15 (U) INTELLIGENCE ANALYSIS AND PLANNING

15.1 (U) OVERVIEW

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

(U//~~FOUO~~) In carrying out its intelligence analysis and planning functions, the FBI is authorized to draw on all lawful sources of information, including analysis of historical information in FBI files (open and closed), records and database systems, and information collected from investigative activities permitted without opening an Assessment set forth in DIOG Section 5.1.1.

(U//~~FOUO~~) *Note:* In the DIOG, the word "assessment" has two distinct meanings. The AGG-Dom authorizes as an investigative activity an "Assessment," which requires an authorized purpose as discussed in DIOG Section 5. The United States Intelligence Community (USIC), however, also uses the word "assessment" to describe written intelligence products, as discussed in Section 15.6.1.2 below.

15.2 (U) PURPOSE AND SCOPE

15.2.1 *(U) FUNCTIONS AUTHORIZED*

(U//~~FOUO~~) The AGG-Dom authorizes the FBI to engage in intelligence analysis and planning to facilitate and support investigative activities and other authorized activities. The functions authorized include:

A) (U//~~FOUO~~) Development of overviews and analyses concerning threats to and vulnerabilities of the United States and its interests, such as domain management as related to the FBI's responsibilities;

B) (U//~~FOUO~~) Research and analysis to produce reports and assessments (analytical products) concerning matters derived from or relevant to investigative activities or other authorized FBI activities; and

C) (U//~~FOUO~~) The operation of intelligence and information systems that facilitate and support investigations and analysis through the compilation and analysis of data and information on an ongoing basis. (AGG-Dom, Introduction B)

15.2.2 *(U) INTEGRATION OF INTELLIGENCE ACTIVITIES*

(U//~~FOUO~~) In order to protect against national security and criminal threats through intelligence-driven operations, the FBI should integrate intelligence activities into all investigative efforts by:

A) (U//~~FOUO~~) Systematically assessing particular geographic areas or sectors to identify potential threats, vulnerabilities, gaps, and collection opportunities in response to FBI collection requirements that support the broad range of FBI responsibilities;

B) (U//~~FOUO~~) Proactively directing resources to collect against potential threats and other matters of interest to the nation and the FBI, and developing new collection capabilities when needed;

C) (U//~~FOUO~~) Continuously validating collection capabilities to ensure information integrity;

D) (U//~~FOUO~~) Deliberately gathering information in response to articulated priority intelligence requirements using all available collection resources, then expeditiously preparing the collected information for analysis and dissemination and promptly disseminating it to appropriate partners at the local, state, national and foreign level; and

E) (U//~~FOUO~~) Purposefully evaluating the implications of collected information on current and emerging threat issues.

15.2.3 *(U) Analysis and Planning Not Requiring the Opening of an Assessment (See DIOG Section 5)*

(U//~~FOUO~~) Without opening an Assessment, an FBI employee may produce written intelligence products that include, but are not limited to, an Intelligence Assessment (analytical product), Intelligence Bulletin and Geospatial Intelligence (mapping) from information already within FBI records. An FBI employee can also analyze information that is obtained pursuant to DIOG Section 5.1.1. If the employee needs information in order to conduct desired analysis and planning that requires the use of Assessment investigative methods beyond those permitted in DIOG Section 5.1.1, the employee must open a Type 3 Assessment or Type 4 Assessment in accordance with DIOG Sections 5.6.3.3. The applicable 801H - 807H classification file (or other 801-series classification file as directed in the *Intelligence Program Policy Guide* (1150PG) must be used to document this analysis. See the *Intelligence Program Policy Guide* (1150PG) for file classification guidance.

15.3 (U) Civil Liberties and Privacy

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

15.4 (U) Legal Authority

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

(U//~~FOUO~~) The scope of authorized activities under Part II of the AGG-Dom is not limited to "investigations" in a narrow sense, such as solving particular investigations or obtaining evidence for use in particular criminal prosecutions. Rather, the investigative activities authorized under the AGG-Dom may be properly used to provide critical information needed for broader analytic and intelligence purposes to facilitate the solution and prevention of crime, protect the national security, and further foreign intelligence objectives. These purposes include use of the information in intelligence analysis and planning under AGG-Dom, Part IV, and

dissemination of the information to other law enforcement, USIC, and White House agencies under AGG-Dom, Part VI. Accordingly, information obtained at all stages of investigative activity is to be retained and disseminated for these purposes as provided in the AGG-Dom, or in FBI policy consistent with the AGG-Dom, regardless of whether it furthers investigative objectives in a narrower or more immediate sense. (AGG-Dom, Part II)

15.5 (U) INTELLIGENCE ANALYSIS AND PLANNING – REQUIRING A TYPE 4 ASSESSMENT

(U//~~FOUO~~) If an FBI employee wishes to engage in intelligence analysis and planning that requires the collection or examination of information not available in existing FBI records or database systems, or from information that cannot be obtained using the activities authorized in DIOG Section 5.1.1, a Type 4 Assessment must be opened and conducted in accordance with DIOG Section 5.6.3.3.

15.6 (U) AUTHORIZED ACTIVITIES IN INTELLIGENCE ANALYSIS AND PLANNING

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

15.6.1 *(U) STRATEGIC INTELLIGENCE ANALYSIS*

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

15.6.1.1 (U) DOMAIN MANAGEMENT

(U//~~FOUO~~) As part of Strategic Analysis Planning activities, the FBI may collect information in order to improve or facilitate "domain awareness" and may engage in "domain management." "Domain management" is the systematic process by which the FBI develops cross-programmatic domain awareness and leverages its knowledge to enhance its ability to: (i) proactively identify threats, vulnerabilities, and intelligence gaps; (ii) discover new opportunities for needed intelligence collection and prosecution; and (iii) set tripwires to provide advance warning of national security and criminal threats. Tripwires are described in DIOG Section 11. Effective domain management enables the FBI to identify significant threats, detect vulnerabilities within its local and national domain, identify new sources and threat indicators, and recognize new trends so that resources can be appropriately allocated at the local level in accordance with national priorities and local threats.

(U//~~FOUO~~) The field office "domain" is the territory for which a field office exercises responsibility, also known as the field office's area-of-responsibility (AOR). Domain awareness is the: (i) strategic understanding of national security and criminal threats and vulnerabilities that exist in the domain; (ii) FBI's positioning to collect against those threats and vulnerabilities; and (iii) the ability to recognize intelligence gaps related to the domain.

(U//~~FOUO~~) Through analysis of previously collected information, supplemented as necessary by properly authorized Type 4 Assessments, domain management should be undertaken at the local and national levels [redacted] b7E

[redacted] See DIOG Section 11 for further discussion of tripwires. Further guidance regarding domain management and examples of intelligence products are contained in the FBIHQ *Intelligence Program Policy Guide* (1150PG).

(U//~~FOUO~~) All information collected during a Type 4 Domain Assessment must be documented in the [redacted] b7E

[redacted] as directed in the [redacted]

[redacted] or predicated investigation must be opened [redacted]

(U//~~FOUO~~) FBIHQ DI provides specific guidance in its PG regarding, the opening, coordination and purpose for a field office and national domain Type 4 Assessments.

15.6.1.2 (U) WRITTEN INTELLIGENCE PRODUCTS

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

(U//~~FOUO~~) Pursuant to Rule 16 of the Federal Rules of Criminal Procedure, 18 U.S.C. Section 3500, and Department of Justice (DOJ) policy, written intelligence products, including classified intelligence products, may be subject to discovery in a criminal prosecution, if they relate to an investigation or are produced from information gathered during an investigation. Therefore, a copy of written intelligence products that are directly related to an investigation must be filed in the appropriate investigative file(s) and must include appropriate classification markings.

(U//~~FOUO~~) A copy of all written intelligence products must be placed in the appropriate investigative classification INTELPRODS sub-file.

15.6.1.3 (U) UNITED STATES PERSON (USPER) INFORMATION

(U//~~FOUO~~) Reports, Intelligence Assessments, and other FBI intelligence products should not contain USPER information, including the names of United States corporations or business entities, if the pertinent intelligence can be conveyed in an understandable way without including personally identifying information.

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

15.6.1.4 (U) INTELLIGENCE SYSTEMS

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

(U//~~FOUO~~) b7E

(U//~~FOUO~~) When developing a new database, the FBI Office of the General Counsel Privacy and Civil Liberties Unit must be consulted to determine whether a Privacy Impact Assessment (PIA) must be prepared.

15.6.1.5 (U) GEOSPATIAL INTELLIGENCE (GEOINT)

(U//~~FOUO~~) Geospatial Intelligence (GEOINT) is the exploitation and analysis of imagery and geospatial information to describe, assess and visually depict physical features and geographically-referenced activities on the Earth. As an intelligence discipline, GEOINT in the FBI encompasses all the activities involved in the collection, analysis, and exploitation of spatial information in order to gain knowledge about the national security/criminal environment and the visual depiction of that knowledge. GEOINT also represents a type of information or intelligence product, namely the information and knowledge that is produced as a result of the discipline's activities.

(U//~~FOUO~~) b7E

This Page is Intentionally Blank.

16 (U) UNDISCLOSED PARTICIPATION (UDP)

16.1 (U) OVERVIEW

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

16.1.1 *(U) AUTHORITIES*

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

(U) First, Executive Order (E.O.) 12333 broadly establishes policy for the United States Intelligence Community (USIC). Executive Order 12333 requires the adoption of procedures for undisclosed participation in organizations on behalf of elements of the USIC within the United States. Specifically, the Order provides "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 first disclosing such person's intelligence affiliation to appropriate officials of the organization, except in accordance with procedures established by the head of the Intelligence Community element concerned .... Such participation shall be authorized only if it is essential to achieving lawful purposes as determined by the Intelligence Community element head or designee." (E.O. 12333, Section 2.9, Undisclosed Participation in Organizations within the United States). The Order also provides, at Section 2.2, that "[n]othing in [E.O. 12333] shall be construed to apply to or interfere with any authorized civil or criminal law enforcement responsibility of any department or agency."

(U) Second, in addition to its role as member of the USIC, the FBI is also the primary criminal investigative agency of the federal government with authority and responsibility to investigate all violations of federal law that are not exclusively assigned to another federal agency. This includes the investigation of crimes involving international terrorism and espionage. As a criminal investigative agency, the FBI has the authority to engage in UDP as part of a predicated investigation or an Assessment. See 28 CFR 0.85 for additional guidance.

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

16.1.2 *(U) MITIGATION OF RISK*

(U//~~FOUO~~) b7E

b7E

16.1.3 *(U) SENSITIVE UDP DEFINED*

(U//~~FOUO~~)

16.1.4 *(U) NON-SENSITIVE UDP DEFINED*

(U//~~FOUO~~)

b7E

16.1.5 *(U) TYPE OF ACTIVITY*

(U//~~FOUO~~)

16.2 (U) PURPOSE, SCOPE, AND DEFINITIONS

16.2.1 *(U) ORGANIZATION*

(U//~~FOUO~~)

b7E

16.2.2 *(U) LEGITIMATE ORGANIZATION*

(U//~~FOUO~~)

b7E

b7E

16.2.3 *(U) PARTICIPATION*

(U//~~FOUO~~)

(U//~~FOUO~~) **UDP** may involve the following:

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

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

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

(U//~~FOUO~~)

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

(U//~~FOUO~~)

(U//~~FOUO~~) Examples of b7E

A) (U//~~FOUO~~) *Example 1:*

(U//~~FOUO~~) *Response to Example 1*:

b7E

B) (U//~~FOUO~~) *Example 2*:

(U//~~FOUO~~) *Response to Example 2*:

16.2.3.1 **(U) UNDISCLOSED PARTICIPATION**

(U//~~FOUO~~)

b7E

16.2.3.2 **(U//~~FOUO~~) INFLUENCING THE ACTIVITIES OF THE ORGANIZATION**

(U//~~FOUO~~)

16.2.3.3 **(U//~~FOUO~~) INFLUENCING THE EXERCISE OF FIRST AMENDMENT RIGHTS**

(U//~~FOUO~~)

16.2.3.4 **(U) APPROPRIATE OFFICIAL**

(U//~~FOUO~~)

b7E

16.2.3.5 **(U) SENSITIVE UNDISCLOSED PARTICIPATION**

(U//~~FOUO~~) Undisclosed participation in the activity of:

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

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

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

(U//~~FOUO~~)

(U//~~FOUO~~)

b7E

16.2.3.6 (U) ALREADY A MEMBER OF THE ORGANIZATION OR A PARTICIPANT IN ITS ACTIVITIES

(U//F~~OUO~~)

b7E

16.3 (U) REQUIREMENTS FOR APPROVAL

16.3.1 *(U) GENERAL REQUIREMENTS*

(U//~~FOUO~~)

16.3.1.1 (U) UNDERCOVER ACTIVITY

(U//F~~OUO~~)

b7E

b7E

16.3.1.2 **(U) CONCURRENT APPROVAL**

(U//~~FOUO~~)

16.3.1.3 **(U) DELEGATION AND "ACTING" STATUS**

(U//~~FOUO~~) b7E

(U//~~FOUO~~)

16.3.1.4 **(U) SPECIFIC REQUIREMENTS FOR GENERAL UNDISCLOSED PARTICIPATION (NON-SENSITIVE UDP)**

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

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

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

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

(U//~~FOUO~~)

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

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

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

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

16.3.1.5 **(U) SPECIFIC REQUIREMENTS FOR SENSITIVE UNDISCLOSED PARTICIPATION (SENSITIVE UDP)**

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

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

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

b7E

16.3.1.5.2 ***(U//~~FOUO~~)***

(U//~~FOUO~~)

16.3.1.5.3 ***(U//~~FOUO~~)***

(U//~~FOUO~~) b7E

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

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

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

16.4 (U) SUPERVISORY APPROVAL NOT REQUIRED

(U//~~FOUO~~) b7E

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

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

b7E

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

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

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

16.5 (U) STANDARDS FOR REVIEW AND APPROVAL

b7E

(U//~~FOUO~~)

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

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

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

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

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

b7E

(U//~~FOUO~~)

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

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

(U//~~FOUO~~)

(U//~~FOUO~~)

b7E

(U//~~FOUO~~)

16.6 (U) REQUESTS FOR APPROVAL OF UNDISCLOSED PARTICIPATION

(U//~~FOUO~~)

(U//~~FOUO~~) b7E

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

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

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

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

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

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

(U//~~FOUO~~) b7E

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

16.7 (U) DURATION

(U//~~FOUO~~) b7E

16.8 (U//~~FOUO~~) SENSITIVE OPERATIONS REVIEW COMMITTEE (SORC)

16.8.1 *(U//~~FOUO~~) SORC NOTIFICATION*

(U//~~FOUO~~) As indicated above, the field office will provide notification to the SORC, through the AD of the FBI Headquarters division with oversight responsibility for the investigation or Assessment concerning the following approved UDP:

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

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

(U//~~FOUO~~) Such notifications will be received by the FBI staff supporting the SORC. The SORC will receive reports of such UDP from the supporting staff on a schedule and in a form to be determined by the SORC.

16.8.2 *(U//~~FOUO~~) SORC REVIEW*

(U//~~FOUO~~) The SORC will review any proposed sensitive UDP in an organization b7E

(U//~~FOUO~~) For more details regarding the organization and functions of the SORC, see DIOG Section 10.2 above and Section 16.9 below.

16.9 (U) FBIHQ APPROVAL PROCESS OF UDP REQUESTS

16.9.1 *(U) SUBMITTING THE UDP REQUEST TO FBIHQ*

(U//~~FOUO~~)

b7E

(U//~~FOUO~~)

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

(U//~~FOUO~~)

16.9.3 ***(U//~~FOUO~~)***

(U//~~FOUO~~)

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

b7E

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

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

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

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

b7E

a) (U//~~FOUO~~)

b) (U//~~FOUO~~)

16.9.4 *(U//~~FOUO~~) PROCEDURES FOR APPROVING EMERGENCY UDP REQUESTS THAT OTHERWISE REQUIRE FBIHQ APPROVAL*

(U//~~FOUO~~) b7E

(U//~~FOUO~~)

(U//~~FOUO~~)

16.10 (U) UDP EXAMPLES

A) (U//~~FOUO~~) **Example A:** b7E

(U//~~FOUO~~) **Analysis A**

B) (U//~~FOUO~~) **Example B**

(U//~~FOUO~~) **Analysis B:** b7E

C) (U//~~FOUO~~) **Example C:**

(U//~~FOUO~~) **Analysis C:**

D) (U//~~FOUO~~) **Example D:** b7E

(U//~~FOUO~~) **Analysis D:**

E) (U//~~FOUO~~) **Example E:**

(U//~~FOUO~~) **Analysis E:**

b7E

F) (U//~~FOUO~~) **Example F**

(U//~~FOUO~~) **Analysis F**

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

(U//~~FOUO~~) **Analysis G**

(U//~~FOUO~~

(U//~~FOUO~~

b7E

H) (U//~~FOUO~~) **Example H:**

(U//~~FOUO~~) **Analysis H:**

I) (U//~~FOUO~~) **Example I:** b7E

(U//~~FOUO~~) **Analysis I:**

J) (U//~~FOUO~~) **Example J:**

(U//~~FOUO~~) **Analysis J:**

K) (U//~~FOUO~~) **Example K:**

(U//~~FOUO~~) **Analysis K:**

L) (U//~~FOUO~~) **Example L:**

b7E

(U//~~FOUO~~) **Analysis L:**

M) (U//~~FOUO~~) **Example M:**

(U//~~FOUO~~) **Analysis M:**

This Page is Intentionally Blank.

17 (U) OTHERWISE ILLEGAL ACTIVITY (OIA)

17.1 (U) OVERVIEW

(U//~~FOUO~~) Otherwise Illegal Activity (OIA) is conduct in the course of duties by an FBI employee (to include an undercover employee (UCE)) or a confidential human source (CHS) which constitutes a crime under local, state, or federal law if engaged in by a person acting without authorization. Certain types of OIA cannot be authorized, such as participation in conduct that would constitute an unlawful investigative technique (e.g., an illegal wiretap) or participation in an act of violence. In this context, "participation in an act of violence" does not include acts taken in self-defense and defense of others by the FBI employee or CHS because such actions would not be illegal.

17.2 (U) PURPOSE AND SCOPE

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

17.3 (U//~~FOUO~~) APPLICATION

(U//~~FOUO~~) OIA can be authorized for an FBI employee or CHS to obtain information or evidence necessary for the success of an investigation under the following limited circumstances:

A) (U//~~FOUO~~) when that information or evidence is not reasonably available without participation in the OIA;

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

C) (U//~~FOUO~~) when necessary to prevent serious bodily injury or death.

17.4 (U) LEGAL AUTHORITY

A) (U) The Attorney General's Guidelines for Domestic FBI Operations, Part V.C;

B) (U) The Attorney General's Guidelines on Federal Bureau of Investigation Undercover Operations, Part IV.H.

17.5 (U//~~FOUO~~) STANDARDS AND APPROVAL REQUIREMENTS FOR OIA

17.5.1 *(U) GENERAL APPROVAL REQUIREMENTS*

(U//~~FOUO~~) OIA that is not within the scope of [redacted] section 17.5.3, or is not part of an approved UCO, must be approved by the [redacted] (*AGG-Dom* Part V, Section C.3.) For national security related investigations, [redacted] is the approving component for OIA that requires approval beyond that authorized for SAC approval. However, as authorized by [redacted] may approve OIA in such investigations. For criminal b7E

investigations, [redacted] is the approving component for OIA that requires approval beyond that authorized [redacted] b7E

17.5.2 *(U) OIA IN AN UNDERCOVER ACTIVITY*

(U//~~FOUO~~) General: The use of the undercover method is discussed in the DIOG Section 18.6.13. OIA is often proposed as part of an undercover scenario or in making the initial undercover contacts before the operation is approved. Specific approval for OIA must be obtained in the context of these undercover activities or operations in addition to general approval of the scenario or the operation.

(U//~~FOUO~~) OIA by an FBI employee in an undercover operation relating to activity in violation of federal criminal law that does not concern a threat to the national security or foreign intelligence: must be approved in conformity with *The Attorney General's Guidelines on FBI Undercover Operations (AGG-UCO)*. Approval of OIA in conformity with the *AGG-UCO* is sufficient and satisfies any approval requirement that would otherwise apply under the AGG-Dom. Additional discussion is provided in the [redacted] b7E
[redacted] A Special Agent in Charge (SAC) may approve the OIA described in subsection 17.5.3.

(U//~~FOUO~~) OIA by an FBI employee in an undercover operation (UCO) relating to a threat to the national security or foreign intelligence collection must conform to the AGG-Dom and the FBI's [redacted]

17.5.3 *(U//~~FOUO~~) FIELD OFFICE REVIEW AND APPROVAL OF OIA FOR AN FBI AGENT OR EMPLOYEE*

(U//~~FOUO~~)An SAC may authorize the following OIA for an FBI employee only when consistent with other requirements of this section, the *AGG-Dom*, the *AGG-UCO*, and other FBI policy. OIA activities described in subsections B, C, D, and F below, require CDC review prior to SAC approval:

A) (U//~~FOUO~~) Otherwise illegal activity that would not be a felony under federal, state, local, or tribal law;

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

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

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

[26] (U//~~FOUO~~) In a controlled transaction, the item(s) will be monitored by the FBI and retained or seized at the conclusion of the transaction.

D) (U//~~FOUO~~) The payment of bribes or kickbacks[27];

(U//~~FOUO~~) *Note:* the payment of bribes and the amount of such bribes in a public corruption matter may be limited by other FBI policy (see the *Public Corruption Policy Guide, 0702PG* and the *Confidential Funding Policy Guide, 0248PG*);

E) (U//~~FOUO~~) The making of false representations in concealment of personal identity or the true ownership of a proprietary, but not including sworn testimony; and

F) (U//~~FOUO~~) Conducting a money laundering transactions [redacted] b7E
[redacted] involving an aggregate amount not exceeding $1 million;

G) (U//~~FOUO~~) The advertising or soliciting of unlawful goods or services; and

H) (U//~~FOUO~~) Gambling activities.

(U//~~FOUO~~) However, a SAC 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 SAC may authorize an activity that may otherwise violate prohibitions of [redacted] only in accordance with standards established by the Director of the FBI and agreed to by the Assistant Attorney General for National Security. (See DIOG subsection 17.5.5 for OIA related to [redacted]

(U//~~FOUO~~) The field office should notify the appropriate FBIHQ operational division and OGC of any OIA proposed activity that in the judgment of the approving official may expose employees or others to significant personal safety risks, create a risk of civil liability, result in adverse publicity, or raise any other sensitive operational concern. As a matter of FBI policy, "judgment" means that the decision of the authorizing official is discretionary.

(U//~~FOUO~~) An SAC may not authorize a violation of export control laws or laws that concern the proliferation of weapons of mass destruction during an investigation relating to a threat to the national security or foreign intelligence collection. See [redacted] b7E
[redacted] for additional guidance on OIA involving WMD counterproliferation and WMD related export violations. See also [redacted] for additional guidance on counterproliferation and export violations not involving WMD.

17.5.4 *(U//~~FOUO~~) OIA BY A CONFIDENTIAL HUMAN SOURCE (CHS) APPROVAL*

(U//~~FOUO~~) OIA by a CHS must be approved and documented in conformity with the *AGG-CHS* and the FBI Confidential Human Source Policy Guide (CHSPG), 1162PG.

[27] (U) Additional approval authority is necessary for the payment of bribes and kickbacks in undercover operations that are considered [redacted] See the [redacted] b7E
[redacted] and the *AGG-UCO*.

17.5.5 *(U//~~FOUO~~) OIA RELATED TO [redacted] INVESTIGATIONS* b7E

(U//~~FOUO~~) In accordance with Part V.C.3 of the AGG-Dom, the Director of the FBI and the Assistant Attorney General for the NSD of the DOJ established the following policy for FBI employees and CHS' concerning OIA as it relates to [redacted] investigations (see as reference EC dated 01/16/2009, 319W-HQ-A1487699-OGC Serial 35).

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

B) (U//~~FOUO~~) NSD has represented that, except in exceptional circumstances, NSD shall act upon such an oral request within 24 hours and shall, within 72 hours, provide the FBI documentation of the authorization, including any terms and conditions.

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

D) (U//~~FOUO~~) Except in exceptional circumstances, any request for approval of OIA tha[redacted] other than those described in paragraph A, must be made in writing to NSD.

(U//~~FOUO~~) For additional information regarding other governmental approvals that may be required for activities that are in violation of federal laws and regulations overseen by federal agencies other than the Department of Justice, see section 17.10.

17.5.5.1 (U//~~FOUO~~) PROCEDURES ON REQUESTS AND APPROVAL FOR OIA RELATED TO [redacted] b7E

(U//~~FOUO~~) For requests, standards of review, and approval procedures of OIA related to [redacted] see the [redacted]

(U//~~FOUO~~) Any questions about this policy or its implementation should be directed to OGC, National Security and Cyber Law Branch, Counterterrorism Law Units.

17.6 (U//~~FOUO~~) DOCUMENTATION OF REQUESTS TO ENGAGE IN OIA BY AN FBI AGENT OR EMPLOYEE

(U//~~FOUO~~) Requests to engage in OIA by an FBI agent or employee must be documented in an EC [redacted] and electronically placed into the appropriate investigative case file. The request must include: b7E

A) (U//~~FOUO~~) A synopsis of the investigation to date in which the OIA is being requested;

B) (U//~~FOUO~~) The name of the agent or employee who will engage in the OIA;

C) (U//~~FOUO~~)The specific proposed OIA in which the agent or employee will engage;

D) (U//~~FOUO~~) The expected duration of the OIA; and

E) (U//~~FOUO~~) Explanation of the justification for the use of OIA.

17.7 (U//~~FOUO~~) STANDARDS FOR REVIEW AND APPROVAL OF OIA

(U//~~FOUO~~) The appropriate approving official for the particular OIA must determine that the benefits to engaging in the requested OIA outweigh the risks involved and are necessary to:

A) (U//~~FOUO~~) To obtain information or evidence necessary for the success of the investigation and not reasonably available without participation in the otherwise illegal activity;

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

C) (U//~~FOUO~~) To prevent death or serious bodily injury.

(U//~~FOUO~~) The approval of OIA must be documented in an EC [redacted] and electronically placed into the appropriate investigative case file. The approval must include:

A) (U//~~FOUO~~) the specific OIA activities approved;

B) (U//~~FOUO~~) the duration of the OIA;

C) (U//~~FOUO~~) If the OIA is required to be approved by [redacted] a copy of the [redacted] approval letter must be electronically placed into the case file.

17.8 (U) OIA NOT AUTHORIZED

(U//~~FOUO~~) The following activities may not be authorized as OIA:

A) (U//~~FOUO~~) Directing or participating in acts of violence:

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

B) (U//~~FOUO~~) Activities or investigative methods that cannot be authorized because they are prohibited by law, including activities that would violate protected constitutional or federal statutory rights in the absence of a court order or warrant such as illegal wiretaps and searches. For example, approving a non-consensual, non-emergency wiretap without a court order; approving the search of a home without a warrant or an exception to the warrant requirement, etc.

17.9 APPROVAL AND DOCUMENTATION OF EMERGENCY OIA

(U//~~FOUO~~) Without prior approval, an FBI employee may engage in OIA that could be authorized under this section only if necessary to meet an immediate threat to the safety of persons or property or to the national security, or to prevent the compromise of an investigation or the loss of a significant investigative opportunity. In such a situation, prior to engaging in the OIA, every effort should be made by the FBI employee to consult with the SAC, and by the SAC to consult with the United States Attorney's Office (USAO) or appropriate DOJ Division where

the authorization of that office or division would be required unless the circumstances preclude such consultation. Circumstances in which OIA occur pursuant to this paragraph without the authorization required must be reported as soon as practicable, but not more than five (5) business days to the SAC, and by the SAC to FBIHQ and to the USAO or appropriate DOJ Division within five (5) business days of being notified. For the requirements for emergency authorization of OIA in [redacted] see the [redacted] b7E

17.10 OTHER GOVERNMENTAL APPROVALS

(U//~~FOUO~~) In addition to the approvals set forth above, additional coordination with other federal agencies may be necessary. Extraterritorial activity may involve conduct which would be in violation of laws and regulations overseen by federal agencies other than the Department of Justice. [redacted] b7E

[redacted] Upon FBI request, when necessary, each of those agencies may issue licenses to authorize activity that is otherwise prohibited.

This Page is Intentionally Blank.

(U//~~LES~~) Electronically Recorded Interviews

Quick Reference Guide

This QRG is for reference only and is not a substitute for official policy. For the most updated policies, see the *Domestic Investigations and Operations Guide* (DIOG) and/or relevant program policy.

b7E

Revised 9-10-18

18 (U) INVESTIGATIVE METHODS

18.1 (U) OVERVIEW

18.1.1 *(U) INVESTIGATIVE METHODS LISTED BY SUB-SECTION NUMBER*

(U) The following investigative methods are listed by DIOG Sub-Section number:

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) On-line services and resources.

18.5.5 (U) CHS use and recruitment.

18.5.6 (U) Interview or request information from the public or private entities.

18.5.7 (U) Information voluntarily provided by governmental or private entities.

18.5.8 (U) Physical Surveillance (not requiring a court order).

18.5.9 (U) Grand jury subpoenas – to providers of electronic communication services or remote computing services for subscriber or customer information only in Type 1 & 2 Assessments.

18.6.1 (U) Consensual monitoring of communications, including electronic communications.

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

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

18.6.4 (U) Administrative subpoenas.

18.6.5 (U) Grand jury subpoenas.

18.6.6 (U) National Security Letters.

18.6.7 (U) FISA Order for business records.

18.6.8 (U) Stored wire and electronic communications and transactional records.

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

18.6.10 (U) Mail covers.

18.6.11 (U) Polygraph examinations.

18.6.12 (U) Searches that Do Not Require a Warrant or Court Order (Trash Cover, Abandoned Property from a Public Receptacle, 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).

18.1.2 *(U) INVESTIGATIVE METHODS LISTED BY NAME (ALPHABETIZED)*

(U) The following investigative methods are listed alphabetized by DIOG name:

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

18.7.3)

(U) Electronic surveillance – Title III. (Section 18.7.2)

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

(U) Grand jury subpoenas. (Section 18.6.5)

(U) Grand jury subpoenas –to providers of electronic communication services or remote computing services for subscriber or customer information only in Type 1 & 2 Assessments. (Section 18.5.9)

(U) Information voluntarily provided by governmental or private entities. (Section 18.5.7)

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

(U) Interview or request information from the public or private entities. (Section 18.5.6)

(U) Mail covers. (Section 18.6.10)

(U) National Security Letters. (Section 18.6.6)

(U) On-line services and resources. (Section 18.5.4)

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

(U) Physical Surveillance (not requiring a court order). (Section 18.5.8)

(U) Polygraph examinations. (Section 18.6.11)

(U) Public information. (Section 18.5.1)

(U) Records or information - FBI and DOJ. (Section 18.5.2)

(U) Records or information - Other federal, state, local, tribal, or foreign government agency. (Section 18.5.3.1)

(U) Searches – with a warrant or court order. (Section 18.7.1)

(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) Stored wire and electronic communications and transactional records. (Section 18.6.8)

(U) Undercover Operations. (Section 18.6.13)

18.1.3 *(U) GENERAL OVERVIEW*

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

(U) The availability of a particular investigative method in a particular investigation may depend upon the level of investigative activity (Assessment, Preliminary Investigation, Full Investigation, and Assistance to Other Agencies).

18.1.4 *(U) CONDUCTING INVESTIGATIVE ACTIVITY IN ANOTHER FIELD OFFICE'S AOR*

(U) Investigative information that may be within another field office's AOR can generally be obtained by setting an investigative lead to that field office. However, investigative circumstances may require employees to travel to another office's AOR to conduct investigative activity. In such circumstances, an employee, with the approval of [redacted] and the [redacted] 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 [redacted] and advance [redacted] before entering another field office's AOR, notification should be made as soon as practicable to the [redacted] and [redacted] in the other office's AOR, including the type of investigative activity(s) that occurred and the circumstances that made obtaining prior approval and concurrence unfeasible. b7E

18.2 (U) LEAST INTRUSIVE METHOD

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

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

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

18.3 (U) PARTICULAR INVESTIGATIVE METHODS

(U//~~FOUO~~) All lawful investigative methods may be used in activities under the AGG-Dom as authorized by the AGG-Dom. Lawful investigative methods include those investigative methods contained in this DIOG as well as additional investigative methods and resources authorized in other FBI policy and guidance (for example, future additions to DIOG Sections 18, as well as PGs). In some instances the authorized investigative methods are subject to special restrictions or review or approval requirements. (AGG-Dom, Part V.A.)

18.3.1 *(U) USE OF CRIMINAL INVESTIGATIVE METHODS IN NATIONAL SECURITY INVESTIGATIONS*

(U//~~FOUO~~) Because national security investigations may implicate criminal issues as well, the availability of criminal investigative methods should be considered when appropriate. However, any use of criminal investigative methods should be closely coordinated with FBIHQ, both operational units and the NSCLB, prior to any anticipated use of this criminal investigative process. The NSCLB maintains liaison with DOJ OI respecting the use of FISA authorized investigative methods in national security investigations.

18.4 (U) INFORMATION OR EVIDENCE OBTAINED IN ASSESSMENTS AND PREDICATED INVESTIGATIONS

(U) The use, retention and/or dissemination of information obtained during authorized investigations must comply with the AGG-Dom and the DIOG. If the originator of information reported to the FBI characterizes an individual, group, or activity in a certain way, and that characterization should be documented for completeness of the FBI record, the FBI record (i.e., 302, EC, LHM) should reflect that another party, and not the FBI, is the originator of the characterization.

(U) During the course of an Assessment or predicated investigation, FBI employees lawfully may collect or passively receive items of evidence or intelligence from a variety of sources. Experience has demonstrated that the relevance of every item of evidence or intelligence collected or received is not always apparent at the time it is obtained. Accordingly, FBI employees have wide latitude to establish or determine the relevance of information as the Assessment or investigation develops. Nevertheless, as a matter of administrative efficiency and

sound business practice, if an FBI employee obtains an item of evidence which clearly is not relevant to the Assessment or investigation and there is no foreseeable future evidentiary or intelligence value of the item for the FBI or the USIC, the item should be returned or destroyed as circumstances warrant, with a record of the disposition documented in the file or in the Guardian FD-71a. Items that are lawfully collected, but for which the relevance is not immediately known, may be sequestered in the investigative file. If it is later determined that the item is relevant, the item may be used in the investigation upon such determination. The determination of relevancy will be made on a case-by-case basis with supervisory direction and may include consultation with the appropriate federal prosecuting office and/or the Chief Division Counsel (CDC) or the Office of the General Counsel (OGC). This policy does not supersede Sections 18.6.4.1 (Administrative Subpoenas); 18.6.5.1 (Federal Grand Jury Subpoena); 18.6.6.1 (National Security Letters); or 18.6.7 (FISA Order for Business Records), or any requirement imposed by statute, regulation or other applicable law.

18.5 (U) AUTHORIZED INVESTIGATIVE METHODS IN ASSESSMENTS

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

(U//~~FOUO~~) [redacted] in the Guardian FD-71a [redacted] b7E

[redacted]

(U) In conducting an Assessment, only the following investigative methods are authorized:

A) (U) Public information. (See Section 18.5.1)

B) (U) Records or information - FBI and DOJ. (See Section 18.5.2)

C) (U) Records or information - Other federal, state, local, tribal, or foreign government agency. (See Section 18.5.3.1)

D) (U) On-line services and resources. (See Section 18.5.4)

E) (U) CHS use and recruitment. (See Section 18.5.5)

F) (U) Interview or request information from the public or private entities. (See Section 18.5.6)

G) (U) Information voluntarily provided by governmental or private entities. (See Section 18.5.7)

H) (U) Physical Surveillance (not requiring a court order). (See Section 18.5.8)

I) (U//~~FOUO~~) Grand jury subpoenas - to providers of electronic communication services or remote computing services for subscriber or customer information only during a Type 1 & 2 Assessment (See Sections 18.5.9 and 18.6.5)

(U//~~FOUO~~) In Assessments, supervisory approval is required prior to use of the following investigative methods: certain interviews, tasking of a CHS in certain circumstances [redacted] b7E

[redacted] and physical surveillance not requiring [redacted]

This Page is Intentionally Blank.

18.5.1 *(U) INVESTIGATIVE METHOD: PUBLIC INFORMATION ("PUBLICLY AVAILABLE INFORMATION")*

18.5.1.1 (U) SCOPE

(U//~~FOUO~~) An FBI employee may obtain public information. (AGG-Dom, Part II.A.4.a and Part VII.L) Public information is "Publicly Available Information" that is:

A) (U) Published or broadcast for public consumption;

B) (U) Available on request to the public;

C) (U) Accessible on-line or otherwise to the public;

D) (U) Available to the public by subscription or purchase;

E) (U) Made available at a meeting open to the public;

F) (U) Obtained by visiting any place or attending an event that is open to the public (e.g., public places); or

G) (U) Observed, heard, smelled, detected or obtained by any casual observer or member of the public and does not involve unconsented intrusion into private places.

(U//~~FOUO~~) The phrase "observed, heard, smelled, detected or obtained by any casual observer or member of the public" includes, for example, plain view observations; overhearing a conversation taking place at an adjacent table in a public restaurant; odor detection (by a person, drug dog, or technical device) emanating from a vehicle, in a public place, or from locations to which the employee has gained lawful access; searching property that has been intentionally abandoned, including property discarded in public trash containers or public dumpsters (but does not include a "trash cover" as set forth in DIOG Section 18.6.12).

(U//~~FOUO~~) The following are examples:

1) (U) Viewing the vehicle identification number or personal property that is exposed to public view and may be seen when looking through the window of a car that is parked in an area that is open to and accessible by members of the public;

2) (U) The examination of books and magazines in a book store or the purchase of such items. See Maryland v. Macon, 472 U.S. 463 (1985); and

3) (U) A deliberate overflight in navigable air space to photograph marijuana plants is not a search, despite the landowner's subjective expectation of privacy. See California v. Ciraolo, 476 U.S. 207 (1986).

(U//~~FOUO~~) *Note:* Consent Searches are authorized in Assessments, as well as in predicated investigations.

(U//~~FOUO~~) *Note:* If the originator of information reported to the FBI characterizes an individual, group, or activity in a certain way, and that characterization should be documented for completeness of the FBI record, the FBI record (i.e., 302, EC, LHM) should reflect that another party, and not the FBI, is the originator of the characterization.

18.5.1.2 (U) APPLICATION

(U//~~FOUO~~) b7E

18.5.1.3 (U) APPROVAL

(U//~~FOUO~~) Supervisory approval is not required for use of this method, except for the special rule for attending a religious service, even if it is open to the public. (See DIOG Section 18.5.1.3.1)

18.5.1.3.1 *(U//~~FOUO~~) SPECIAL RULES: "SPECIAL RULE FOR RELIGIOUS SERVICES" AND "SPECIAL RULE FOR OTHER SENSITIVE ORGANIZATIONS"*

18.5.1.3.1.1 (U//~~FOUO~~) SPECIAL RULE FOR RELIGIOUS SERVICES – REGARDLESS OF WHETHER IT IS OPEN TO THE GENERAL PUBLIC

A) (U//~~FOUO~~) *In Assessments:* b7E
An FBI employee attending a religious service overtly must have SSA approval. Higher approvals may be required under certain circumstances, such as attendance that rises to the level of UDP (see DIOG Section 16)

B) (U//~~FOUO~~) *In Predicated Investigations:*
An FBI employee attending a religious service overtly must have SSA approval. Higher approvals may be required under certain circumstances, such as attendance that rises to the level of UDP (see DIOG Section 16) (see DIOG Section 18.6.13).

18.5.1.3.1.2 (U//~~FOUO~~) SPECIAL RULE FOR OTHER SENSITIVE ORGANIZATIONS

A) (U//~~FOUO~~) *In Assessments:* b7E

B) (U//~~FOUO~~) *In Predicated Investigations*

18.5.1.4 (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.

18.5.2 *(U) INVESTIGATIVE METHOD: RECORDS OR INFORMATION – FBI AND DEPARTMENT OF JUSTICE (DOJ)*

18.5.2.1 (U) SCOPE

(U//~~FOUO~~) An FBI employee may access and examine FBI and other DOJ records and may obtain information from any FBI personnel or other DOJ personnel. Access to certain FBI records may be restricted to designated FBI personnel because of the sensitive nature of the information in the record, the classification of the record, or the tool used to gather the information contained in the record. These include, but are not limited to: FBI records concerning human source identification; espionage investigations; code word; other compartmented information; records that include raw FISA collections; and Rule 6(e) material. (AGG-Dom, Part II.A.4.b)

(U//~~FOUO~~) *Note:* If the originator of information reported to the FBI characterizes an individual, group, or activity in a certain way, and that characterization should be documented for completeness of the FBI record, the FBI record (i.e., 302, EC, LHM) should reflect that another party, and not the FBI, is the originator of the characterization.

18.5.2.2 (U) APPLICATION

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

[redacted]

18.5.2.3 (U) APPROVAL

(U//~~FOUO~~) Supervisory approval is not required to use this method, except that if the use of records constitutes pattern-based data mining under the Federal Data Mining Reporting Act of 2007, it must be reviewed and approved according to Section 18.5.2.4 below.

18.5.2.4 (U) PATTERN-BASED DATA MINING

(U//~~FOUO~~) As used here, pattern-based data mining (PBDM) means queries or other analysis of electronic databases using two or more search criteria designed to discover or locate a predictive pattern or anomaly indicative of terrorist or criminal activity on the part of any individual or individuals (as defined in [redacted] b7E

[redacted] Any such analysis based solely on racial, ethnic, national origin or religious characteristics is strictly prohibited.

(U//~~FOUO~~) For purposes of this requirement, pattern-based data mining does not include activities using one or more personal identifiers to identify an individual or analysis designed to discover links between a specific subject and unknown individuals or entities, even if the subject's actual identity is not yet known. Pattern-based data mining does not include queries or analysis designed solely to identify potential human sources of intelligence nor does it include activities designed to identify an individual or individuals associated with criminal or terrorist activity that has already occurred. [redacted]

[redacted] In contrast, database queries using criteria [redacted]

[redacted] because the queries are being used to investigate a crime that has already occurred. Queries designed to identify individuals or entities who have had contact with a specific individual are not pattern-based data mining; rather, such queries are subject-based data mining, even if the specific individual's actual identity is presently unknown. b7E

(U//~~FOUO~~) The majority of data analysis performed during FBI Assessments and predicated investigations is based on specific individuals or events and therefore does not constitute pattern-based data mining because it is either link analysis or is not predictive of future behavior.

(U//~~FOUO~~) A Privacy Threshold Analysis (PTA) for pattern-based data mining must be completed and forwarded to the Privacy and Civil Liberties Unit, OGC. See the *Privacy Policy Implementation Guide*, 0299PG, for additional details.

(U//~~FOUO~~) The Sensitive Operations Review Committee (SORC) must also receive notice of any proposal to use pattern-based data mining as defined above. Additionally, pursuant to the *Federal Agency Data Mining Reporting Act of 2007*,[28] the FBI must advise the DOJ of all agency initiatives that involve the use of PBMD, so that those activities may be included in the Department's annual report to Congress. (See the *Pattern-based Data Mining Reporting Requirements Policy Directive*, 0310D).

18.5.2.5 (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.

(U//~~FOUO~~) The request for the records and the records received from DOJ and used during an Assessment or predicated investigation must be maintained as part of the appropriate file (e.g., 801 classification file, or investigation file).

[28] (U) 42 U.S.C. § 2000cc-3

This Page is Intentionally Blank.

18.5.3 *(U) INVESTIGATIVE METHOD: RECORDS OR INFORMATION – OTHER FEDERAL, STATE, LOCAL, TRIBAL, OR FOREIGN GOVERNMENT AGENCY*

18.5.3.1 (U) SCOPE

(U//~~FOUO~~) An FBI employee may access and examine records maintained by, and request information from, other federal, state, local, or tribal, or foreign governmental entities or agencies. When requesting information using this authority, care must be taken to ensure the entity to which the request is made understands that it is not compelled to provide such information or create a new record to assist the FBI. (AGG-Dom, Part II.A.4.c)

(U//~~FOUO~~) *Note:* If the originator of information reported to the FBI characterizes an individual, group, or activity in a certain way, and that characterization should be documented for completeness of the FBI record, the FBI record (i.e., 302, EC, LHM) should reflect that another party, and not the FBI, is the originator of the characterization.

18.5.3.2 (U) APPLICATION

(U//~~FOUO~~) b7E

18.5.3.3 (U) APPROVAL

(U//~~FOUO~~)

(U//~~FOUO~~) ***Requests to other Federal Agencies:*** The FBI may request, for a law enforcement purpose, that another federal agency disclose Privacy Act-protected records through a written request (5 U.S.C. 552a(b)(7)). Such written requests must be for a civil or criminal law enforcement purpose and must be made by the Director or his designee. (See 28 CFR 16.40(c); OMB Guidelines, 40 Fed. Reg. at 28 sec. 955.) Pursuant to these provisions, the Director hereby delegates his authority to request formally from federal agencies information and records otherwise protected from disclosure by the Privacy Act, at FBIHQ, to all Section Chiefs and above, and in the field, to all SACs and ADICs. This authority may not be redelegated to a person below the rank of SAC in the field and SC in FBIHQ.

(U) The FBI may also request another federal agency to disclose Privacy Act-protected records pursuant to that agency's published routine uses. See 5 U.S.C. sec. 552a(b)(3). These requests need not be made in writing, and there are no restrictions on which FBI personnel may ask for such information.

(U//~~FOUO~~) ***Requests to Foreign Agencies:*** Requests for records or information from a foreign government entity or agency must be appropriately coordinated through the applicable FBI LEGAT office, International Operations Division (IOD), INTERPOL, relevant FBIHQ operational division, and/or DOJ Office of International Affairs, as necessary. Direct contact with foreign government agencies is authorized in certain circumstances, such as an imminent threat situation.

(U//~~FOUO~~) If the analysis of records obtained in this manner constitutes Pattern-based Data Mining (PBDM) under the Federal Data Mining Reporting Act of 2007, it must be reviewed and approved according to Section 18.5.2.3, above.

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

[redacted]

18.5.3.4 **(U) USE/DISSEMINATION**

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

(U//~~FOUO~~) The request for the records and the records received from an outside entity and used during an Assessment or predicated investigation must be maintained as part of the appropriate file (e.g., 801 classification file, or investigation file).

This Page is Intentionally Blank.

18.5.4 *(U) INVESTIGATIVE METHOD: ON-LINE SERVICES AND RESOURCES*

18.5.4.1 (U) SCOPE

(U//~~FOUO~~) An FBI employee may use any online service or resource that is publically available or that the FBI has obtained by subscription or purchase for official use. This includes those online services and resources that are only available to law enforcement entities [redacted] (AGG-Dom, Part II.A.4.d) b7E

(U//~~FOUO~~) *Example:* Publicly available online services or resources include, but are not limited to [redacted] Online resources that may be purchased by the FBI for official use include, but are not limited to: [redacted]

(U//~~FOUO~~) *Note:* If the originator of information reported to the FBI characterizes an individual, group, or activity in a certain way, and that characterization should be documented for completeness of the FBI record, the FBI record (i.e., 302, EC, LHM) should reflect that another party, and not the FBI, is the originator of the characterization.

18.5.4.2 (U) APPLICATION

(U//~~FOUO~~) This investigative method may be used prior to opening an Assessment, in Assessments, predicated investigations, foreign intelligence collection investigations, and for assistance to other agencies in accordance with DIOG Section 12 ("Assistance to Other Agencies"). See DIOG Appendix L for additional information on the standards for on-line activity by FBI employees in both affiliated and nonaffiliated capacities, and in both public and private venues.

18.5.4.3 (U) APPROVAL

(U//~~FOUO~~) Supervisory approval is not required to use this method, although subscribing to or purchasing any new service or resource must be done according to FBI contracting procedures. Additionally, in many instances, employees are required to successfully complete on-line training curriculum prior to accessing or using FBI sponsored on-line applications, tools or, systems.

18.5.4.4 (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.

18.5.5 *(U) INVESTIGATIVE METHOD: CHS USE AND RECRUITMENT*

18.5.5.1 (U) SCOPE

(U//~~FOUO~~) The FBI may use and recruit human sources in Assessments and predicated investigations in conformity with the AGG-Dom, *Attorney General Guidelines Regarding the Use of FBI Confidential Human Sources (AGG-CHS)*, the *Confidential Human Source Policy Guide (CHSPG), 1162PG*, and the *Confidential Human Source Validation Standards Manual (CHSVSM), 0258PG*. (AGG-Dom, Part II.A.4.e) In this context, "use" means obtaining information from, tasking, or otherwise operating such sources. (AGG-Dom, Part VII.V)

(U//~~FOUO~~) *Note:* If the originator of information reported to the FBI characterizes an individual, group, or activity in a certain way, and that characterization should be documented for completeness of the FBI record, the FBI record (i.e., 302, EC, LHM) should reflect that another party, and not the FBI, is the originator of the characterization.

(U) [redacted] b7E

18.5.5.2 (U) APPLICATION

(U//~~FOUO~~) This investigative method may be used in Assessments, predicated investigations, foreign intelligence collection investigations, and for assistance to other agencies when it is not otherwise prohibited by AGG-Dom, Part III.B.2.

(U) When collecting positive foreign intelligence, the FBI must operate openly and consensually with an USPER, to the extent practicable.

(U//~~FOUO~~) A CHS can be "used" in support of an Assessment and a predicated investigation or for the purpose of validating, vetting or determining the suitability of another CHS as part of an Assessment.

18.5.5.3 (U) APPROVALS

(U//~~FOUO~~) All investigative methods should be evaluated to ensure compliance with the admonition that the FBI should use the least intrusive method if reasonable based upon the circumstances of the investigation. That requirement should be particularly observed during an Assessment when using a CHS because the use of a CHS during an Assessment may be more intrusive than many other investigative methods. Use of a CHS in an Assessment should take place only after considering whether there are effective, less intrusive means available to obtain the desired information. The CHS must comply with all constitutional, statutory, and regulatory restrictions and limitations. In addition:

A) (U//~~FOUO~~) CHS use and direction must be limited in focus and scope to what is necessary to accomplish the authorized purpose and objective of the Assessment or predicated investigation [redacted] b7E

B) (U//~~FOUO~~) During an Assessment [redacted] (see the Special Rule for Religious Services and the Special Rule for Other Sensitive Organizations below) only to the extent that such information is necessary to achieve the specific objective of the Assessment. If such contact reveals

information or facts about an individual, group or organization that meets the requirements to open a predicated investigation, a predicated investigation may be opened, as appropriate.

C) (U//~~FOUO~~) **Special Rule for Religious Services** – regardless of whether it is open to the general public:

1) (U//~~FOUO~~) ***In Assessments:*** b7E An FBI employee attending a religious service overtly must have SSA approval. Higher approvals may be required under certain circumstances, such as attendance that rises to the level of UDP (see DIOG Section 16).

2) (U//~~FOUO~~) ***In Predicated Investigations:*** An FBI employee attending a religious service overtly must have SSA approval. Higher approvals may be required under certain circumstances, such as attendance that rises to the level of UDP (see DIOG Section 16) (see DIOG Section 18.6.13).

D) (U//~~FOUO~~) **Special Rule for Other Sensitive Organizations:**

1) (U//~~FOUO~~) ***In Assessments:*** b7E

2) (U//~~FOUO~~) ***In Predicated Investigations***

E) (U//~~FOUO~~) **Public Information:**

F) (U//~~FOUO~~) **Non-Public Information**

G) (U//~~FOUO~~) This principle does not, however, eliminate the legal concept of a consent search or the doctrine of misplaced confidence that may be relied on by the government to gain access to otherwise protected places or information when the CHS has been granted access by a consenting party and the

CHS stays within the scope of the consent provided. The doctrine of misplaced confidence provides that a person assumes the risk when dealing with a third party that the third party might be a government agent and might breach the person's confidence.

b7E

(U) Example:

(U//~~FOUO~~) *Scenario*

(U//~~FOUO~~) *Response*

(U//~~FOUO~~)

18.5.5.4 (U//~~FOUO~~) Applicability of the Misplaced Confidence Doctrine During CHS Online Activity

U//~~FOUO~~)

b7E

(U//~~FOUO~~)

b7E

(U//~~FOUO~~

18.5.5.5 **(U) USE/DISSEMINATION**

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

This Page is Intentionally Blank.

18.5.6 *(U) INVESTIGATIVE METHOD: INTERVIEW OR REQUEST INFORMATION FROM THE PUBLIC OR PRIVATE ENTITIES*

18.5.6.1 (U) SCOPE

(U//~~FOUO~~) An interview is the questioning of an individual (including a subject or target) in order to gather information that is pertinent to and within the scope of an authorized Assessment or predicated investigation, or otherwise within the scope of FBI authority. An "interrogation" is a type of interview. For purposes of this policy provision, the terms "interview" and "interrogation" are interchangeable. In accordance with DIOG Section 5.1.1, the initial questioning of a complainant is not an interview, nor is re-contacting a complainant to clarify information that was initially provided. Normally, an FBI employee should disclose the employee's affiliation with the FBI and true purpose of the interview at the outset. The person being interviewed is voluntarily providing information and his/her Constitutional rights must be respected. (AGG-Dom, Part II.A.4.f and AGG-Dom, Part II.B.4)

(U//~~FOUO~~) It is the policy of the FBI that an employee[29] must not use force, threats, improper promises, or physical abuse when conducting an interview, or the threat of such abuse to the person being interviewed, or to any third party. It is also the policy of the FBI that an employee must not impose severe physical conditions on the person being interviewed.

(U//~~FOUO~~) All persons, whether in custody or not, located domestically or overseas, who are interviewed by FBI employees must be treated in accordance with FBI policy at all times. In addition, FBI employees must adhere, at all times, to the Constitution and laws of the United States, including but not limited to the prohibition against torture found in chapter 113C of Title 18, United States Code, when conducting any interview or interrogation regardless of geographic location of the interview or interrogation.

(U) During custodial and noncustodial interviews, when an agent knows or reasonably should know that the person being interviewed has a disability, reasonable and necessary steps must have taken to provide physical accessibility, reasonable accomodations, and effective communication. The factual circumstances of the interview will determine what reasonable and necessary steps should be taken.

(U//~~FOUO~~) FBI employees do not have the authority to promise leniency or immunity from prosecution. Additionally, the interviewer should make reasonable efforts to obtain information that is accurate, relevant, timely, and complete. An interview may only elicit a description of how an individual exercises a right guaranteed by the First Amendment to the Constitution if such information is pertinent to and within the scope of an authorized activity; similarly, regardless of how such information is elicited, it may not be maintained in FBI files unless it is pertinent to and within the scope of an authorized activity.

(U//~~FOUO~~) Nothing in this section prohibits asking for or accepting volunteered access to personal or real property. "Consent Searches" are authorized in Assessments, as well as in predicated investigations.

---

[29] The term "FBI employee" includes, but is not limited to, professional investigative staff, intelligence analyst, special agent, task force officer (TFO), task force member (TFM), task force participant (TFP), detailee, and FBI contractor.

(U//~~FOUO~~)

b7E

(U//~~FOUO~~) *Note:* If the originator of information reported to the FBI characterizes an individual, group, or activity in a certain way, and that characterization should be documented for completeness of the FBI record, the FBI record (i.e., 302, EC, LHM) should reflect that another party, and not the FBI, is the originator of the characterization.

18.5.6.2 (U) APPLICATION

(U//~~FOUO~~)

b7E

18.5.6.3 (U) VOLUNTARINESS

(U//~~FOUO~~) Information that is sought during an interview must be provided voluntarily. It is the policy of the FBI that an employee must not use force, threats, improper promises, or physical abuse when conducting an interview, or the threat of such abuse to the person being interviewed, or to any third party. It is also the policy of the FBI that an employee must not impose severe physical conditions on the person being interviewed.

(U//~~FOUO~~) FBI employees do not have the authority to promise leniency or immunity from prosecution. If, during a noncustodial interview, the interviewee indicates he or she wishes to consult an attorney, the interviewer should assess whether continuing the interview would negatively affect the voluntariness of any further information provided. In determining whether a statement has been given voluntarily, courts evaluate a "totality of the circumstances," which may include consideration of the following factors:

A) (U//~~FOUO~~) Whether the interviewee was notified of any charges against him/her or advised of his/her rights;

B) (U//~~FOUO~~) The interviewee's age, intelligence, experience, and physical condition;

C) (U//~~FOUO~~) Whether there was any physical abuse or threats of abuse during the interview;

b7E

D) (U//~~FOUO~~) The number of officers present and whether weapons were displayed during the interview;

E) (U//~~FOUO~~) Whether threats or psychological pressure was used during the interview;

F) (U//~~FOUO~~) Whether the interviewee was deprived of food, sleep, medication, or outside communication during the interview;

G) (U//~~FOUO~~) The duration of the interview, and whether any trickery, ruse, or deception was used; and

H) (U//~~FOUO~~) Whether there were any promises of leniency or other inducements made during the interview.

(U//~~FOUO~~) See Sections 18.5.6.3.8, 18.5.6.3.9, and 18.5.6.4.13 below for additional considerations when interviewing juveniles.

(U//~~FOUO~~) These factors are illustrative. The presence of any one or more of the factors mentioned above will not necessarily make a statement involuntary.

18.5.6.4 (U) APPROVAL/PROCEDURES

(U//~~FOUO~~) Generally, interviews do not require supervisory approval, except for:

A) (U//~~FOUO~~) Circumstances involving the Advice of Rights in Connection with Operational Terrorists inside the United States (See Section 18.5.6.4.1.4 below);

B) (U) Contact with Represented Parties (See Section 18.5.6.4.5 below);

C) (U) Member of the U.S. Congress and their Staffs (See Section 18.5.6.4.6 below);

D) (U) White House Personnel (See Section 18.5.6.4.7 below);

E) (U) Members of the News Media (See Section 18.5.6.4.8 below); and

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

(U//~~FOUO~~) PGs may require prior notice to FBIHQ for other interview types.

18.5.6.4.1 *(U) DOMESTIC CUSTODIAL INTERVIEWS*[32]

(U//~~FOUO~~) An FBI employee must advise a person who is in custody of his/her *Miranda* rights, per the *Advice of Rights, FD-395* form, before beginning an interview inside the United States with the exception of questioning reasonably prompted by a concern for public safety, (See DIOG Section 18.5.6.4.1.3 below), or questioning in connection with an operational terrorist inside the United States (See DIOG Section 18.5.6.4.1.4 below). It is critical that the person understand his/her rights before questioning. By signing the FD-395, the defendant acknowledges that he/she has been advised of his/her rights and is willing to proceed without a lawyer present. Once the advice of rights is provided and the interviewee voluntarily, knowingly, and intelligently waives those rights, the interview may proceed until such time as the interviewee invokes a right to silence and/or counsel. [redacted] b7E

[32] (U) For policy concerning interviews outside the United States, see Section 18.5.6.6.

[redacted] b7E

(U//~~FOUO~~) A person is "in custody" for purposes of *Miranda* when his/her freedom of movement is significantly restricted. Custody can arise short of formal arrest when, judging from the totality of the circumstances, a reasonable person in the position of the interviewee would believe that he/she is in custody. A brief, temporary investigative detention is not custody provided it is reasonable in scope. In assessing whether a temporary detention is reasonable in scope and thus not custody for purposes of *Miranda*, factors to consider include the degree of force used to affect the detention, use of restraining devices and whether the individual was moved from the location of the stop. Employees can clarify custodial status by telling the person that he/she is not under arrest. See DIOG subsection 18.5.6.4.17.3 below regarding requirements for recording custodial interviews. All statements made during a custodial interview of persons arrested by the FBI for federal crimes,[33] prior to initial appearance and while in a place of detention with suitable recording equipment, must be electronically recorded (with very limited exceptions as listed in DIOG subsection 18.5.6.4.17.4, below).

(U//~~FOUO~~) For specific requirements to interview a federal prisoner held in the custody of the Bureau of Prisons (BOP) or United States Marshals Service (USMS) see DIOG Appendix C.

18.5.6.4.1.1 (U) MIRANDA WARNINGS REQUIRED DOMESTICALLY

(U//~~FOUO~~) *Miranda* warnings are required when a person:

A) (U//~~FOUO~~) Has been arrested and is in federal, tribal, state, or local custody;

B) (U//~~FOUO~~) Is significantly restricted in his freedom of movement to a degree normally associated with a formal arrest; or

C) (U//~~FOUO~~) Regardless of custody, has previously been formally charged, prosecution is pending, and the subject matter of the interview concerns the pending charge.

(U//~~FOUO~~) For the purposes of *Miranda*, an interview refers to express questioning and any words or actions that are reasonably likely to elicit an incriminating response. In a custodial interview, the individual must be advised of the names and official identities of the employee(s) conducting the interview, the nature of the inquiry, and provided *Miranda* warnings, per the FD-395 form, before being interviewed. After being advised of his/her rights, if an interviewee who is in custody, invokes the right to counsel and/or the right to remain silent, this must be honored and the interview must cease. However, once the advice of rights is provided and the interviewee voluntarily, knowingly, and intelligently waives those rights, the interview may proceed until such time as the interviewee invokes a right to silence and/or counsel. [redacted] b7E

Once the interviewee invokes his or her right to remain silent and/or right to counsel, the interview must immediately be terminated. The fact that the interviewee invoked the right

[33] This policy does not apply to a person arrested for a state or local crime during a joint or Task Force investigation.

to counsel and/or the right to remain silent should be recorded on the FD-395 and the form should be executed in all other respects.

18.5.6.4.1.2 (U) MIRANDA WARNINGS NOT REQUIRED DOMESTICALLY

(U//~~FOUO~~) There are certain custodial interviews in which the protection *Miranda* provides against self-incrimination may not be served by reading the standard warnings and obtaining a waiver. In the following circumstances, *Miranda* warnings are not required for custodial interviews:

A) (U//~~FOUO~~) standard booking questions;

B) (U//~~FOUO~~) an interview of the incarcerated individual as a victim or witness in an unrelated matter that does not pertain to any pending charges against the interviewee;

C) (U//~~FOUO~~) the public safety exception (discussed in more detail below); and

D) (U//~~FOUO~~) in connection with arrests of operational terrorists inside the United States (discussed in more detail below).

18.5.6.4.1.3 (U//~~FOUO~~) PUBLIC SAFETY EXCEPTION

(U//~~FOUO~~) The warning and waiver of rights is not required when questions are asked that are reasonably prompted by a concern for public safety [redacted] b7E

[redacted] This public safety exception could also apply to other situations where imminent threat(s) to the safety of law enforcement officers or member(s) of the public could be alleviated by questions necessary to neutralize the threat.

18.5.6.4.1.4 (U//~~FOUO~~) ADVICE OF RIGHTS IN CONNECTION WITH ARRESTS OF OPERATIONAL TERRORISTS INSIDE THE UNITED STATES[34]

(U//~~FOUO~~) Identifying and apprehending suspected terrorists, interrogating them to obtain intelligence about terrorist activities and impending terrorist attacks, and lawfully detaining them so that they do not pose a continuing threat to our communities are critical to protecting the American people. The DOJ and the FBI believe that we can maximize our ability to accomplish these objectives by continuing to adhere to FBI policy regarding the use of *Miranda* warnings for custodial interrogation of operational terrorists[35] who are arrested inside the United States:

---

[34] (U//~~FOUO~~) This guidance applies only to arrestees who have not been indicted and who are not known to be represented by an attorney. For policy concerning the interrogation of indicted defendants, see Section 18.5.6.4.1; and for policy concerning contact with represented persons, see DIOG Section 18.5.6.4.5.

[35] (U//~~FOUO~~) For these purposes, an operational terrorist is an arrestee who is reasonably believed to be either a high-level member of an international terrorist group; or an operative who has personally conducted or attempted to conduct a terrorist operation that involved risk to life; or an individual knowledgeable about operational details of a pending terrorist operation.

A) (U//~~FOUO~~) If applicable, agents should ask any and all questions that are reasonably prompted by an immediate concern for the safety of the public or the arresting agents without advising the arrestee of his *Miranda* rights.[36]

B) (U//~~FOUO~~) After all applicable public safety questions have been exhausted, agents should advise the arrestee of his/her *Miranda* rights and seek a waiver of those rights before any further interrogation occurs, absent the exceptional circumstances described below.

C) (U//~~FOUO~~) There may be exceptional cases in which, although all relevant public safety questions have been asked, agents nonetheless conclude that continued unwarned interrogation is necessary to collect valuable and timely intelligence not related to any immediate threat, and that the government's interest in obtaining this intelligence outweighs the disadvantages of proceeding with unwarned interrogation.[37]

(U//~~FOUO~~) In these exceptional cases, agents must seek SAC approval, which cannot be delegated, to proceed with an unwarned interrogation after the public safety questioning is concluded. Whenever feasible, the SAC will consult with FBIHQ (including OGC) and DOJ attorneys before granting approval. Presentment of an arrestee may not be delayed simply to continue the interrogation, unless the arrestee has timely waived prompt presentment.

(U//~~FOUO~~) The determination whether particular unwarned questions are justified on public safety grounds must always be made on a case-by-case basis based on all the facts and circumstances. In light of the magnitude and complexity of the threat often posed by terrorist organizations, particularly international terrorist organizations, and the nature of their attacks, the circumstances surrounding an arrest of an operational terrorist may warrant significantly more extensive public safety interrogation without *Miranda* warnings than would be permissible in an ordinary criminal investigation. Depending on the facts, such interrogation might include, for example [redacted] b7E

[redacted]

(U//~~FOUO~~) As noted above, if there is time to consult with FBIHQ (including OGC) and Department of Justice attorneys regarding the interrogation strategy to be followed prior to reading the arrestee his *Miranda* rights, the field office should endeavor to do so. Nevertheless, the agents on the scene who are interacting with the arrestee are in the best

---

[36](U//~~FOUO~~) The Supreme Court held in *New York v. Quarles*, 467 U.S. 649 (1984), that if law enforcement officials engage in custodial interrogation of an individual that is "reasonably prompted by a concern for the public safety," any statements the individual provides in the course of such interrogation shall not be inadmissible in any criminal proceeding on the basis that the warnings described in *Miranda v. Arizona*, 384 U.S. 436 (1966), were not provided. The Court noted that this exception to the *Miranda* rule is a narrow one and that "in each case it will be circumscribed by the {public safety} exigency which justifies it." 467 U.S. at 657.

[37](U//~~FOUO~~) The Supreme Court has strongly suggested that an arrestee's Fifth Amendment right against self-incrimination is not violated at the time a statement is taken without *Miranda* warnings, but instead may be violated only if and when the government introduces an unwarned statement in a criminal proceeding against the defendant. *See Chavez v. Martinez*, 538 U.S. 760, 769 (2003) (plurality op.); *id.* at 789 (Kennedy, J., concurring in part and dissenting in part); *cf. also id.* at 778-79 (Souter, J., concurring in the judgment); *See also United States v. Patane*, 542 U.S. 630, 641 (2004) (plurality opinion) ("[V]iolations [of the Fifth Amendment right against self-incrimination] occur, if at all, only upon the admission of unwarned statements into evidence at trial."); *United States v. Verdugo-Urquidez*, 494 U.S. 259, 264 (1990) ("[A] violation [of the Fifth Amendment right against self-incrimination] occurs only at trial.").

position to assess what questions are necessary to secure their safety and the safety of the public, and how long the post-arrest interview can practically be delayed while interrogation strategy is being discussed.

18.5.6.4.2 *(U//~~FOUO~~) MIRANDA WARNINGS FOR SUSPECTS IN CUSTODY OVERSEAS*

(U//~~FOUO~~) The decision to use or not use *Miranda* warnings during an overseas custodial interrogation will have to be made on a case-by-case basis and weigh many factors. Overall, if there is a reasonable likelihood of a prosecution in a U.S. civilian criminal court of the person being interrogated while in custody overseas, agents should discuss with FBIHQ, FBI OGC, and DOJ whether warnings should be provided to the person being interrogated. Once the determination is made to provide *Miranda* warnings as part of an overseas custodial interrogation, if the person being interrogated invokes his right to remain silent or consult with an attorney, this invocation should be honored. If use of *Miranda* warnings is appropriate given the circumstances of the case, the following DOJ-approved modified waiver form should be used. The form is the *Standard Advice of Rights for Suspects in Foreign Custody, FD-1081*.

18.5.6.4.3 *(U) CONSTITUTIONAL RIGHTS TO SILENCE AND COUNSEL UNDER MIRANDA*

A) (U//~~FOUO~~) ***Silence:*** If a custodial interviewee invokes his/her right to remain silent, FBI employees should not attempt a subsequent interview until a significant period of time has elapsed (a two-hour period has been held to be significant) or the interviewee requests to be interviewed anew. In either case, an FBI employee will ensure that the interviewee is again advised of his/her *Miranda* rights and indicates that he/she understand those rights before further questioning. If the interviewee again asserts his/her right to remain silent or the right to counsel, questioning must cease at that time. Assertion of the right to silence, like assertion of the right to counsel, must be unequivocal and unambiguous. A waiver of the right to remain silent occurs when an interviewee knowingly and voluntarily makes a statement; assertion of the right to remain silent requires more than mere silence in the face of questioning. This right, like the right to counsel, can be invoked at any time during custodial interrogation. Agents may continue questioning someone who has not clearly invoked his/her right to remain silent, but if the custodial interviewee asserts his/her right to silence, questioning must cease at that time.

B) (U//~~FOUO~~) ***Counsel:*** If a custodial interviewee invokes his/her right to counsel, questioning must cease. FBI employees may not attempt a subsequent interview unless counsel is present, the custodial interviewee initiates contact, or there has been a break in custody of at least 14 days.

1) (U//~~FOUO~~) When a custodial interviewee who has invoked his/her right to counsel initiates a subsequent interview, an FBI employee must ensure that the interviewee is advised of and understands his/her *Miranda* rights before proceeding with the interview. Not every statement by a custodial interviewee can fairly be interpreted as initiating a subsequent interview. In order to constitute the initiation of an interview, the custodial interviewee must either directly request such or use words that are reasonably interpreted as expressing a desire to be interviewed. If the words used are ambiguous, the FBI employee should clarify the custodial interviewee's intent by asking directly whether the custodial interviewee wants to be interviewed. The words and responses, if any, to such clarifying questions should be documented. General conversation by a custodial interviewee cannot be interpreted as indicating a desire to be interviewed and cannot be

used standing alone to predicate a second interview after the right to counsel has been invoked. If the interviewee again asserts his/her right to counsel, or invokes his/her right to silence, questioning must cease at that time.

2) (U//~~FOUO~~) When an uncharged and/or unrepresented interviewee who has previously invoked his/her right to counsel experiences a break-in-custody of at least 14 days, he/she may be approached for a subsequent interview. FBI employees, however, must ensure that the custodial interviewee is again advised of and waives his/her *Miranda* rights before proceeding with the interview. A break-in-custody for these purposes can occur even if an interviewee is continuously incarcerated. Questions as to what constitutes a break-in-custody should be directed to the CDC or OGC.

3) (U//~~FOUO~~) Contact with a represented person outside the presence of his/her counsel may implicate state ethics rules for attorneys (AUSAs). Before making such contact, employees are encouraged to contact the CDC, OGC, or the USAO. Once a represented person has been charged, information may only be elicited from the person: 1) regarding an unrelated or uncharged matter or 2) when counsel is present. Questions as to whether an individual is in fact represented or may be questioned as to a particular matter should be directed to the CDC or OGC.

18.5.6.4.4 *(U) Sixth Amendment Right to Counsel*

(U//~~FOUO~~) The Sixth Amendment Right to Counsel requires the government to advise and obtain a waiver of the Right to Counsel prior to interviewing the person to whom the right has attached. The Right to Counsel attaches upon indictment regardless of whether the indicted person realizes an indictment has been returned. The Right to Counsel also attaches upon the filing of information and at the time of an initial appearance on a Federal Complaint. The Right to Counsel is offense specific. When applicable, a warning regarding the Right to Counsel and subsequent knowing and voluntary waiver must occur prior to an interview, regardless of whether the person is in custody. Providing a person with a *Miranda* warning and obtaining a waiver per the use of Form FD-395 will permit the interview of the person after the Right to Counsel has attached. The Sixth Amendment right to counsel does not prohibit the government from re-contacting the subject if the subject refuses initially to waive this right or otherwise has requested or obtained counsel following an Initial Appearance. However, further attempts to interview the subject may be prohibited if the subject invoked his right to counsel and remained in continuous custody or there was an insufficient break in custody (consistent with *Miranda* and its progeny). In addition [redacted] b7E

[redacted]

18.5.6.4.5 *(U) Contact with Represented Persons*

(U//~~FOUO~~) CDC or OGC review is required before contact with represented persons in the absence of prior notice to counsel. Such contact 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 CDC must follow applicable law and DOJ procedure when reviewing the request to contact the represented individual in the absence of prior notice to counsel. The SAC, CDC, or their designees, and the United States Attorney or his or her designees must consult periodically on applicable law and DOJ procedure relative to contact

with represented persons. The field office may raise inconsistent application of: (i) state ethics rules; or (ii) rules for contacts with represented persons with the USAO and request that it consult with the DOJ Professional Responsibility Advisory Office. (AGG-Dom, Part V.B.1)

18.5.6.4.6 *(U) MEMBERS OF THE UNITED STATES CONGRESS AND THEIR STAFFS*

(U//~~FOUO~~) Generally, FBI employees may accept information offered from Congressional offices just as they would accept information from other sources, and they may act upon it accordingly [redacted] b7E

[redacted]

18.5.6.4.7 *(U) WHITE HOUSE PERSONNEL*

(U//~~FOUO~~) FBI employees may accept information offered by White House personnel just as they would accept information from other sources, and they may act upon it accordingly. [redacted] b7E

[redacted] Additional guidance regarding contact with White House personnel may be found in the AG Memorandum captioned "Communications with White House and Congress" dated May 11, 2009. (See DIOG Appendix D) *Note:* [redacted]

[redacted]

18.5.6.4.8 *(U) MEMBERS OF THE NEWS MEDIA*

18.5.6.4.8.1 (U) APPROVAL REQUIREMENTS

(U) Attorney General approval, including notice to the Director of the DOJ's Office of Public Affairs, must be obtained prior to conducting an interview of a member of the news media for any offense which the member of the news media is suspected of having committed in the course of, or arising out of, the coverage or investigation of a news story, or while engaged in the performance of his/her official duties as a member of the news media. [redacted] b7E

[redacted]

(U//~~FOUO~~) Requests for this approval must be submitted with an EC to the AD of the operational FBIHQ division that is responsible for the investigative classification and the AD of the Office of Public Affairs (OPA). The requesting EC must be reviewed by the CDC and approved by the SAC after coordinating the request with the local USAO. The EC must contain the necessary facts and investigative justification for the interview consistent with the DOJ guidelines set forth in 28 CFR § 50.10(f). See also the *DOJ News*

Media Policy Memo, dated February 21, 2014, *DOJ News Media Policy*, and the *DOJ News Media Policy Memo, dated January 14, 2015*.

(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.

18.5.6.4.8.1.1 ***(U) EXIGENT CIRCUMSTANCES***

(U) [redacted] may authorize the questioning of a member of the news media as described in DIOG subsection *18*.5.6.4.8.1 if he/she determines that exigent use of such a technique is necessary [redacted] b7E

(U) [redacted]

(U) See also the *DOJ News Media Policy Memo, dated February 21, 2014*, *DOJ News Media Policy*, and the *DOJ News Media Policy Memo, dated January 14, 2015*.

18.5.6.4.8.2 **(U) USE OF SUBTERFUGE WITH A MEMBER OF THE NEWS MEDIA**

(U//~~FOUO~~) To the extent operational needs allow, investigators must operate openly and consensually with members of the news media [redacted]

After consultation with the OPA and OGC, the AD of the operational division must decide whether to approve the request. If the request requires approval by DOJ (because the interview is related to an offense committed by the member of the news media during the course of news gathering) the AD of the operational division is responsible for submitting all requests for approval to the DOJ per 28 CFR 50.10.

(U//~~FOUO~~) FBIHQ operational division PGs may contain additional notice requirements.

18.5.6.4.9 ***(U) DURING AN ASSESSMENT - REQUESTING INFORMATION WITHOUT REVEALING FBI AFFILIATION OR THE TRUE PURPOSE OF A REQUEST***

A) (U//~~FOUO~~) In the normal course of an interview, an FBI employee should divulge the employee's affiliation with the FBI and the true purpose of the interview.

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

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

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

b7E

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

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

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

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

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

6) (U//~~FOUO~~)

7) (U//~~FOUO~~)

(U//~~FOUO~~)

(U//~~FOUO~~)

(U//~~FOUO~~)

b7E

(U//~~FOUO~~)

18.5.6.4.10 ***(U) CONSULTATION AND DISCUSSION***

(U//~~FOUO~~)

18.5.6.4.11 ***(U) EXAMPLES***

18.5.6.4.11.1 **(U) EXAMPLE 1**

(U//~~FOUO~~)

b7E

(U//~~FOUO~~) Answer:

18.5.6.4.11.2 **(U) EXAMPLE 2**

(U//~~FOUO~~)

(U//~~FOUO~~) Answer

18.5.6.4.11.3 **(U) EXAMPLE 3**

(U//~~FOUO~~) b7E

(U//~~FOUO~~) Answer:

18.5.6.4.11.4 **(U) EXAMPLE 4**

(U//~~FOUO~~)

(U//~~FOUO~~) Answer:

18.5.6.4.11.5 **(U) EXAMPLE 5**

(U//~~FOUO~~) b7E

(U//~~FOUO~~) Answer:

18.5.6.4.11.6 **(U) EXAMPLE 6**

(U//~~FOUO~~)

b7E

(U//~~FOUO~~) Answer

18.5.6.4.11.7 **(U) EXAMPLE 7**

(U//~~FOUO~~)

b7E

(U//~~FOUO~~) Answer:

18.5.6.4.11.8 **(U) EXAMPLE 8**

(U//~~FOUO~~)

b7E

(U//~~FOUO~~) Answer

18.5.6.4.11.9 **(U) EXAMPLE 9**

(U//~~FOUO~~)

b7E

(U//~~FOUO~~) Answer

18.5.6.4.12 ***(U//~~FOUO~~) PREDICATED INVESTIGATIONS - REQUESTING INFORMATION WITHOUT REVEALING FBI AFFILIATION OR THE TRUE PURPOSE OF A REQUEST***

(U//~~FOUO~~) In the normal course of an interview, the FBI employee should divulge the employee's affiliation with the FBI and the true purpose of the interview b7E

(U//~~FOUO~~

18.5.6.4.13 ***(U//~~FOUO~~) INTERVIEWS OF MINOR VICTIMS AND WITNESSES, COGNITIVELY IMPAIRED VICTIMS AND WITNESSES, AND ADULTS WHO REPORT THAT THEY WERE VICTIMIZED AS MINORS***

(U//~~FOUO~~) Interviews of some victims and witnesses require additional consideration so that FBI employees can elicit accurate information while minimizing potential trauma. The provisions in this subsection apply to interviews of:

1. (U//~~FOUO~~) Minor victims and witnesses (i.e., victims and witnesses under the age of 18 years).
2. (U//~~FOUO~~) Cognitively impaired victims and witnesses.
3. (U//~~FOUO~~) Adults who report that they were victimized as minors.

(U//~~FOUO~~) When interviewing these victims and witnesses, FBI employees should consider all of the following factors:

A. (U//~~FOUO~~) The age, mental health, exposure to trauma, maturity, and competency of the victim or witness
B. (U//~~FOUO~~) Whether the victim or witness is an emancipated minor
C. (U//~~FOUO~~) The victim's or witness's relationship to the suspect(s)
D. (U//~~FOUO~~) Safety concerns
E. (U//~~FOUO~~) The gravity of the offense at issue

F. (U//~~FOUO~~) Any alternative sources of evidence
G. (U//~~FOUO~~) The importance of the information or potential testimony to the investigation
H. (U//~~FOUO~~) The victim's or witness's degree of involvement, if any, with the offense under investigation

(U//~~FOUO~~) Whenever feasible and appropriate under the circumstances of an investigation, FBI personnel should obtain consent to conduct an interview from the parent/guardian of a minor victim or witness, or the guardian/caregiver of a cognitively impaired adult victim or witness.

(U//~~FOUO~~) In accordance with the *Attorney General Guidelines for Victim and Witness Assistance* (AGG-VWA), the FBI is required, whenever possible, to utilize personnel properly trained in forensic interviewing techniques for interviews of minor victims and witnesses (see AGG-VWA Art. III, L.1.e(2)). This standard helps to elicit accurate information from minor victims and witnesses while minimizing potential trauma. Additionally, whenever possible, interviews of minor victims and witnesses regarding alleged abuse or sexual exploitation should take place in-person (rather than exclusively by telephone or video conference).[38] A forensic interview may also be appropriate for a victim or witness (of any age) who reports that he or she was victimized as a minor or who is cognitively impaired. See the *Victim Services Policy Guide* (1010PG) for additional standards concerning forensic interviews.

18.5.6.4.14 *(U) Interviews of Juvenile Subjects*

18.5.6.4.14.1 (U) Custodial Interviews (No Arrest)

(U//~~FOUO~~) If a juvenile is not placed under arrest, but is deemed to be "in custody" based on the objective circumstances surrounding the interview, the interviewer must advise the juvenile of his or her rights as set forth on the FD-395 before beginning an interview and cease the interview if the juvenile invokes a right. See DIOG subsection 18.5.6.4.1.

(U//~~FOUO~~) In determining whether a juvenile is in custody, agents must apply an objective test: Was there a formal arrest or a deprivation of freedom of movement equivalent to an arrest? If the juvenile's age is known to the interviewer or is objectively apparent, the juvenile's age must be considered in the custody analysis. Age is not necessarily the determining or decisive factor in every case, but should be carefully considered given that a reasonable adult may view the circumstances surrounding the interview differently than a reasonable juvenile.

18.5.6.4.14.2 (U) Interviews Between Arrests for Federal Offenses and Initial Appearances Before Magistrate Judges

(U//~~FOUO~~) The requirements of the Juvenile Delinquency Act apply after a juvenile, as defined by federal law, is arrested for a federal offense. See DIOG subsection 19.12 for policy on arrests of juveniles.

---

[38] (U//~~FOUO~~) Appropriate circumstances for using telephone or video conferencing technology may include (but are not limited to) situations in which a child and adolescent forensic interviewer (CAFI) conducts an interview of a minor victim in-person, with the case agent on the phone, or situations in which a minor victim is located outside the continental United States.

(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 (i.e., a 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.

(U//~~FOUO~~) Whether a juvenile may be interviewed for a confession or admission of his or her own guilt between the time of arrest for a federal offense and the initial appearance before the magistrate depends on the law of the circuit in which the arrest occurs and requires the approval of a CDC or an AUSA.

A. (U//~~FOUO~~) If a CDC or an AUSA approves an interview of a juvenile based on the law of the circuit, the juvenile may waive his or her Fifth Amendment rights and consent to an interview. Whether a waiver is knowing and voluntary will be determined based on the totality of the circumstances surrounding the interview. Among the factors the court will likely consider are:

   i. (U//F~~OUO~~) The juvenile's age, experience, education, background, and intelligence.
   ii. (U//F~~OUO~~) Whether the juvenile has the capacity to understand the warnings given, the nature of Fifth Amendment rights, and the consequences of waiving them.

   (U//F~~OUO~~) The presence and co-signature of a parent or guardian during the waiver of rights (FD-395) may not necessarily be required for a voluntary waiver, but is always a significant factor to be considered and tends to dispel claims of coercion.

   (U//F~~OUO~~) An agent may also question a juvenile concerning the guilt of a third party if such questioning does not cause any delay in bringing the juvenile before the magistrate.

   (U//F~~OUO~~) When an agent conducts a custodial interview of an arrested juvenile prior to initial appearance and while in a place of detention with suitable recording equipment, the interview must be recorded in accordance with DIOG subsection 18.5.6.4.17.3.

B. If the interview is <u>not</u> allowed under the law of the circuit, information volunteered by the arrested juvenile concerning his or her own guilt should be recorded in the agent's notes for use in subsequent proceedings. Any questions concerning the law that applies in the particular circuit should be directed to the CDC or AUSA.

18.5.6.4.14.3 (U) INTERVIEWS OF JUVENILES UNDER ARREST BY NON-FEDERAL LAW ENFORCEMENT

(U//~~FOUO~~) The requirements of the Juvenile Delinquency Act, as described in subsections 18.5.6.4.14.2 and 19.12. only apply when a juvenile (as defined by federal law) is arrested for a federal offense. Therefore, Juvenile Delinquency Act requirements do <u>not</u> apply if a juvenile is suspected of having committed a federal offense but is under arrest by state or local law enforcement officers on a state or local charge. FBI employees are cautioned, however, that they may not collude or create the appearance of collusion

with non-federal officers to delay an arrest on federal charges to circumvent the Juvenile Delinquency Act requirements. Agents should consult a CDC or AUSA as to the advisability of a juvenile interview under the particular circumstances.

18.5.6.4.15 ***(U) DOCUMENTATION***

(U//~~FOUO~~) When it is anticipated that the results of an interview may become the subject of court testimony, the interview must be recorded on an FD-302 [redacted] b7E
[redacted]. See DIOG subsection 18.5.6.4.16 below for guidance on the use of the FD-302. The FD-302 must contain a record of statements made by the interviewee and not contain the interviewer's opinion or contextual comments. If the interviewer's opinions or contextual comments are relevant, they must be documented in an EC or other appropriate document.

If the interviewee characterizes an individual, group, or activity in a certain way, FBI records (i.e., 302s, ECs, LHMs) should reflect that the interviewee, not the FBI, is the source of the characterization.

(U//~~FOUO~~) Certain types of written material developed during the course of an interview must be retained including:

A) (U//~~FOUO~~) Written statements signed by the witness. When possible, written statements should be taken in all investigations in which a confession or admission of guilt is obtained unless the confession is obtained during an electronically-recorded interview session. If a witness gives a signed statement, and then gives additional information orally, both the signed statement and the oral information should be recorded on an FD-302 or [redacted] b7E

B) (U//~~FOUO~~) Written statements, unsigned by the witness, but approved or adopted in any manner by the witness. An example of such a written statement would be a written statement that the subject orally admits is true but will not sign; and

C) (U//~~FOUO~~) Original notes of an interview when the results may become the subject of court testimony. Materials generated via email, text messages, or similar means during an online interview must be retained as original notes. Because some forms of synchronous communication tools, such as text messaging, have limited or no storage, print, or production capabilities, they should not be used for substantive communications with law enforcement colleagues or civilians who may become witnesses. **If these tools are, nonetheless, used for substantive communications as part of an interview, the communications must be memorialized verbatim in an FD-302.**

D) (U//~~FOUO~~) If an FBI employee and an AUSA conduct an interview, and the AUSA asks or tells the FBI employee to refrain from recording the substance of the interview or taking notes, the FBI employee should decline to participate in the interview and should not be present when it takes place unless the interview is part of the trial preparation of the witness (or unless another law enforcement agent present is given the responsibility for taking notes and documenting the substance of the interview). FBI employees generally do not report the substance of trial preparation unless new material information or impeachment information is developed. FBI employees should consult with the trial AUSA to determine how to document any new information, including impeaching information, developed during the trial preparation interviews.

E) (U) [redacted] b7E

b7E

(U) See also DIOG Section 3.3.1.14 (Retain Original Notes Made During An Investigation).

(U//~~FOUO~~) All original handwritten interview notes must be retained as "original note material" in the 1A section of a file. The original handwritten notes may be scanned, but the physical original handwritten notes must be retained regardless of whether or not the notes are scanned. Also see *Importing Nontransitory Records into Sentinel and Preserving Certain Investigative Nontransitory Records in Original Formats* (1601D).

18.5.6.4.16 ***(U) USE OF THE FD-302***

(U) **Documenting Information of Record:** Any matter that may be testimonial must be documented using an FD-302 within Sentinel[39]. b7E

(U) Whenever a person being interviewed could be called upon to testify at any time in a future trial, or hearing, the results of the interview must be reported in an FD-302.

(U) All FBI employees present during an interview b7E must be identified by name on the FD-302. The employee preparing the FD-302 is listed as the author of the document and all other employees present must be listed as co-authors. The author and co-author(s) of the FD-302 must review the FD-302, and then electronically sign the final FD-302 in Sentinel to attest it is accurate and complete. If someone other than an FBI employee and co-author(s) are present during the interview, the third party's presence during all or part of the interview must be noted in the FD-302.

(U) The FD-302 opening paragraph must state the official identity of the interviewing agent(s), the purpose of the interview, and the identity of the individual being interviewed to include relevant identifying information such as a date of birth, address, or other identifying data. It is also permissible to place more details or extensive personal, biographical, criminal history, business related information, other agency record information, etc in the body or at the end of the report. When an ongoing interview is carried out over a period of days, the dates should also be set out in the details of the FD-302. In such cases, the report should clearly delineate the particular date(s) the information was obtained. A composite interview report may be utilized in certain circumstances (see "composite FD-302" below for additional guidance).

(U) If during an interview, the interviewee provides unrelated information relevant to other criminal, national security, intelligence, or public safety matters from the original purpose of

[39] (U b7E

the interview, the interviewer may take the information. When documenting such unrelated information, each topic must be documented in a separate FD-302, filed to the appropriate investigative classification, and disseminated as appropriate.

(U) The preparation of the FD-302 must be initiated as soon as practicable, following the conclusion of the interview or other activity that may be testimonial. b7E

(U) Interview notes must be retained in accordance with DIOG subsections 3.3.1.14 and 18.5.6.4.15 above.

(U) **Composite FD-302**: In limited situations involving an extended or a series of related interviews of a subject, witness, or victim, the preparation of a composite FD-302 may be necessary. Preparation of a composite FD-302 at the conclusion of the interview may be the most logical and orderly way in which to document the totality of the interview. In these situations, in the judgment of the interviewer, a single composite FD-302 might be appropriate when:

(U) b7E

(U)

(U)

(U)

(U)

(U) If agents elect to prepare a composite FD-302, they must, without exception, ensure the composite FD-302 captures all material information in the extended interviews, including that which may also be considered exculpatory or impeaching. This includes, but is not limited to, any materially inconsistent statements of the witness and anything that may tend to mitigate guilt or punishment of the accused.

(U) The preparation of the composite FD-302 must be initiated as soon as practicable, following the conclusion of the last interview. b7E

(U) Interview notes must be retained in accordance with DIOG subsections 3.3.1.14 and 18.5.6.4.15.

(U) **Adoption of an FD-302**: In consultation with the assigned AUSA or DOJ attorney, the agent may seek to have the interviewee adopt an FD-302 as the statement he/she intended to give. Adoption by the witness may be in the form of (1) a signed statement, (2) an unsigned statement adopted by oral declaration, or (3) the report of information furnished by the witness, the substance of which was reviewed fully with the witness and adopted by the interviewee as the full and correct report of the statement he/she desired to furnish. Should the witness adopt an FD-302 as their statement, the agent must have the witness declare that it

represents a full and correct report of their statement and then sign and date the first page of the FD-302, including any corrections, edits or additions he/she make on that page. The witness should also initial and date each subsequent page of the report and also make any corrections, edits or additions to the FD-302. The adoption of the FD-302 by the witness can provide a defense to any allegations that the FD-302 represents information the interviewer claims the witness said, rather than what the witness actually stated. The original (i.e. physical paper version) FD-302 adopted by the witness should be retained in the 1A section of the investigative file after it has been scanned and electronically placed into the relevant investigative file(s).

18.5.6.4.17 *(U) ELECTRONIC RECORDING OF INTERVIEWS*

18.5.6.4.17.1 (U) OVERVIEW

(U) b7E

(U//~~FOUO~~)

(U//~~FOUO~~)

(U//~~FOUO~~)

18.5.6.4.17.2 (U) RECORDED NONCUSTODIAL INTERVIEWS

18.5.6.4.17.2.1 *(U) OVERTLY RECORDED NONCUSTODIAL INTERVIEWS*

(U//~~FOUO~~) FBI employees have the option to conduct an overtly recorded noncustodial interview. An overtly recorded interview occurs when an FBI employee, identified as such, advises the interviewee that the interview is or will be recorded, or the interviewee is otherwise clearly aware that the interview is in fact being recorded b7E

(U//~~FOUO~~) The FBI employee must provide notification to as soon as practicable after completion of an overtly recorded noncustodial interview(s). The notification may be in the form of the interview summary FD-302 described in DIOG subsection 18.5.6.4.17.2.2 below.

(U//~~FOUO~~) Additionally, prior to conducting the interview, the interviewing employee should consider the factors listed below [redacted] b7E

[redacted]

A. (U//~~FOUO~~) Whether the purpose of the interview is to gather evidence for prosecution or intelligence for analysis or both;
B. (U//~~FOUO~~) If prosecution is anticipated, the type and seriousness of the crime, including, in particular, whether the crime requires mens rea, or a mental element, such as knowledge or intent to defraud, proof of which would be considerably aided by the interviewee's admissions in his/her own words;
C. (U//~~FOUO~~) Whether the interviewee's own words and appearance (in video recordings) would help rebut any doubt about the meaning, context or voluntariness of his/her statement or confession raised by his/her age, mental state, educational level, or understanding of the English language; or is otherwise expected to be an issue at trial, such as to rebut an insanity defense; or may be of value to behavioral analysts;
D. (U//~~FOUO~~) If interviewers anticipate that the interviewee might be untruthful during an interview, whether a recording of the false statement would enhance the likelihood of charging and convicting the person for making a false statement;
E. (U//~~FOUO~~) The insufficiency of other available evidence to prove the charge beyond a reasonable doubt;
F. (U//~~FOUO~~) The preference of the USAO and the Federal District Court regarding recorded interviews or confessions;
G. (U//~~FOUO~~) Local laws and practice—particularly in task force investigations where state prosecution is possible;
H. (U//~~FOUO~~) Whether interviews with other witnesses or subjects in the same or related investigations have been electronically recorded; and
I. (U//~~FOUO~~) The potential to enlist the witness or subject's cooperation and the value of using his/her own words to elicit his/her cooperation.

18.5.6.4.17.2.2 *(U) Overtly Recorded Noncustodial Interview: Documentation and Handling*

(U//~~FOUO~~) After completing the recorded interview, the agent must document in an FD-302 the fact that the interview took place. [redacted] b7E

[redacted]

(U) b7E

(U//~~FOUO~~)

(U//~~FOUO~~)

(U//~~FOUO~~) Any handwritten notes taken during the recorded interview must be retained as original note material. See also DIOG Section 3.3.1.14 ("Retain Original Notes during an Investigation").

18.5.6.4.17.2.3 *(U) SURREPTITIOUSLY RECORDED NONCUSTODIAL INTERVIEWS*

(U//~~FOUO~~) b7E

18.5.6.4.17.2.4 *(U) SURREPTITIOUSLY RECORDED NONCUSTODIAL INTERVIEW: DOCUMENTATION AND HANDLING*

(U//~~FOUO~~) b7E

b7E

(U

(U//~~FOUO~~)

(U//~~FOUO~~)

(U//~~FOUO~~) Any handwritten notes taken during the recorded interview must be retained as original note material. See also DIOG Section 3.3.1.14 ("Retain Original Notes during an Investigation").

18.5.6.4.17.3 **(U) CUSTODIAL RECORDED INTERVIEWS (WARRANT/PROBABLE CAUSE)**

18.5.6.4.17.3.1 ***(U) OVERVIEW***

(U//~~FOUO~~) There is a presumption that statements made by persons in FBI custody must be recorded following arrest and prior to initial appearance when the arrestee is in a place of detention with suitable recording equipment. All statements made during a custodial interview of persons arrested by the FBI for federal crimes,[40] prior to initial appearance and while in a place of detention with suitable recording equipment, must be electronically recorded (with very limited exceptions as listed in DIOG subsection 18.5.6.4.17.4, below).

b7E

[40] This policy does not apply to a person arrested for a state or local crime during a joint or Task Force investigation.

b7E

(U//~~FOUO~~)

For factors bearing on voluntariness, see DIOG subsection 18.5.6.3. For factors bearing on Miranda compliance, see DIOG subsection 18.5.6.4.1.1

(U//~~FOUO~~) Employees must use suitable equipment as approved by b7E

(U//~~FOUO~~)

(U//~~FOUO~~)

18.5.6.4.17.3.2 ***(U) OVERTLY RECORDED CUSTODIAL INTERVIEWS***

(U//~~FOUO~~) FBI employees may conduct an overtly recorded custodial interview. An overtly recorded custodial interview occurs when an FBI employee, identified as such, advises the interviewee that the interview is or will be recorded, or the interviewee is otherwise clearly aware that the interview is in fact being recorded b7E

18.5.6.4.17.3.3 ***(U) OVERTLY RECORDED CUSTODIAL INTERVIEW: DOCUMENTATION AND HANDLING***

(U//~~FOUO~~) After completing the recorded interview, the agent must document in an FD-302 the fact that the interview took place.

b7E

(U) Transcription of the recording is optional. The FBI will provide electronic copies for distribution pre-indictment. Post-indictment, the USAO will pay for transcripts of recordings as necessary.

(U//~~FOUO~~) Any handwritten notes taken during the recorded interview must be retained as original note material. See DIOG Section 3.3.1.14 ("Retain Original Notes during Investigation").

(U//~~FOUO~~) b7E

18.5.6.4.17.3.4 *(U) SURREPTITIOUSLY RECORDED CUSTODIAL INTERVIEWS*

(U//~~FOUO~~) FBI employees may conduct a surreptitiously recorded custodial interview b7E

18.5.6.4.17.3.5 *(U) SURREPTITIOUSLY RECORDED CUSTODIAL INTERVIEW: DOCUMENTATION AND HANDLING*

(U//~~FOUO~~) After completing the recorded interview, the agent must document in an FD-302 the fact that the interview took place b7E

b7E

(U) Transcription of the recording is optional. The FBI will provide electronic copies for distribution pre-indictment. Post-indictment, the USAO will pay for transcripts of recordings as necessary.

(U//~~FOUO~~) Any handwritten notes taken during the recorded interview must be retained as original note material. See DIOG Section 3.3.1.14 ("Retain Original Notes during Investigation").

(U//~~FOUO~~ b7E

18.5.6.4.17.4 **(U) EXCEPTIONS TO MANDATORY RECORDING OF POST-ARREST CUSTODIAL INTERVIEWS**

(U//~~FOUO~~) Unless conducted pursuant to prior written approval, the interviewing employee must document in an EC, as soon as practicable b7E after the completion of the interview, the exercise of an exception to the mandated requirement to record a custodial post-arrest interview. The EC must be captioned, and must specifically address the reason(s) why the interview was not recorded Upon approval, the EC must be electronically placed into the substantive investigative case file, and a notification copy sent to the FBIHQ operational unit with program responsibility over the investigative classification, appropriate OGC/ILU or NLSB Unit, and to the Division's Compliance Officer. For tracking purposes and for a periodic review by DOJ, the EC must be electronically placed into file A copy of this EC documenting the basis for utilizing an exception to the mandatory recording of post-arrest custodial recorded interview policy must be made available to the AUSA by the "office of origin" field office overseeing the investigation.

A. (U//~~FOUO~~) Refusal of subject to be recorded during the interview: If the subject is advised that the interview will be recorded and they indicate that they are willing to provide a statement but wish not to be recorded, then the recording need not take place.

a. (U//~~FOUO~~)

b7E

B. (U//~~FOUO~~) Public Safety Exception: If the questioning is reasonably prompted by an immediate concern for the safety of the public or the arresting agent under New York v. Quarles then recording is not mandatory (see, e.g. DIOG 18.5.6.4.1.3).

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

a. (U//~~FOUO~~)

b7E

b. (U//~~FOUO~~)

c. (U//~~FOUO~~)

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

i. (U//~~FOUO~~)

ii. (U//~~FOUO~~)

iii. (U//~~FOUO~~)

iv. (U//~~FOUO~~)

v. (U//~~FOUO~~)

vi. (U//~~FOUO~~)

e. (U//~~FOUO~~) This is not meant to be an exhaustive list and other considerations may counsel in favor of b7E

D. (U//~~FOUO~~) Recording is not reasonably practicable: In the event that the circumstances of the arrest does not allow for the recording of the interview

E. (U//~~FOUO~~) "Residual" Exception: agree that a significant and articulable law enforcement purpose requires not recording the interview. Some considerations may include This exception is to be used judiciously and very infrequently.

18.5.6.4.17.5 (U) ELECTRONICALLY RECORDED INTERVIEW QUICK REFERENCE GUIDE

(U//~~FOUO~~) See Electronically Recorded Interview quick reference guide (QRG) in the IPO's QRG Library.

18.5.6.4.18 *(U) INTERVIEWS RELATING TO CLOSED FILES*

(U//~~FOUO~~) An interview initiated by an employee should only be conducted if it is within the scope of an open authorized Assessment or predicated investigation. On the other hand, there are situations in which an individual contacts the FBI to report information concerning a

matter that has been closed or placed in a zero file classification, or is unrelated to any current or previous investigation. In these situations, an FBI employee may collect whatever information the person is willing to provide, except solely First Amendment information, and may document the results of the contact in a Guardian FD-71a, an EC, or an FD-302. These documents may be electronically placed in files that are relevant to an open Assessment or predicated investigation, a closed Assessment or predicated investigation, a zero classification file, or a control file (if no further investigative activity is required).

(U//~~FOUO~~ b7E

18.5.6.4.19 *(U) FBIHQ Operational Division Requirements*

A) (U//~~FOUO~~) *Counterintelligence Division:* b7E

B) (U//~~FOUO~~) *Other FBIHQ Divisions:* Each FBIHQ division may provide additional interview notice requirements in its PG.

18.5.6.5 (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.

18.5.6.6 (U//~~FOUO~~) Overseas Interviews

18.5.6.6.1 *(U//~~FOUO~~) Interviews Outside the United States*

(U//~~FOUO~~) It is the policy of the FBI that an employee[41] b7E

(U//~~FOUO~~)

[41] The term "FBI employee" includes, but is 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.

b7E

(U

18.5.6.6.2 *(U//~~FOUO~~) MIRANDA WARNINGS FOR PERSONS IN CUSTODY OVERSEAS*

(U//~~FOUO~~)

b7E

This Page is Intentionally Blank.

18.5.7 *(U) INVESTIGATIVE METHOD: INFORMATION VOLUNTARILY PROVIDED BY GOVERNMENTAL OR PRIVATE ENTITIES*

18.5.7.1 (U) SCOPE

(U//~~FOUO~~) An FBI employee may accept information voluntarily provided by federal, state, local, tribal, or foreign governmental or private entities and individuals. (AGG-Dom, Part II.A.4.g) Voluntarily provided information includes, but is not limited to, oral as well as documentary and physical evidence such as a computer hard drive or other electronic media that contains information, paper documents containing information, or physical objects (e.g., handgun or narcotics).

(U//~~FOUO~~) Nothing in this section prohibits asking for or accepting volunteered access to personal or real property.

(U//~~FOUO~~) *Note:* Consent Searches are authorized in Assessments, as well as predicated investigations.

(U//~~FOUO~~) *Note:* If the originator of information reported to the FBI characterizes an individual, group, or activity in a certain way, and that characterization should be documented for completeness of the FBI record, the FBI record (i.e., 302, EC, LHM) should reflect that another party, and not the FBI, is the originator of the characterization.

18.5.7.2 (U) APPLICATION

(U//~~FOUO~~) b7E

18.5.7.3 (U) APPROVAL

(U//~~FOUO~~) Supervisory approval is not required to accept voluntarily provided information. Personnel may not request nor knowingly accept information where disclosure would be prohibited by federal law. See, e.g., 18 U.S.C. § 2702 (prohibiting an entity providing electronic communications services from divulging certain communications and other records, except in certain circumstances).

18.5.7.4 (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.

18.5.8 *(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~~)

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; b7E 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

18.5.8.2 **(U) APPLICATION**

(U//~~FOUO~~) b7E

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.

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

(U//~~FOUO~~) b7E

18.5.8.3.4 ***(U)***

(U//~~FOUO~~)

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 a 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~~)***

(U//~~FOUO~~)

b7E

(U//~~FOUO~~)

(U//~~FOUO~~)

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

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

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

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

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

(U//~~FOUO~~) b7E

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

(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] b7E
[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)

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] b7E
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.

18.5.9.3.1 *(U) MEMBERS OF THE NEWS MEDIA*[44]

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

[44] 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.

18.5.9.4 (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~~) b7E

a. (U

b. (U

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 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

[47] (U b7E

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.

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

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) On-line services and resources. (See Section 18.5.4)

5) (U) CHS use and recruitment. (See Section 18.5.5)

6) (U) Interview or request information from the public or private entities. (See Section 18.5.6)

7) (U) Information voluntarily provided by governmental or private entities. (See Section 18.5.7)

8) (U) Physical Surveillance (not requiring a court order). (See Section 18.5.8)

B) (U) 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)[49]

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)

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

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

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

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

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

(U//~~FOUO~~) [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)*, dated 11/18/2015, 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]

b7E

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

[redacted]

(U//~~FOUO~~) *For example:* b7E

[redacted]

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

[redacted]

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

(U//~~FOUO~~)

[redacted]

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 [redacted] except for the use of consensual computer monitoring discussed in subsection 18.6.1.6.1.2. b7E

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

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

(U//~~FOUO~~) **NOTE:** [redacted]

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

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

b7E

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

b7E

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:* b7E

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

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~~)

b7E

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

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

(U//~~FOUO~~)

(U//~~FOUO~~)

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-759s). 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

(U//~~FOUO~~)

b7E

(U//~~FOUO~~) For additional information see the [redacted] b7E

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//~~FOUO~~) 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//~~FOUO~~) 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//~~FOUO~~) 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//~~FOUO~~) 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//~~FOUO~~) 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//~~FOUO~~) 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 - [redacted] b7E

[redacted]

18.6.2.7.2 *(U) ACQUIRING ONLY THE TRESPASSER COMMUNICATIONS*

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

18.6.2.7.7 *(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-759s and *FD-1070 (Authorization to Intercept the Communications of a Computer Trespasser form)* 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 (LPR) Policy* 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 Guide, 0643DPG*.

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

(U//~~FOUO~~) When a video camera is physically operated as a hand-held video and is 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//~~FOUO~~) 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//~~FOUO~~) b7E

18.6.3.7 (U) SPECIFIC PROCEDURES

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

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

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

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

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//~~FOUO~~) ***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//~~FOUO~~) 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) [redacted] b7E

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

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

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 appropriate hyperlink to the VSU Web page.

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

(U) See VSU Intranet site.

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

(U) See VSU Intranet site.

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

(U) See VSU Intranet site.

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

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

[redacted] b7E

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..

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//~~FOUO~~) ***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//~~FOUO~~) ***Multi-offense investigations:*** [redacted] b7E

[redacted]

(U//~~FOUO~~) ***Confidentiality:*** [redacted]

[redacted]

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//~~FOUO~~) 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//~~FOUO~~) 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~~) b7E

(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. b7E

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.

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~~) [redacted] b7E

[redacted]

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. Additional guidance on toll record reimbursement, specific circumstances that preclude reimbursement, and a template telecommunications provider response letter, can be found on the [redacted] page at b7E

[redacted]

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~~)

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

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**[50]

(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.

[50] 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.

18.6.4.3.5 *(U) COMPLIANCE/MONITORING*

18.6.4.3.5.1 **(U) LIMITS ON USE**

(U//~~FOUO~~)

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//F~~OUO~~) 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//F~~OUO~~) 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.

This Page is Intentionally Blank.

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

18.6.5.1 (U) OVERVIEW OF COMPULSORY PROCESS[53]

(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. The Attorney General has issued revised guidance for the Disclosure and Use of Grand Jury Information under Rule 6(e)(3)(D) (hereinafter "*FGJ Guidelines*").

b7E

18.6.5.4 **(U) SCOPE**

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

[redacted]

[redacted] 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) [redacted] b7E

[redacted]

(U//~~FOUO~~) 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[54]

(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 *DOJ News Media Policy Memo, dated February 21, 2014*, *DOJ News Media Policy*, and the *DOJ News Media Policy Memo, dated January 14, 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.

18.6.5.8 (U) NOTICE AND REPORTING REQUIREMENTS

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

[54] 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.

18.6.5.9 (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. b7E

(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

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, 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.

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

b7E

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 *Guidelines for the Disclosure and Use of Grand Jury Information Under Rule 6(e)(3)(D)*, issued by the Deputy Attorney General on May 15, 2008, 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. b7E

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

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)(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//~~FOUO~~) 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. *(Guidelines for the Disclosure and Use of Grand Jury Information Under Rule 6(e)(3)(D))*, issued by the Deputy Attorney General on May 15, 2008.

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//~~FOUO~~) 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

b7E

C) (U//~~FOUO~~) 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//~~FOUO~~) 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] b7E
[redacted] in Guardian or another FBI system, [redacted] is entered into a computer database, the data must be marked with the 6(c) warning and [redacted] restricted within the system.

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(c) 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]

[58] [redacted]

b7E

(U//~~FOUO~~)

(U//~~FOUO~~)

(U//~~FOUO~~)

b7E

(U//~~FOUO~~)

(U//~~FOUO~~)

(U//~~FOUO~~)

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***

b7E

(U)

(U//~~FOUO~~)

(U//~~FOUO~~)

(U//~~FOUO~~)

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

(U//~~FOUO~~) b7E

(U//~~FOUO~~)

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

(U//~~FOUO~~) b7E

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

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

18.6.5.16 (U) FGJ MATERIAL COMPLIANCE AND MONITORING

(U//~~FOUO~~) [redacted] of 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 319O-HQ-A1561245-(field office designator). The field office may set its own unique

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~~)

b7E

(U//~~FOUO~~)

18.6.6.2 (U) APPLICATION

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

b7E

(U//~~FOUO~~)

(U//~~FOUO~~)

(U//~~FOUO~~)

b7E

(U//~~FOUO~~)

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

(U//~~FOUO~~)

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

(U//~~FOUO~~) b7E

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

(U//~~FOUO~~)

(U//~~FOUO~~)

(U//~~FOUO~~)

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

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

b7E

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

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

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

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

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

(U//~~FOUO~~)

(U//~~FOUO~~)

b7E

(U//~~FOUO~~)

(U//~~FOUO~~)

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

(U//~~FOUO~~)

b7E

(U//~~FOUO~~)

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

b7E

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

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

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

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

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

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

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

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

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**

(U//~~FOUO~~) b7E

[59] 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.

18.6.6.3.8 (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]

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

[redacted]

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

[redacted]

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

[redacted]

18.6.6.3.10 **(U) OVERPRODUCTION**

(U//~~FOUO~~)

b7E

(U//~~FOUO~~)

(U//~~FOUO~~)

b7E

(U//~~FOUO~~)

(U//~~FOUO~~)

(U//~~FOUO~~)

b7E

(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~~)

(U//~~FOUO~~)

b7E

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

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

(U//~~FOUO~~)

(U//~~FOUO~~) b7E

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

(U//~~FOUO~~)

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

(U//~~FOUO~~) b7E

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~~)

(U//~~FOUO~~)

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

(U//~~FOUO~~) b7E

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~~)

b7E

neither the NSL nor the return information is classified.

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

(U//~~FOUO~~)

b7E

(U//~~FOUO~~)

b7E

(U//~~FOUO~~)

(U//~~FOUO~~)

(U//~~FOUO~~)

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 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. b7E

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

(U//~~FOUO~~)

b7E

(U//~~FOUO~~)

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 b7E relevant to an authorized national security investigation

(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

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

(U//~~FOUO~~)

b7E

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

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

b7E

18.6.8.2 (U) APPLICATION

(U//~~FOUO~~)

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[60]

(U//~~FOUO~~) b7E

[60] 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) 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//~~FOUO~~) NOTICE—ORDERS NOT TO DISCLOSE THE EXISTENCE OF A WARRANT, SUBPOENA, OR COURT ORDER

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

(U)

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 a 18 U.S.C. § 2703(d) order); 18 U.S.C. § 2711(3) (court of competent jurisdiction includes any federal court having jurisdiction over the offense being investigated without geographic limitation).

(U) 18 U.S.C. § 2703(d) orders may also be issued by state courts. See 18 U.S.C. §§ 2711(3), 3127(2)(B). 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 on-line 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. b7E

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

(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) that there is reason to believe notification of the existence of the subpoena may have an adverse result. b7E

(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 [redacted] b7E

[redacted]

(U) [redacted]

[redacted]

(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) [redacted] b7E

[redacted]

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[63]: (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).

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

b7E

C) (U) ***Members of the News Media:***[64] 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***

(U)

b7E

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 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:

---

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

[64] 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.

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).

c) (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 [redacted] b7E

[redacted]

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

[redacted]

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]

b7E

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.

b7E

(U//~~FOUO~~)

b7E

(U//~~FOUO~~)

(U//~~FOUO~~) The 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

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~~)

C) (U//~~FOUO~~) *Filling Requirements:* [redacted] b7E

[redacted]

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 [redacted]

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 [redacted] 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/ILU, 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*[65]

(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.

[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*

(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 b7E must be made using

Routing a paper copy for signatures is not required. See the *Foreign Intelligence Surveillance Act aand Standard Minimization Procedures Policy Guide*, (1145PG), for additional guidance on FISA PR/TT requirements.

(U//~~FOUO~~) See the for additional guidance.

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.

18.6.9.5.1.3 (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~~) b7E

A) (U) The Attorney General may authorize the installation and use of a PR/TT upon a determination that an emergency exists and that the factual basis exists for a court order. The FISC must be informed at the time of the authorization and an application for a court order must be made to the court 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.

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, b7E

at any time.

18.6.9.5.1.4 (U) COMPLIANCE REQUIREMENTS

(U//~~FOUO~~) 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***[68]

(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.

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):

[68] 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.

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, b7E

During regular business hours,

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~~) b7E

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

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

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

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

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
[redacted] 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]
[redacted] These reporting requirements do not apply to PR/TT authorized pursuant to consent or under the provisions of FISA.

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

[redacted]

(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 b7E

content, except in cases of emergency—to prevent an immediate danger of death, serious physical injury, or harm to the national security.

(U//~~FOUO~~) b7E

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

(U//~~FOUO~~) b7E

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

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

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

(U//~~FOUO~~) b7E

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

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

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

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

b7E

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

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

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//~~FOUO~~)

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

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. b7E

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

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

(U//~~FOUO~~) ***Authority:*** b7E

(U//~~FOUO~~)

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

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

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) b7E

(U)

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~~) b7E

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

address information on the DIOG Resources Page.

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

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

(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~~) b7E

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

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

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

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

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~~)

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

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

(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)

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 b7E must be maintained in the investigative file. Other

communications between the FBI and the USPS [redacted] b7E
by subsection 18.6.10.8 [redacted]

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

[redacted] (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~~) [redacted] b7E

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

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

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

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.*** [redacted] b7E

B) (U//~~FOUO~~) ***National Security Mail Cover – Overproduction.*** [redacted]

b7E

This Page is Intentionally Blank.

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

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

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~~) b7E

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

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

(U)

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

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

[redacted]

18.6.11.5 **(U) DURATION OF APPROVAL**

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

[redacted]

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. [redacted]

[redacted]

This Page is Intentionally Blank.

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]

(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[71] OF A LOST OR MISPLACED ITEM*

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

b7E

D) (U

(U)

b7E

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~~) [redacted] b7E

[redacted] See the *Abandonment of Unclaimed Property Policy Guide*, 0820PG.

This Page is Intentionally Blank.

18.6.13 *(U) INVESTIGATIVE METHOD: UNDERCOVER OPERATIONS*

18.6.13.1 (U) SUMMARY

(U//~~FOUO~~) b7E

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

(U//~~FOUO~~) ***Application:*** b7E

18.6.13.2 (U) LEGAL AUTHORITY

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

B) (U) AGG-UCO

18.6.13.3 (U) DEFINITION OF INVESTIGATIVE METHOD

A) (U//~~FOUO~~) ***Undercover Activity (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//~~FOUO~~) The Covert Approach, which may be authorized in an approved Type 5 Assessment, pursuant to the procedures detailed in the CHSPG, is not undercover activity subject to the provisions of this section (DIOG 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//~~FOUO~~) ***Undercover Operation:*** An "undercover operation" is an operation that involves a series of related "undercover activities" over a period of time by an "undercover employee." A "series of related undercover activities" consists of more than five separate substantive contacts by an undercover employee with the individual(s) under investigation.

b7E

(U//~~FOUO~~)

b7E

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 the The Criminal Undercover Operations Review Committee (CUORC) and the 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 and the FBIHQ operational division PGs.

b7E

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

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

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

A) (U//~~FOUO~~) The risks of personal injury to individuals, property damage, financial loss to persons or business, damage to reputation, or other harm to persons;

B) (U//~~FOUO~~) The risk of civil liability or other loss to the government;

C) (U//~~FOUO~~) The risk of invasion of privacy or interference with privileged or confidential relationships and any potential constitutional concerns or other legal concerns;

D) (U//~~FOUO~~) The risk that individuals engaged in undercover operations may become involved in illegal conduct;

E) (U//~~FOUO~~) The suitability of government participation in the type of activity that is expected to occur during the operation (*AGG-UCO*, Part IV.A); and

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

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

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

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

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

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

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

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

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

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

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

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

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

18.6.13.4.3 ***(U//~~FOUO~~) APPROVAL REQUIREMENTS FOR UCOS*** b7E

(U//~~FOUO~~)

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

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

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

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

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~~) b7E

18.6.13.5 (U) OIA IN UNDERCOVER OPERATIONS

(U//~~FOUO~~)

A) (U)

B) (U

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

C) (U

D) (U

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

E) (U

F) (U

G) (U)

H) (U

(U

[72] (U) b7E

[73] (U)

(U//~~FOUO~~) b7E

18.6.13.6 **(U) DURATION OF APPROVAL**

(U//~~FOUO~~) b7E

18.6.13.7 **(U) ADDITIONAL GUIDANCE**

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

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

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

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

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

This Page is Intentionally Blank.

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) On-line services and resources. (See Section 18.5.4)
5) (U) CHS use and recruitment. (See Section 18.5.5)
6) (U) Interview or request information from the public or private entities. (See Section 18.5.6)
7) (U) Information voluntarily provided by governmental or private entities. (See Section 18.5.7)
8) (U) Physical Surveillance (not requiring a court order). (See Section 18.5.8)

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

1) (U) Consensual monitoring of communications, including electronic communications. (See Section 18.6.1)
2) (U) Intercepting the communications of a computer trespasser. (See Section 18.6.2)
3) (U) Closed-circuit television/video surveillance, direction finders, and other monitoring devices. (See Section 18.6.3)
4) (U) Administrative subpoenas. (See Section 18.6.4)
5) (U) Grand jury subpoenas. (See Section 18.6.5)
6) (U) National Security Letters. (See Section 18.6.6)
7) (U) FISA Order for business records. (See Section 18.6.7)
8) (U) Stored wire and electronic communications and transactional records. (See Section 18.6.8)[74]
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)

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

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

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

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

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

This Page is Intentionally Blank.

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

18.7.1.1 (U) SUMMARY

(U) The Fourth Amendment to the United States Constitution governs all searches and seizures by government agents. The Fourth Amendment contains two clauses. The first establishes the prohibition against unreasonable searches and seizures. The second provides that no warrant (authorizing a search or seizure) will be issued unless based on probable cause. Although an unlawful search may not preclude a prosecution, it can have serious consequences for the government. These include adverse publicity, civil liability against the employee or the government and the suppression of evidence from the illegal seizure.

(U//FOUO) ***Application*** b7E

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

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

18.7.1.2 (U) LEGAL AUTHORITY

(U) Searches conducted by the FBI must be in conformity with FRCP Rule 41; FISA, 50 U.S.C. §§ 1821-1829; 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. b7E

18.7.1.3.4.3 (U) Mail Openings

(U) Mail in United States postal channels may be searched only pursuant to court order, or presidential authorization. United States Postal Service regulations governing such

activities must be followed. A search of items that are being handled by individual couriers, or commercial courier companies, under circumstances in which there is a reasonable expectation of privacy, or have been sealed for deposit into postal channels, and that are discovered within properties or premises being searched, must be carried out according to unconsented FISA or FRCP Rule 41 physical search procedures.

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

(U) Contents in "electronic storage" (e.g., unopened e-mail/voice mail) require a search warrant. See 18 U.S.C. § 2703(a). A distinction is made between the contents of communications that are in electronic storage (e.g., unopened e-mail) for less than 180 days and those in "electronic storage" for longer than 180 days, or those that are no longer in "electronic storage" (e.g., opened e-mail). In enacting the ECPA, Congress concluded that customers may not retain a "reasonable expectation of privacy" in information sent to network providers. However, the contents of an e-mail message that is unopened should nonetheless be protected by Fourth Amendment standards, similar to the contents of a regularly mailed letter. On the other hand, if the contents of an unopened message are kept beyond six months or stored on behalf of the customer after the e-mail has been received or opened, it should be treated the same as a business record in the hands of a third party, such as an accountant or attorney. In that case, the government may subpoena the records from the third party without running afoul of either the Fourth or Fifth Amendment. If a search warrant is used, it may be served on the provider without notice to the customer or subscriber.

18.7.1.3.4.4.1 *(U) Search Warrant*

(U//~~FOUO~~) Investigators can obtain the full contents of a network account with a search warrant. ECPA does not require the government to notify the customer or subscriber when it obtains information from a provider using a search warrant. Warrants issued under 18 U.S.C. § 2703 must either comply with FRCP Rule 41 or be an equivalent state warrant. Warrants issued pursuant to 18 U.S.C. § 2703 do not require personal service on the customer; the warrants are only 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 a 18 U.S.C. § 2703(d) court order with notice.

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

18.7.1.3.4.4.2 *(U) NATIONWIDE SCOPE*

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

18.7.1.3.4.4.3 *(U) SERVICE OF PROCESS*

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

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

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

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

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

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

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

(U) b7E

(U)

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 a 18 U.S.C. § 2703[d] order); 18 U.S.C. § 2711(3) (court of competent jurisdiction includes any federal court having jurisdiction over the offense being investigated without geographic limitation).

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

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

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

A) (U) All "record(s) or other information pertaining to a subscriber to or customer of such service (not including the contents of communications [held by providers of electronic communications service and remote computing service])," and

B) (U) Basic subscriber information that can be obtained using a subpoena without notice. 18 U.S.C. § 2703(c)(1).

18.7.1.3.4.5 ***(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.

(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

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

18.7.1.5 (U) DURATION OF APPROVAL

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

18.7.1.6 (U) SPECIFIC PROCEDURES

18.7.1.6.1 *(U) OBTAINING A WARRANT UNDER FRCP RULE 41*

18.7.1.6.1.1 (U) PROBABLE CAUSE

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

18.7.1.6.1.2 (U) REQUESTING A WARRANT IN THE PRESENCE OF A JUDGE

A) (U) ***Warrant on an Affidavit:*** When a federal law enforcement officer or an attorney for the government presents an affidavit in support of a warrant, the judge may require the affiant to appear personally and may examine under oath the affiant and any witness the affiant produces.

B) (U) ***Warrant on Sworn Testimony:*** The judge may wholly or partially dispense with a written affidavit and base a warrant on sworn testimony if doing so is reasonable under the circumstances.

C) (U) ***Recording Testimony:*** Testimony taken in support of a warrant must be recorded by a court reporter or by a suitable recording device, and the judge must file the transcript or recording with the clerk, along with any affidavit.

---

[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.

18.7.1.6.1.3 (U) REQUESTING A WARRANT BY TELEPHONIC OR OTHER MEANS

A) (U) ***In General:*** A magistrate judge may issue a warrant based on information communicated by telephone or other appropriate means, including facsimile transmission.

B) (U) ***Recording Testimony:*** Upon learning that an applicant is requesting a warrant, a magistrate judge must: (i) place under oath the applicant and any person on whose testimony the application is based; and (ii) make a verbatim record of the conversation with a suitable recording device, if available, or by a court reporter, or in writing.

C) (U) ***Certifying Testimony:*** The magistrate judge must have any recording or court reporter's notes transcribed, certify the transcription's accuracy, and file a copy of the record and the transcription with the clerk. Any written verbatim record must be signed by the magistrate judge and filed with the clerk.

D) (U) ***Suppression Limited:*** Absent a finding of bad faith, evidence obtained from a warrant issued under FRCP Rule 41(d)(3)(A) is not subject to suppression on the ground that issuing the warrant in that manner was unreasonable under the circumstances.

18.7.1.6.1.4 (U) ISSUING THE WARRANT

(U) In general, the magistrate judge or a judge of a state court of record must issue the warrant to an officer authorized to execute it. The warrant must identify the person or property to be searched, identify any person or property to be seized, and designate the magistrate judge to whom it must be returned. The warrant must command the officer to: (i) execute the warrant within a specified time no longer than 14 days; (ii) execute the warrant during the daytime, unless the judge for good cause expressly authorizes execution at another time; and (iii) return the warrant to the magistrate judge designated in the warrant.

18.7.1.6.1.5 (U) WARRANT BY TELEPHONIC OR OTHER MEANS

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

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

B) (U) ***Preparing an Original Warrant:*** The magistrate judge must enter the contents of the proposed duplicate original warrant into an original warrant.

C) (U) ***Modifications:*** The magistrate judge may direct the applicant to modify the proposed duplicate original warrant. In that case, the judge must also modify the original warrant.

D) (U) ***Signing the Original Warrant and the Duplicate Original Warrant:*** Upon determining to issue the warrant, the magistrate judge must immediately sign the original warrant, enter on its face the exact time it is issued, and direct the applicant to sign the judge's name on the duplicate original warrant.

18.7.1.6.1.6 (U) WRITTEN OPERATION ORDERS FOR SEARCH OPERATIONS

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

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

(U) Prior to conducting a search operation deemed a high risk, the agent must prepare a written operation order (OPORDER) to include the five critical categories: Situation, Mission, Execution, Administration and Equipment, and Control and Communication (SMEAC), and must utilize the *Law Enforcement Operations Order (OPORDER), FD-888*. In situations where an FBI SWAT Team(s) or the Critical Incident Response Group's (CIRG), Tactical Section is involved, the Operations Order Template must be used in lieu of the FD-888. See the [redacted] b7E
and the [redacted] for more on the use of the SWAT Teams and CIRG, Tactical Section in high risk operations.

(U) When an agent knows or reasonably should know that an individual who may be encountered during the search operation has a disability, the disability must be accounted for in the same way as any other operational contingency.

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

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

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

18.7.1.6.1.7 (U) EXECUTING AND RETURNING THE WARRANT

A) (U) ***Noting the Time:*** The officer executing the warrant must enter on its face the exact date and time it is executed.

B) (U) ***Inventory:*** An officer present during the execution of the warrant must prepare and verify an inventory of any property seized. The officer must do so in the presence of another officer and the person from whom, or from whose premises, the property was taken. If either one is not present, the officer must prepare and verify the inventory in the presence of at least one other credible person.

C) (U) ***Receipt:*** The officer executing the warrant must: (i) give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken; or (ii) leave a copy of the warrant and receipt at the place where the officer took the property.

D) (U) ***Return:*** The officer executing the warrant must promptly return it — together with a copy of the inventory — to the magistrate judge designated on the warrant. The judge must, on request, give a copy of the inventory to the person from whom, or from whose premises, the property was taken and to the applicant for the warrant.

18.7.1.6.1.8 (U) FORWARDING PAPERS TO THE CLERK

(U) The magistrate judge to whom the warrant is returned must attach to the warrant a copy of the return, the inventory, and all other related papers and must deliver them to the clerk in the district where the property was seized. (FRCP Rule 41)

18.7.1.6.1.9 (U) WARRANT FOR A TRACKING DEVICE

A) (U) ***Noting the Time:*** The officer executing a tracking device warrant must enter on it the exact date and time the device was installed and the period during which it was used.

B) (U) ***Return:*** Within 10 calendar days after the use of the tracking device has ended, the officer executing the warrant must return it to the judge designated in the warrant.

C) (U) ***Service:*** Within 10 calendar days after use of the tracking device has ended, the officer executing the warrant must serve a copy of the warrant on the person who was tracked. Service may be accomplished by delivering a copy to the person who, or whose property was tracked; or by leaving a copy at the person's residence or usual place of abode with an individual of suitable age and discretion who resides at that location and by mailing a copy to the person's last known address. Upon request of the government, the judge may delay notice as provided in FRCP Rule 41(f)(3).

18.7.1.6.1.10 (U) DELAYED NOTICE

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

18.7.1.6.2 *(U) OBTAINING A FISA WARRANT*

(U) Applications for court-authorized physical search pursuant to FISA must be made by a federal officer in writing upon oath or affirmation and with the specific approval of the Attorney General. (See 50 U.S.C. § 1823). 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,* (1145PG), 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) 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).

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~~) b7E

(U//~~FOUO~~)

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 must be used for copies of all of the supporting documentation relied upon when making the certifications contained on the must include:

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

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

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

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

18.7.1.6.2.10 **(U//F~~OUO~~) FISA RENEWALS**

(U//~~FOUO~~)

b7E

b7E

(U//~~FOUO~~)

(U//~~FOUO~~)

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

(U//~~FOUO~~) b7E

18.7.1.6.2.11 **(U) COMPLIANCE AND MONITORING FOR FISA**

(U//~~FOUO~~) b7E

18.7.1.6.2.12 **(U) FISA OVERCOLLECTION**

(U//~~FOUO~~) b7E

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. b7E

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//~~FOUO~~) ***Application:***

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[78]

(U//~~FOUO~~) All Title III applications involving one of the seven "sensitive circumstances," listed below, including all extensions and renewals, must be reviewed by OGC and approved by FBIHQ. 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.

(U//~~FOUO~~) The field office must include a copy of the completed *CDC Title III Checklist (FD-926)* when forwarding the initial sensitive Title III applications to OGC and FBIHQ for

[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 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.

review. After the initial submission, the CDC checklist must be completed by the appropriate OGC unit for all subsequent extensions or renewals of sensitive Title IIIs.

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

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

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

B) (U//~~FOUO~~) Significant privacy concerns are anticipated (e.g., placing a microphone in a bedroom or bathroom);

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

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

E) (U//~~FOUO~~) Any situation deemed appropriate by the AD of CID or OGC.

(U//~~FOUO~~) The following two sensitive circumstances require the approval of the Director, the Acting Director, Deputy Director, or the Executive Assistant Director (EAD) for the Criminal Cyber Response and Services Branch or National Security Branch, or the respective Assistant Director for Criminal Investigative Division (CID), Cyber Division, Counterterrorism Division (CTD), Weapons of Mass Destruction Directorate (WMDD), or Counterintelligence Division (CD), and such approvals must be documented in an EC:

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

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

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

18.7.2.7 (U) PROCEDURES FOR EMERGENCY TITLE III INTERCEPTIONS

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

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

(U//~~FOUO~~) b7E

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

A) (U) immediate danger of death or serious physical injury to any person,

B) (U) conspiratorial activities threatening the national security interest, or

C) (U) conspiratorial activities characteristic of organized crime.

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

18.7.2.7.1 *(U) OBTAINING EMERGENCY AUTHORIZATION*

(U//~~FOUO~~) b7E

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

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

b7E

C) (U//~~FOUO~~

D) (U//~~FOUO~~

(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 b7E *form*, which must reflect the date and time of the emergency authorization.

(U//~~FOUO~~) The government may also request, at the time it files for court-authorization for the emergency, court-authorization to continue the interception beyond the initial 48 hour period. If continued authorization is sought at the same time, one affidavit may be submitted in support of both requests. However, the affidavit must clearly indicate what information was communicated to the AG or his designee at the time the emergency interception was approved and what information was developed thereafter. Two separate applications and proposed orders should be submitted to the court in this situation – one set for the emergency and one set for the extension. If continued interceptions are not being sought, no further authorization

is needed from OEO. The AUSA should, however, still submit the application, affidavit, and order to OEO for review. If continued interceptions are sought, that application, affidavit, and order must be reviewed by OEO and approved by DOJ like any other Title III request. In either situation, the affidavit must also be submitted through the operational unit for OGC review, when time allows.

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

A) (U//~~FOUO~~)
B) (U//~~FOUO~~)
C) (U//~~FOUO~~)

(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~~) 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 of the same persons (both subjects and interceptees), facilities or places named in the current affidavit. To comply with this requirement, a "search," e.g., an automated indices search of the FBI's 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

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] b7E

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

18.7.2.12.2 *(U//~~FOUO~~) Serializing Title III Documents*

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

b7E

(U//~~FOUO~~)

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

(U//~~FOUO~~)

18.7.2.12.4 ***(U//~~FOUO~~)***

(U//~~FOUO~~) b7E

18.7.2.12.5 ***(U//~~FOUO~~)***

(U//~~FOUO~~) b7E

(U//~~FOUO~~)

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

(U//F~~OUO~~) 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//~~FOUO~~)***

(U//~~FOUO~~)

b7E

(U//~~FOUO~~)

(U//~~FOUO~~)

18.7.2.12.8 ***(U//~~FOUO~~) TITLE III WIRETAP REPORT***

18.7.2.12.8.1 **(U//~~FOUO~~) REPORTING WIRETAP INFORMATION TO DOJ**

(U//~~FOUO~~) 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//~~FOUO~~) In support of DOJ's statutory obligation

b7E

18.7.2.12.8.2 **(U//~~FOUO~~)**

(U//~~FOUO~~)

b7E

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

b7E

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

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

18.7.2.12.8.3 **(U//~~FOUO~~)**

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

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

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

18.7.2.12.8.4 **(U//~~FOUO~~)**

(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 b7E

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

(U//~~FOUO~~) In joint FBI operations involving state and local law enforcement agencies wherein electronic surveillance is conducted through a federal Title III installation, any state officer being used as an affiant must be federally deputized. The FBI will be the administering agency responsible for the indexing and recordkeeping.

(U//~~FOUO~~) In joint FBI operations involving state and local law enforcement agencies wherein electronic surveillance is conducted pursuant to the authorization of a state court (i.e., a wiretap authorized by a state court, as opposed to a federal court), b7E

18.7.2.14 **(U) EVIDENCE HANDLING**

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

18.7.3.2.5.1 **(U//~~FOUO~~) FISA VERIFICATION OF ACCURACY PROCEDURES** b7E

(U//~~FOUO~~)

(U//~~FOUO~~)

(U//~~FOUO~~)

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

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

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

b7E

3) (U//~~FOUO~~

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

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

(U//~~FOUO~~) b7E

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

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

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

(U//~~FOUO~~) b7E

(U//~~FOUO~~)

(U//~~FOUO~~)

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~~) b7E

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

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

18.7.3.2.10 ***(U) OTHER APPLICABLE POLICIES***

18.7.3.2.10.1 **(U) FISA**

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

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

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

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

18.7.3.2.11 ***(U)COLLECTION HANDLING***

(U//~~FOUO~~) All ELSUR downloading, processing, and handling of original, derivative, and copies of original or derivative ELSUR evidence must be conducted by an ELSUR operations technician (EOT) or other designated official (e.g. an agent who has successfully completed ELSUR training in Virtual Academy). ELSUR evidence must not be uploaded into 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~~) b7E

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

2) (U)

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

18.7.3.3 (U) FISA Title VII (Acquisition of Foreign Intelligence Information)

18.7.3.3.1 *(U) Summary*

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

18.7.3.3.2 *(U) Legal Authority*

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

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

18.7.3.3.3 *(U) Definition of Investigative Method*

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

18.7.3.3.4 *(U//~~FOUO~~) Standards for Use and Approval Requirements for Investigative Method*

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

18.7.3.3.5 *(U) Duration of Approval*

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

18.7.3.3.6 *(U//~~FOUO~~) Specific Collection Procedures for Title VII*

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

18.7.3.3.6.1 (U) Section 702 - Procedures for Targeting Non-U.S. Persons (Non-USPERs) Who Are Outside the United States

(U//~~FOUO~~) Under Section 702, the Government has the authority to target non-USPERs who are located outside the United States if the collection is effected with the assistance of an electronic communication service provider, as that term is defined in FISA. This section does not require a traditional FISA request. Rather, under this section, the Attorney General and the Director of National Intelligence may authorize, for periods of

up to one year, the targeting of non-United States persons reasonably believed to be located outside the United States to acquire foreign intelligence information, provided they execute a Certification that is submitted to and approved by the FISC. The Certifications are accompanied by an affidavit signed by the FBI Director. In addition, the FBI is required to file "Targeting Procedures" that ensure that only non-U.S. persons (non-USPERs) reasonably believed to be located outside the United States will be targeted for collection and "to prevent the intentional acquisition of any communications as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States." Additionally, the statute prohibits targeting any person reasonably believed to be located outside the United States for the purpose of obtaining the communications of a particular, known person reasonably believed to be in the United States. Finally, the FBI is also required to follow 702-specific minimization procedures.

18.7.3.3.6.2 (U) SECTION 703 - CERTAIN ACQUISITIONS INSIDE THE UNITED STATES TARGETING UNITED STATES PERSONS OUTSIDE THE UNITED STATES

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

18.7.3.3.6.3 (U) SECTION 704 - OTHER ACQUISITIONS TARGETING UNITED STATES PERSONS OUTSIDE THE UNITED STATES

(U//~~FOUO~~) Under Section 704, the Government has the authority to target USPERs who are reasonably believed to be located outside the United States if the collection occurs outside the United States (i.e. without the assistance of a United States' electronic communication service provider). The statute requires that the FISA court issue an order finding probable cause to believe that the USPER target is a foreign power, an agent of a foreign power, or an officer or employee of a foreign power and is reasonably believed to be located outside the United States "under circumstances in which the targeted United States person has a reasonable expectation of privacy and a warrant would be required if the acquisition were conducted in the United States for law enforcement purposes." To obtain authority to collect information under this section, the FBI must submit a FISA request and obtain a FISC order (the order will not include secondary orders). The process to obtain a FISA 704 order is similar to, but more streamlined than, that for obtaining a traditional FISA under the standard FISA process. There are two notable differences between Section 704 and traditional FISA authorities. First, the application is not required to identify the specific facilities, places, premises, or property at which the acquisition will be directed. Second, Section 704 allows for the targeting of "an officer or employee of a foreign power" even if the target is not knowingly engaging in clandestine intelligence gathering activities, sabotage, or international terrorism. Refer to the FISA Unit's intranet website for further information. Section 704 also allows for emergency authorization. Unlike traditional FISA orders, however, surveillance authorized pursuant to this section must cease if the USPER enters the United States but may be re-started if the person is again reasonably believed to be outside the United States during the authorized period of surveillance. If there is a need to continue surveillance while the target is located inside the United States a separate court order must be obtained. The use of any information collected using FISA 704 authority must comply with the applicable minimization procedures.

(U//~~FOUO~~) b7E

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

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

(U//~~FOUO~~) Section 705(b) provides that if an order has been obtained under Section 105 (electronic surveillance under Title I of FISA) or 304 (physical search under Title III of FISA), the Attorney General may authorize the targeting of the USPER target while such person is reasonably believed to be located outside the United States. The Attorney General has this authority under E.O. 12333 § 2.5. In other words, when the FISA Court authorizes surveillance of an USPER target, the Attorney General, under Section 705(b)

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

(U//~~FOUO~~) b7E

18.7.3.3.6.5 **(U) FISA OVERCOLLECTION**

(U//~~FOUO~~) b7E

This Page is Intentionally Blank.

19 (U) ARREST PROCEDURE POLICY

19.1 (U) ARREST WARRANTS

19.1.1 *(U) COMPLAINTS*

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

19.1.2 *(U) ARREST WARRANTS*

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

19.1.3 *(U) JURISDICTION*

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

19.1.4 *(U) PERSON TO BE ARRESTED*

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

19.2 (U) ARREST WITH WARRANT

19.2.1 *(U) POLICY*

(U) Whenever possible, an arrest warrant must be obtained prior to an arrest. SSAs may authorize agents[80] to execute arrest warrants and, in extraordinary circumstances, FBIHQ should be notified in advance of the arrest. For example, SSAs should notify FBIHQ when the arrest may have a significant impact on an investigation in another field office or when the arrest is

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

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

(U) Upon the execution of an arrest warrant, the apprehending field office/division must promptly enter a "locate" within NCIC. The Office of Origin (OO) of the warrant must enter a "clear" within NCIC within 24 hours of the "locate." See DIOG subsection 19.4.4 (Initial Processing) below.

19.2.2 *(U) PROMPT EXECUTION*

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

19.2.3 *(U) ARREST PLANS*

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

(U) Prior to conducting an arrest operation deemed a high risk, the agent must prepare a written operation order (OPORDER) to include the five critical categories: Situation, Mission, Execution, Administration and Equipment, and Control and Communication (SMEAC), and must utilize the *Law Enforcement Operations Order (OPORDER), FD-888.* In situations where an FBI SWAT Team(s) or the Critical Incident Response Group's (CIRG), Tactical Section is involved, the Operations Order Template must be used in lieu of the FD-888. See the *Special Weapons and Tactics Policy Guide,* 0963PG and *Hostage Rescue Team Policy Guide,* 1051PG for more on the use of the SWAT Teams and CIRG's Tactical Section in high risk operations.

(U) When an agent knows or reasonably should know that an individual who may be encountered during the arrest operation has a disability, the disability must be accounted for in the same way as any other operational contingency.

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

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

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

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

19.2.4 *(U) ARREST TECHNIQUES – GENERAL*

(U) b7E

19.2.4.1 (U) INITIAL APPROACH DURING AN ARREST OPERATION

(U) 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

(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) b7E

(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*

(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.

19.2.4.5 (U) TRANSPORTATION OF ARRESTED PERSONS

(U) b7E

b7E

(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 circumstnaces.

(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 bodidly 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 insstructions on Form R-84. If the arresting agent(s) or TFO(s) cannot submit the arrestee's fingerprint electronically through JABS or ARES, the FD-249 "Criminal Fingerprint" card may be used as an alternative means to submit fingerprint to CJIS. The arresting agent(s) or TFO(s) must complete all known fields on the FD-249 card.

(U) [redacted] b7E

(See DIOG subsection 18.5.6.4.17 for guidance on [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.

19.4.4.1 (U) REQUESTS OF SUBJECTS IN CUSTODY

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

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

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

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

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

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

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

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

19.5 (U) USE OF FORCE

19.5.1 *(U) IDENTIFICATION*

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

19.5.2 *(U) PHYSICAL FORCE*

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

(U) [redacted] b7E

(U) See FBI Deadly Force Policy - *Appendix Ic (U) DOJ Policy on Use of Force.*

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

19.5.3 *(U) RESTRAINING DEVICES*

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

(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.

(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

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) b7E

(U)

(U)

(U)

(U)

(U)

b7E

(U) See also DIOG subsection 18.6.12.4.1.D

(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
Antigua and Barbuda	Hong Kong[81]	Saint Vincent and the Grenadines

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

(U) **Mandatory Notification Countries or Jurisdictions**

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[82]	Mauritius	Tunisia
Costa Rica	Moldova	Turkmenistan
Cyprus	Mongolia	Tuvalu
Czech Republic	Nigeria	Ukraine
Dominica	Philippines	United Kingdom[83]
Fiji	Poland (non-permanent residents only)	
Gambia	Romania	Uzbekistan
Georgia	Russia	Zambia
Ghana	Saint Kitts and Nevis	Zimbabwe
Grenada		

[82] (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.

[83] (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.

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

[redacted]

(U) The requesting field office seeking exigent authority must set out the circumstances that justify seeking exigent approval authority and communicate the basis for the request to [redacted] b7E

[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 documentation to DOJ, including documenting the receipt of AG approval. This documentation must be electronically placed into the case file.

(U) See also the *DOJ News Media Policy Memo, dated February 21, 2014*, *DOJ News Media Policy*, and the *DOJ News Media Policy Memo, dated January 14, 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 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.

b6
b7C

20 (U) OTHER INVESTIGATIVE RESOURCES

CLASSIFIED BY: NSICG
REASON: 1.4 (C)
DECLASSIFY ON: 12-31-2041
DATE: 08-02-2022
ALL INFORMATION CONTAINED HEREIN IS UNCLASSIFIED EXCEPT WHERE SHOWN OTHERWISE

20.1 (U) OVERVIEW

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

20.1.1 *(U//~~FOUO~~)* [redacted] *(CIA AND NSA)*

b3
b7E

(U) See Section 20.2 below.

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

(U) See Section 20.3 below.

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

(U) See Section 20.4 below.

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

(U) See Section 20.5 below.

20.2 (U//~~FOUO~~) [redacted] (CIA AND NSA)

b3
b7E

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

20.2.1 *(U) AUTHORIZED INVESTIGATIVE ACTIVITY*

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

b3
b7E

(U) See [redacted]

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

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

b1
b3
b7E

[redacted] The program reports the [redacted]

20.3.1 *(U) AUTHORIZED INVESTIGATIVE ACTIVITY*

b7E

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

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] b7E

[redacted]

(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 [redacted] b7E

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

(U//~~FOUO~~) Example 2: [redacted]

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

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

21.2 (U) FBI NATIONAL COLLECTION REQUIREMENTS

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

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

(U//~~FOUO~~) b7E

(U) For example:

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

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

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

(U//~~FOUO~~) Before any investigative activity is conducted in order to respond to an FBI national collection requirement, an Assessment or predicated investigation must be opened or already open. An Assessment cannot be opened solely based upon an FBI national collection requirement. An authorized purpose (national security or criminal threat) and clearly defined objective(s) must exist prior to opening an Assessment. During an Assessment, the FBI is authorized to collect against any FBI national collection requirement that is relevant to the Assessment. 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//~~FOUO~~) b7E

(U//~~FOUO~~)

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//F~~OUO~~) 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.