Records obtained under the RFPA via a grand jury subpoena must be destroyed or returned to the financial institution if not used for one of the purposes noted above, unless such records have been used in the prosecution of a crime for which the grand jury issued an indictment or a presentment or for a purpose authorized by Rule 6(e) of the FRCP (see 12 U.S.C. § 3420). If the records have been used in the prosecution, then the records—or a description of them—may only be maintained by a government authority if they are placed in the sealed records of the grand jury, unless such records have been introduced as evidence and thus disclosed publically in the criminal proceedings.

(U//~~FOUO~~) Given the differences in how federal judicial circuits define matters occurring before the grand jury under Rule 6(e)

b7E

(U//~~FOUO~~) Although grand jury subpoenas are not subject to the certification of compliance, customer notice, or the civil liability provisions of the RFPA, they are subject to the FGJ reimbursement procedures established through the USAO.

O.3.5 (U) CRIMINAL SEARCH WARRANTS

(U//~~FOUO~~) A search warrant may be used to obtain a customer's account-related records from a financial institution under the RFPA, with notice to the customer (DOJ Form 464) of the search occurring within 90 days after execution. There are no changes in the procedures to obtain a search warrant.

b7E

b7E

[redacted]

O.3.6 (U) CUSTOMER AUTHORIZATION

(U) Customers may authorize access to identified records for up to 90 days by signing a revocable statement specifying the recipient, the purpose for disclosure, and an acknowledgement that he or she is aware of his or her rights under the RFPA. A customer-signed authorization (e.g., DOJ Form 462 "Voluntary Customer Authorization for Financial Records") is required when the records are obtained from the financial institution. This method of obtaining financial records typically applies in applicant-type investigations or when the financial records of a cooperative witness are being sought. The customer may revoke such authorization at any time before the records are disclosed.

O.3.7 (U) NATIONAL SECURITY LETTERS (NSL)

(U//~~FOUO~~) Financial institutions must comply with a request for a customer's or an entity's financial records made pursuant to 12 U.S.C. § 3414 by the FBI when the Director of the FBI [redacted] b7E
[redacted] certifies in writing, via an NSL, to the financial institution that such records are sought for [redacted]
[redacted] For additional information regarding NSLs, including nondisclosure requirements (i.e., notification to customer), see DIOG subsection 18.6.6.

O.3.8 (U) EMERGENCY ACCESS

(U//~~FOUO~~) A government authority may obtain financial records from a financial institution if the government authority determines that a delay in obtaining access to the records would create imminent danger of physical injury, serious property damage, or flight from prosecution. Access may be obtained immediately by merely presenting the financial institution with DOJ Form 461 signed by a supervisory official as described below (see DIOG subsection O.7.1). Within five days of obtaining access to the financial records, the government authority must file a signed, sworn statement of the supervisory official with the court, setting forth the grounds for the emergency access (12 U.S.C. § 3414(b) (3)).

(U//~~FOUO~~) Since notice is delayed under this provision, notification must subsequently be provided to the customer whose records were accessed (12 U.S.C. § 3409(c)).

(U//~~FOUO~~) Pursuant to Attorney General's Order 821-79, the Director has delegated this authority to include all supervisory officials, including those individuals serving as acting supervisory special agents and relief supervisors. (See the *Delegation of Authority to Sign Certificate of Compliance and File a Sworn Affidavit with the Court Authorizing Emergency*

Access to Financial Records Under the Right to Financial Privacy Act [RFPA] [12 U.S.C § 3414(b)].)

O.3.9 (U) Access To Financial Records For Certain Intelligence And Protective Purposes

(U//~~FOUO~~) Nothing in the RFPA (except for 12 U.S.C. §§ 3415, 3417, 3418, and 3421) applies to the production and disclosure of financial records pursuant to a request from a government official authorized to [redacted] b7E

[redacted]

(U) [redacted]

[redacted] This provision does not apply to those individuals for whom disclosure is necessary to comply with the government's request or to an attorney whom the financial institution may consult with to obtain legal advice or assistance with respect to that request.

O.4 (U) Customer Notice Requirements And Procedures

(U//~~FOUO~~) Required notice (i.e., disclosure of the request, using DOJ Form 464) advises the customer that his or her records are being sought (e.g., by administrative subpoena) and the nature of the inquiry, which may include a statement to the effect that the customer is not a subject of the investigation. If customer notification is not delayed pursuant to a court order, a supervisory request, or a notice exception, the records sought do not have to be produced, and the customer has ten days, if notice is personally served, and 14 days, if notice is mailed, to complete and file an affidavit detailing why the records are not relevant to a legitimate law enforcement inquiry. The customer must then serve a copy of the affidavit on the government authority and be prepared to present additional facts in court. If the customer does not comply with the above within the prescribed time limits, the records may be made available by the financial institution. Any FBI supervisory official (defined in subsection O.7.1) may execute a written request for financial records. Pursuant to a written request, customer notice may be delayed for period of up to 90 days (see subsection O.4.1.1. below).

(U//~~FOUO~~) The request serves as notification of the nondisclosure requirement.

O.4.1 (U) Exceptions To Customer Notice

(U//~~FOUO~~) Notwithstanding the restrictions on obtaining financial records, financial institutions are permitted to notify government authorities of possible violations of law reflected in their

records. In these situations, neither the financial institution nor the FBI is required to give any notice to the customer; however, the information provided may only include names or other identifying information concerning the individual or entity, the account involved, and the nature of the suspected illegal activity. The purpose of this exception under the RFPA is so that the government may use this information to obtain direct access to the customer's financial records through other legal means. In addition, there are no criminal penalties under the RFPA that prevent an institution from notifying its customer in the absence of a court order; however, recourse, such as obstruction of justice charges, may be available.

(U//~~FOUO~~) When basic account information is requested, it may be obtained under the RFPA without notice to the customer; however, a DOJ Form 461 must be filed with the financial institution (12 U.S.C. § 3403(b)) prior to receipt of the records. This information is limited to the customer's name, address, account numbers, and types of accounts. It may subsequently be disclosed to other non-DOJ federal agencies without further notice to the customer but does require that an additional transfer certification be completed (DOJ Form 474 "Certification for Transferring Records Obtained Pursuant to The Right to Financial Privacy Act of 1978") and delivered to that agency (12 U.S.C. § 3413(g)).

O.4.1.1 (U) DELAY OF NOTICE

(U//~~FOUO~~) Delays of customer notice (i.e., disclosure of the request, 12 U.S.C. § 3409) may be obtained for access to the records sought through the use of administrative subpoenas, judicial subpoenas, formal written requests, search warrants, NSLs, emergencies, and subsequent interagency transfers. [redacted] b7E
Delays of up to 90 days (or 180 days in the case of a search warrant) may be requested in the application to a court where there is a reason to believe (lesser standard than probable cause) that notice would cause (1) danger to life or physical safety, (2) flight from prosecution, (3) destruction of, or tampering with, evidence, (4) intimidation of a potential witness, (5) other serious jeopardy to an investigation or an official proceeding, or (6) undue delay to a trial or an ongoing official proceeding. To obtain a delay of notice, a sworn, written statement must be presented to a judge or magistrate that one or more of above situations exist. Extensions of the delay of notice may be similarly obtained based on necessity.

(U//~~FOUO~~) In addition to delaying the timing of the government notification to the customer, the court order issued should also prohibit the financial institution from disclosing to the customer that records pertaining to that customer are being sought [redacted] b7E

[redacted]

O.4.2 (U) CUSTOMER CHALLENGE

(U//~~FOUO~~) In instances where notice is not delayed, a customer may challenge a judicial subpoena or a formal written request. Grand jury subpoenas, being generally excepted by the RFPA and having no notice provisions, cannot be challenged at the time of access. NSLs are governed by nondisclosure procedures outlined in DIOG subsection 18.6.6.

(U//~~FOUO~~) Within 10 or 14 days, depending on the method of notice (served or mailed), the customer may file a motion to quash a judicial subpoena in U.S. district court or an application to enjoin the FBI from pursuing a formal, written request. Close coordination should be maintained

between the field office and the United States Attorney's Office (USAO) throughout the customer challenge process.

(U//~~FOUO~~) In support of the motion or application, the customer must file a sworn statement that he or she is the person whose records are being sought, and that he or she:

(a) (U) Has reason to believe the records sought are not relevant to the inquiry.

(b) (U) Believes that the RFPA has not been substantially complied with.

(c) (U) Has another legal reason for denying access.

(U//~~FOUO~~) The challenge does not shift the burden of proof to the customer, but it does require more than a mere allegation. The FBI field office, in coordination with the relevant USAO, must then convince the judge or magistrate that the records sought are relevant to a legitimate law enforcement inquiry. Relevance means anything that might be used as evidence or that might logically lead to evidence. Denial of customer challenge motions or applications is not appealable until after the trial or other proceeding.

(U//~~FOUO~~) If the FBI and USAO fail to justify attempted access to these records, the subpoena will be quashed or the formal, written request enjoined. If the government justifies access, the subpoena will be enforced, and the formal written request may be pursued with the financial institution.

(U//~~FOUO~~) If, after obtaining court access to the information, the USAO determines that no legal proceeding will be contemplated against the customer, the USAO must promptly notify the customer of his or her status related to the investigation.

(U//~~FOUO~~) Any applicable statute of limitation is suspended during the time the customer's motion or application is pending in court.

(U//~~FOUO~~) In the case of judicial subpoenas, venue for the customer challenge is restricted to the court that issued the subpoena. When a formal, written request is used, the customer may challenge in any one of three districts:

1. (U) The District of Columbia
2. (U) The site of the financial institution
3. (U) The site of the residence of the customer

O.4.3 (U) CERTIFICATE OF COMPLIANCE (12 U.S. C. § 3403(B))

(U//~~FOUO~~) No financial institution or officer or employee or agent of a financial institution may release the financial records of any customer to any government authority until the government authority certifies to the institution, in writing, that it has complied with the applicable provisions of the RFPA (e.g., customer notice or delay order). The government authority must provide the

financial institution with a DOJ Form 461 and, upon receipt of the certificate, the financial institution must provide the requested records to the government.

O.4.4 (U) RECEIPT OF RECORDS

(U//~~FOUO~~) Upon receipt of a request from a government authority, the financial institution must assemble the requested records and be prepared to deliver them once they receive the Certificate of Compliance under 12 U.S.C. § 3403(b) (see 12 U.S.C. § 3411).

O.5 (U) DISSEMINATION OF INFORMATION

O.5.1 (U) TO THE DEPARTMENT OF JUSTICE (DOJ)

(U//~~FOUO~~) Generally, the FBI may transfer records freely within the DOJ [redacted] b7E

[redacted] Transfers between and among the components of the DOJ are not restricted by the RFPA, except during an investigation of a financial institution whenever customer records are obtained through that investigation and the customer had no notice or challenge opportunity. In those circumstances, the customer records obtained may not be used for a separate inquiry on the customer. However, enough information about the separate inquiry on the customer may be given to another component so that access may be sought independently.

O.5.2 (U) TO OTHER FEDERAL DEPARTMENTS (NON-DOJ)

(U//~~FOUO~~) Financial records obtained under the RFPA may be transferred to another federal agency under 12 U.S.C. § 3412 only if an official of the transferring agency certifies, in writing (DOJ Form 474) to the file, that "there is reason to believe that the records are relevant to a legitimate law enforcement inquiry of the receiving agency." This may require a statement from the receiving agency. Within 14 days of the transfer, the customer must be notified of the transfer by the transferring agency unless the government has obtained, in connection with its original access or at the time of the transfer, a court order delaying that notice under the provisions of 12 U.S.C. § 3409.

O.5.3 (U) TRANSFERS TO STATE, LOCAL, AND FOREIGN GOVERNMENTS

(U//~~FOUO~~) [redacted] b7E

[redacted] because they are not subject to the RFPA.

[redacted]

O.6. (U) MATTERS OUTSIDE THE SCOPE OF THE RFPA

O.6.1 (U) FINANCIAL INSTITUTIONS

(U//~~FOUO~~) The RFPA does not require customer notice when the institution in possession of such records is the subject of the investigation. Nonetheless, the Certificate of Compliance is necessary. Customer records obtained under this exception may only be used or transferred in furtherance of that specific investigation. If evidence of another violation is developed, enough information (not records) may be given the appropriate agency, including the FBI, to identify the

record and violation. Thereafter, the receiving agency may proceed as if independent of the initial inquiry.

O.6.2 (U) Corporations Or Other Legal Entities

(U//~~FOUO~~) Investigations directed at corporations or other legal entities not protected by the RFPA may be conducted in same fashion as subsection O.6.1 above.

O.6.3 (U) Not Identifiable With Customer

(U//~~FOUO~~) A financial institution can disclose records if the information contained therein is not identified with, or identifiable as being derived from, the records of a particular customer.

O.6.4 (U) Parties In Interest

(U//~~FOUO~~) The RFPA does not apply when the government and the customer are litigants in a judicial or an administrative adjudicatory proceeding.

O.6.5 (U) Other

(U//~~FOUO~~) Other matters specifically excluded are: (1) certain designated supervisory agencies of financial institutions, (2) the Internal Revenue Service, (3) the General Accounting Office, (4) certain reports required of financial institutions, (5) the account's identifying information only, and (6) the administration of guaranty or loan insurance programs.

O.7 (U) Roles And Responsibilities

O.7.1 (U) FBI Supervisory Personnel

(U//~~FOUO~~) Before records may be obtained under any provision of the RFPA [redacted] b7E

[redacted]

[redacted] any FBIHQ or field office superviso [redacted]

[redacted] (See Delegation of Authority in subsection O.3.8.)

(U//~~FOUO~~) Access to financial records for certain intelligence and protective purposes requires a certification, in writing (via an NSL), to the financial institution, stating that such records are sought for foreign counterintelligence purposes to protect against international terrorism or clandestine activities [redacted] b7E

[redacted]

O.7.2 (U) Special Agents And Task Force Officers (TFO)

(U//~~FOUO~~) All special agents and TFOs should obtain familiarity with the RFPA in order to ensure compliance therewith. Although the RFPA does not apply to state and local law enforcement, deputized TFOs working on FBI-led task forces are considered federal law

enforcement agents; therefore, they are bound by the RFPA's requirements when working on federal cases.

O.7.3 (U) CHIEF DIVISION COUNSEL (CDC)

(U//~~FOUO~~) The CDC provides training on the requirements of the RFPA, as needed, during field office legal training.

O.7.4 (U) OFFICE OF THE GENERAL COUNSEL (OGC)

(U//~~FOUO~~) OGC ensures that any changes to the law or significant developments in the case law of the RFPA are communicated to CDCs.

O.8 (U) REMEDIES AND SANCTIONS

(U//~~FOUO~~) Failure to adhere to the statutory requirements of the RFPA could lead to notification by the financial institution to the customer that the FBI requested his or her records and that there is a possibility that the FBI could be held liable in a civil action brought by the customer. An FBI employee may also be subject to disciplinary action for willful or intentional violation of the RFPA and may be subject to civil liability. The customer cannot, however, seek other remedies not specified in the statute such as suppression of the records (12 U.S.C. § 3417(d)).

O.9 (U) REIMBURSEMENT COST

(U//~~FOUO~~) The RFPA is an exception to the general rule that federal agencies do not pay for information associated with compliance with a grand jury subpoena. The RFPA specifically requires the FBI to reimburse the financial institution for specific costs as set forth in the statute (see 12 U.S.C. § 3415). Reimbursement should be accomplished through the routine commercial vouchering procedures. The schedule of authorized fees is set forth in 12 CFR § 219.3, Appendix A [redacted] b7E

This Page is Intentionally Blank.

P Appendix P: (U) ACRONYMS

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
ASAC	Assistant Special Agent in Charge
ASC	Assistant Section Chief
ATF	Bureau of Alcohol, Tobacco, Firearms and Explosives
AUSA	Assistant United States Attorney
BOP	Bureau of Prisons
CALEA	Communications Assistance for Law Enforcement Act
CCRSB	Criminal Cyber Response and Services Branch
CD	Counterintelligence Division
CDC	Chief Division Counsel
CFR	Code of Federal Regulations
CHS	Confidential Human Source
CHSPG	Confidential Human Source Policy Guide
CIA	Central Intelligence Agency

CID	Criminal Investigative Division
CMS	Collection Management Section
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 Attaché
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
	b7E
EAD	Executive Assistant Director
EC	Electronic Communication
ECF	Electronic Case File
ECPA	Electronic Communication Privacy Act
ECS	Electronic Communication Service
EDA	ELSUR Data Application
EI	Enterprise Investigation

ELSUR	Electronic Surveillance
EO	Executive Order
EOT	ELSUR Operations Technician
ESN	Electronic Serial Number
ESU	DOJ OEO, Electronic Surveillance Unit
ETR	Electronic Technical Request
FBIHQ	FBI Headquarters
FGJ	Federal Grand Jury
FICP	Foreign Intelligence Collection Program
FISA	Foreign Intelligence Surveillance Act
FISC	Foreign Intelligence Surveillance Court
	b7E
FO IP	Field Office Intelligence Program
FPO	Field Office Policy Officer
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
IINI	Innocent Images National Initiative
ILB	Investigative Law Branch
ILU	Investigative Law Unit
IMD	Information Management Division

IOB	Intelligence Oversight Board
IOD	International Operations Division
IP	Intelligence Program
IP Address	Internet Protocol Address
IPO	Internal Policy Office
ISP	Internet Service Provider
JDA	Juvenile Delinquency Act
JTTF	Joint Terrorism Task Force
LEGAT	Legal Attaché
LHM	Letterhead Memorandum
LO	Lead Office
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
NSCLB	National Security and Cyber Law Branch
NSD	National Security Division, DOJ
NSL	National Security Letter
NSSE	National Special Security Events

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
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 Guide
PI	Preliminary Investigation
PIA	Privacy Impact Assessment
PIAB	President's Intelligence Advisory Board
PII	Personally Identifiable Information
PSA	Performance Summary Assessments
PTA	Privacy Threshold Analysis
RA	Resident Agency
RFPA	Right to Financial Privacy Act

b7E

RICO	Racketeer Influenced and Corrupt Organizations
SA	Special Agent
SAC	Special Agent-in-Charge
SC	Section Chief
SIA	Supervisory Intelligence Analyst
SIU	Strategic Initiative's Unit
SIM	Sensitive Investigative Matter
SOG	Special Operations Group
SORC	Sensitive Operations Review Committee
SSA	Supervisory Special Agent
SSG	Special Surveillance Group
SSIA	Senior Supervisory Intelligence Analyst
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
UCA	Undercover Activity
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
USMS	United States Marshals Service
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
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~~) Analytic Intelligence Products: an intelligence product that contains at least one analytic assessment based on cited evidence and supported through logical argumentation.

(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, disability, sexual orientation, or gender identity of the subject, or a combination of only those factors. An "articulated objective" means a defined statement exists containing the essential attainable elements toward fulfilling an authorized purpose.

(U) Child: a person under the age of 18 years. See AGG-VWA III.L.b.(1).

(U) Child abuse: the physical or mental injury, sexual abuse or sexual exploitation, or negligent treatment of a child. Child abuse does not include discipline administered by a parent or a legal guardian to his or her child provided that it is reasonable in manner and moderate in degree and otherwise does not constitute cruelty. See 34 U.S.C. § 20341(c) and AGG-VWA III.L.b.(2).

(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) Elder (or elderly person): a person aged 60 or older. See 42 U.S.C. § 1397j(5).

(U) Elder abuse: any action against a person who is 50 years of age or older that constitutes the willful —

A) Infliction of injury, unreasonable confinement, intimidation, or cruel punishment with resulting physical harm, pain, or mental anguish.

B) Deprivation by a person, including a caregiver, of goods or services with intent to cause physical harm.

See 34 U.S.C. § 12291(a).

(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 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. b7E

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 (AGG-ET)* (2020), (ii) the *Memorandum of Understanding Concerning Overseas and Domestic Activities of the Central Intelligence Agency and the Federal Bureau of Investigation* (2005), and (iii) the *Memorandum of Understanding between the Department of State, the Department of Treasury and the Department of Justice Regarding the U.S. Chief of Mission* (1996).

(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.

(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: Any human source, to include both confidential human sources as defined in the Attorney General's Guidelines Regarding the Use of FBI Confidential Human Sources and non-CHSs, who can provide the FBI with information to address collection needs or advance an investigation. Non-CHSs (i.e., non-symbolled sources) include liaison contacts, witnesses, victims, walk-ins, call-ins, etc.

(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) Member of the Public with a Disability: a person with a disability who meets the essential eligibility requirements for participation in, or receipt of benefits from, a traditional law enforcement program or activity conducted by the FBI. See the Department of Justice's *Guidance on Interactions with Members of the Public with Disabilities in Traditional Law Enforcement Programs and Activities* (January 2017).

(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) Otherwise vulnerable individuals: includes persons who are developmentally challenged, mentally ill, or physically disabled (see Art.III.L.3.a and Art.V.J.2 of the *Attorney General Guidelines for Victim and Witness Assistance*). For example, persons with physical or mental limitations or disabilities that substantially impair their ability to adequately provide for their own care or protection of their person or property.

(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) Predicated Investigation: While Assessments only require an "authorized purpose" to initiate, a predicated investigation requires factual predication to open. As defined in the AGG-Dom, a predicated investigation that relates to a federal crime or national security threat may be opened as a Preliminary Investigation (based on "information or allegation") or a Full Investigation (based on an "articulable factual basis"). See DIOG Sections 6 and 7, respectively. Enterprise Investigations (DIOG Section 8) and Positive Foreign Intelligence Investigations (DIOG Section 9) are types of Full Investigations.

(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. 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 online 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: 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: Consensual monitoring during one of the following scenarios:

A) (U) Investigation of a member of Congress, a federal judge, a member of the executive branch at Executive Level IV or above, or a person who has served in such capacity

within the previous two years. (Executive Levels I through IV are defined in 5 U.S.C. §§ 5312-5315.)

B) (U) Investigation of the governor, lieutenant governor, or attorney general of any state or territory, or a judge or a justice of the highest court of any state or territory, concerning an offense involving bribery, conflict of interest, or extortion related to the performance of official duties.

C) (U) A party to the communication is in the custody of the Bureau of Prisons (BOP) or the United States Marshals Service (USMS) or is being or has been afforded protection in the Witness Security Program.

D) (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) Severe form of trafficking, as defined by the Trafficking Victims Protection Act (TVPA) (22 U.S.C. § 7102(11)), is either of the following:

A) (U) Sex trafficking (the recruitment, harboring, transportation, provision, obtaining, patronizing, or soliciting of a person for commercial sex) in which a commercial sex act is induced by force, fraud, or coercion, or in which the person induced to perform such acts has not attained 18 years of age.

B) (U) The recruitment, harboring, transportation, provision, or obtaining of a person for labor or services, through the use of force, fraud, or coercion for the purpose of subjection to involuntary servitude, peonage, debt bondage, or slavery.

(U) Sexual abuse: has multiple statutory definitions:

- (U) As defined by 34 U.S.C. § 20341(c)(4): the employment, use, persuasion, inducement, enticement, or coercion of a child to engage in, or assist another person to engage in, sexually explicit conduct or the rape, molestation, prostitution, or other form of sexual exploitation of children, or incest with children.
- (U) As defined by 42 U.S.C. § 5106g(a)(4): the term "sexual abuse" includes-

  A) (U) The employment, use, persuasion, inducement, enticement, or coercion of any child to engage in, or assist any other person to engage in, any sexually explicit conduct or simulation of such conduct for the purpose of producing a visual depiction of such conduct.

  B) (U) The rape, and in cases of caretaker or inter-familial relationships, statutory rape, molestation, prostitution, or other form of sexual exploitation of children, or incest with children.

(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, Tribal, or Territorial: 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 [redacted] b7E

[redacted]

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. [redacted] b7E

[redacted]

C) (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: [redacted] b7E

[redacted]

(U) Suspected abuse: The knowledge of facts leading a reasonable person to suspect that a child, elderly person, or otherwise vulnerable individual is subject to (or has been subjected to) actions that knowingly inflict physical or psychological harm or injury. This includes, but is not

limited to physical abuse, mental abuse, exploitation (including sexual exploitation), sexual abuse, and negligent treatment.

(U//F~~OUO~~) Task force personnel: a term that collectively encompasses task force officers (TFO), task force members (TFM), and task force participants (TFP):

A) (U) An individual is a **task force officer (TFO)** when all of the following apply:

1. (U//~~FOUO~~) The individual is a certified federal, state, local, territorial, or tribal law enforcement officer (LEO).
2. (U//~~FOUO~~) The individual is authorized to carry a firearm.
3. (U//~~FOUO~~) The individual has appropriate federal authority to investigate and enforce violations of federal law within the scope of the individual's task force assignment. State and local TFOs must be deputized to have federal investigative and enforcement authority. Federal TFOs must also have federal investigative authority sufficient to meet their task force assignments or be appropriately deputized consistent with guidance from OGC and the FBIHQ division. See the *Joint Task Force Policy Guide* (1178PG) for additional information on deputations.
4. (U//~~FOUO~~) The individual is eligible and has initiated the FBI's process for obtaining federal law enforcement credentials.
5. (U//~~FOUO~~) The individual is assigned under the supervision of an FBI-led task force.
6. (U//~~FOUO~~) The individual has initiated a request for a security clearance issued by the FBI. If the TFO fails to complete the security clearance process, he or she must be removed as a TFO.
7. (U//~~FOUO~~) The individual is authorized to have access to FBI facilities.

(U//F~~OUO~~) An FBI TFO is mandated to attend all DIOG-related training and is bound by all rules, regulations, and policies set forth in the DIOG (and other applicable DIOG-related policies) when acting in the capacity of an FBI TFO.

B) (U) An individual is a **task force member (TFM)** when all of the following apply:

1. (U//~~FOUO~~) The individual is an employee of a federal, state, local, territorial, or tribal agency.
2. (U//~~FOUO~~) The individual is assigned under the supervision of an FBI-led task force.
3. (U//~~FOUO~~) The individual has an active security clearance recognized by the FBI.
4. (U//~~FOUO~~) The individual is authorized to have access to FBI facilities.

(U//~~FOUO~~) For example, a law enforcement or civilian employee of another federal, state, local, territorial, or tribal agency may have particular access or expertise that is

needed by the task force, but does not satisfy the requirements to be a TFO (e.g., a Bureau of Prisons senior intelligence analyst who is not deputized but may hold a clearance from another agency).

(U//~~FOUO~~) An FBI TFM is mandated to attend all DIOG-related training and is bound by all rules, regulations, and policies set forth in the DIOG (and other applicable policies) when acting in the capacity of an FBI TFM.

C) (U) An individual is a **task force participant (TFP)** when all of the following apply:

1. (U//F~~OUO~~) The individual is an employee of a federal, state, local, territorial, or tribal agency.
2. (U//F~~OUO~~) The individual does not otherwise qualify as a TFO or a TFM.
3. (U//~~FOUO~~) The individual has been approved as a TFP by the supervisor responsible for the task force, and the approval has been documented in the appropriate task force file.

(U//~~FOUO~~) For example, a civilian employee of another federal, state, local, territorial, or tribal agency may have particular expertise that is needed by the task force (e.g., forensic computer examiner), but the employee does not satisfy the requirements to be a TFO (e.g., the individual is not a sworn LEO) or a TFM (e.g., the individual does not have a security clearance).

(U//~~FOUO~~) When participating as an FBI TFP, the individual is bound by the rules, regulations, and policies set forth in the DIOG (and other applicable policies). DIOG-related training for a TFP may be required by the head of the FO or FBIHQ division that governs the activities of the joint task force.

(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 (UCA): An "undercover activity" is any investigative activity involving the use of an assumed name or cover identity by an employee of the FBI or another Federal, state, tribal or local law enforcement organization working with the FBI. An element of UCA is the conduct of investigative activity to seek information relevant to federal crimes or national security threats by means of interaction with a third party(ies).

(U//~~FOUO~~) Undercover Employee (UCE): An employee of the FBI, or employee of federal, state, or local law enforcement agency, USIC entity, or foreign intelligence agency working under the direction and control of the FBI during a particular investigation or operation whose relationship with the FBI is concealed from third parties in the course of an investigative or intelligence collection operation by the maintenance of a cover or alias identity.

(U//FOUO) Undercover Operation (UCO): 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 individual(s) under investigation [redacted] b7E

[redacted]

(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:

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) An USPER does not include 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.

(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. See classified Appendix G for further guidance concerning the determination of United States person status.

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

(U) "Without delay": initiating the mandatory reporting requirements in subsections 14.8 and 14.9 without unnecessary or unreasonable deviations and no later than 24 hours after learning of facts that lead the employee to suspect that abuse is occurring (or has occurred).

This Page is Intentionally Blank.

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

Part	Section	Section Title	DIOG Supersession
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
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

Part	Section	Section Title	DIOG Supersession
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
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

Part	Section	Section Title	DIOG Supersession
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

Part	Section	Section Title	DIOG Supersession
MIOG Intro	Section 2	2-2.7 Deleted	DIOG Preamble
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

Part	Section	Section Title	DIOG Supersession
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
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

Part	Section	Section Title	DIOG Supersession
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
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 TURKING	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

Part	Section	Section Title	DIOG Supersession
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
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

Part	Section	Section Title	DIOG Supersession
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
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

Part	Section	Section Title	DIOG Supersession
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
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

Part	Section	Section Title	DIOG Supersession
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	9-1.1Surveillance 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
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

Part	Section	Section Title	DIOG Supersession
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
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

Part	Section	Section Title	DIOG Supersession
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
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

Part	Section	Section Title	DIOG Supersession
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
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

Part	Section	Section Title	DIOG Supersession
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 b7E
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
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	11-1.3.1High-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

Part	Section	Section Title	DIOG Supersession
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
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

Part	Section	Section Title	DIOG Supersession
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
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

Part	Section	Section Title	DIOG Supersession
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
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

Part	Section	Section Title	DIOG Supersession
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
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
MIOG II	Section 23	23-6.10.2 Corporations or Other Legal Entities	DIOG Appendix O - RFPA
MIOG II	Section 23	23-6.10.3 Not Identifiable with Customer	DIOG Appendix O - RFPA
MIOG II	Section 23	23-6.10.4 Parties in Interest	DIOG Appendix O - RFPA
MIOG II	Section 23	23-6.10.5 Federal Grand Jury	DIOG Appendix O - RFPA

Part	Section	Section Title	DIOG Supersession
MIOG II	Section 23	23-6.10.6 Foreign Counterintelligence	DIOG Appendix O - RFPA
MIOG II	Section 23	23-6.10.7 Telephone Company Toll Records	DIOG Appendix O - RFPA
MIOG II	Section 23	23-6.10.8 Other	DIOG Appendix O - RFPA
MIOG II	Section 23	23-6.11 Dissemination of Information	DIOG Appendix O - RFPA
MIOG II	Section 23	23-6.11.1 To Department of Justice	DIOG Appendix O - RFPA
MIOG II	Section 23	23-6.11.2 To Other Departments	DIOG Appendix O - RFPA
MIOG II	Section 23	23-6.12 Penalties	DIOG Appendix O - RFPA
MIOG II	Section 23	23-6.12.1 Civil	DIOG Appendix O - RFPA
MIOG II	Section 23	23-6.12.2 Disciplinary Action	DIOG Appendix O - RFPA
MIOG II	Section 23	23-6.12.3 Other	DIOG Appendix O - RFPA
MIOG II	Section 23	23-6.13 Cost Reimbursement	DIOG Appendix O - RFPA
MIOG II	Section 23	23-6.14 Reporting Requirements	DIOG Appendix O - RFPA
MIOG II	Section 23	23-6.14.1 Dissemination of Information Obtained	DIOG Appendix O - RFPA
MIOG II	Section 23	23-6.14.2 Statistical Reporting	DIOG Appendix O - RFPA
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

Part	Section	Section Title	DIOG Supersession
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[redacted]	DIOG 19.2 and Appendix G b7E
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, the[redacted]	See IPO MOU Library b7E
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

Part	Section	Section Title	DIOG Supersession
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]	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
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)

b7E

Part	Section	Section Title	DIOG Supersession
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]	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
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

b7E

Part	Section	Section Title	DIOG Supersession
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.
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.

Part	Section	Section Title	DIOG Supersession
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.
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

Part	Section	Section Title	DIOG Supersession
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 ____?
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

Part	Section	Section Title	DIOG Supersession
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
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.

Part	Section	Section Title	DIOG Supersession
MAOP II	3-4.6	Reclassifying Cases and Error Correction	DIOG 6.11.C; 7.11.C; 8.8.C; and 9.12.C
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

Part	Section	Section Title	DIOG Supersession
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
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

Part	Section	Section Title	DIOG Supersession
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
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"

Part	Section	Section Title	DIOG Supersession
N/A	EC	[redacted]	34.D
N/A	EC	[redacted] Legal Advice and Opinions, Tax Return Information, and Return information Relevant to Terrorism Cases; Ex Parte Orders	Appendix N
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 an 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

b7E

b7E

Part	Section	Section Title	DIOG Supersession
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
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 numbe[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

b7E

Part	Section	Section Title	DIOG Supersession
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
N/A	CPN 00541N	Recordkeeping Policy for ELSUR Administrative Information Resulting from Joint Criminal Investigative Operations	DIOG 18.7.2.13 Revised 03/31/2020
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 IMD, Case ID# [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.

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) Online 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 18.5.3.1)

(U) Searches that Do Not Require a Warrant or Court Order (Trash Cover, Abandoned Property from a Public Receptacle, Administrative Inventory Search of a Lost/Misplaced Item) and Inventory Searches Generally. (Section 18.6.12)

(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.

18.5.3.1 (U) Records or information - Other federal, state, local, tribal, or foreign government agency.

18.5.4 (U) Online 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 (e.g., Trash Cover, Abandoned Property from a Public Receptacle, or Administrative Inventory Search of a Lost/Misplaced Item) and Inventory Searches Generally.

18.6.13 (U) Undercover operations.

18.7.1 (U) Searches – with a warrant or court order.

18.7.2 (U) Electronic surveillance – Title III

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