DOMESTIC INVESTIGATIONS AND OPERATIONS GUIDE

FEDERAL BUREAU OF INVESTIGATION
OCTOBER 15, 2011

NOTICE OF SUPERSESSION:

This document amends and supersedes the previous *Domestic Investigations and Operations Guide (DIOG)*, published December 16, 2008

CONTACT INFORMATION:

Questions or comments pertaining to the DIOG can be directed to:

The Resource Planning Office (RPO), Corporate Policy Office (CPO) at

HQ_DIV00_CORPORATE_POLICY_OFFICE

or the Office of the General Counsel (OGC)

PRIVILEGED INFORMATION:

Any use of this document, including direct quotes or identifiable paraphrasing, will be marked with the following statement:

This is a privileged document that cannot be released in whole or in part to persons or agencies outside the Federal Bureau of Investigation, nor can it be republished in whole or in part in any written form not containing this statement, including general use pamphlets, without the approval of the Director of the Federal Bureau of Investigation.

FOR OFFICIAL FBI INTERNAL USE ONLY—DO NOT DISSEMINATE
FOR OFFICIAL USE ONLY

TABLE OF CONTENTS

b7E

b7E

b7E

b7E

b7E

b7E

APPENDICES

This Page is Intentionally Blank.

(U) PREAMBLE

August 17, 2011

(U) As the primary investigative agency of the federal government, the FBI has the authority and responsibility to investigate all violations of federal law that are not exclusively assigned to another federal agency. The FBI is further vested by law and by Presidential directives with the primary role in carrying out criminal investigations and investigations of threats to the national security of the United States. This includes the lead domestic role in investigating international terrorist threats to the United States, and in conducting counterintelligence activities to counter foreign entities' espionage and intelligence efforts directed against the United States. The FBI is also vested with important functions in collecting foreign intelligence as a member agency of the United States Intelligence Community (USIC). (AGG-Dom, Introduction)

(U) While investigating crime, terrorism, and threats to the national security, and collecting foreign intelligence, the FBI must fully comply with all laws and regulations, including those designed to protect civil liberties and privacy. Through compliance, the FBI will continue to earn the support, confidence and respect of the people of the United States.

(U) To assist the FBI in its mission, the Attorney General signed the *Attorney General's Guidelines for Domestic FBI Operations* (AGG-Dom) on September 29, 2008. The primary purpose of the AGG-Dom and the Domestic Investigations and Operations Guide (DIOG) is to standardize policy so that criminal, national security, and foreign intelligence investigative activities are accomplished in a consistent manner, whenever possible (e.g., same approval, notification, and reporting requirements). In addition to the DIOG, each FBIHQ operational division has a policy implementation guide (PG) that supplements this document. Numerous FBI manuals, electronic communications, letterhead memoranda, and other policy documents are incorporated into the DIOG and the operational division policy implementation guides, thus, consolidating the FBI's policy guidance. The FBIHQ Corporate Policy Office (CPO) plays an instrumental role in this endeavor. Specifically, the CPO maintains the most current version of the DIOG on its website. As federal statutes, executive orders, Attorney General guidelines, FBI policies, or other relevant authorities change, CPO will electronically update the DIOG after appropriate coordination and required approvals.

(U) This revised DIOG is a direct result of more than 700 comments received from field and Headquarters employees after release of the initial DIOG in December 2008. Each suggestion was reviewed by a working group comprised of experienced field agents and Chief Division Counsels, as well as representatives from the CPO, the Office of General Counsel (OGC), and the Office of Integrity and Compliance (OIC). Many of these changes and suggestions have been incorporated in the revised DIOG. These changes to the DIOG should better equip you to protect the people of the United States against crime and threats to the national security and to collect foreign intelligence. This is your document, and it requires your input so that we can provide the best service to our nation. If you discover a need for change, please forward your suggestion to FBIHQ CPO.

(U) Thank you for your outstanding service!

Robert S. Mueller, III

Director

This Page is Intentionally Blank.

1 (U) SCOPE AND PURPOSE

1.1 (U) SCOPE

(U) The Domestic Investigations and Operations Guide (DIOG) applies to all investigative activities and intelligence collection activities conducted by the FBI within the United States, in the United States territories, or outside the territories of all countries. This policy document does not apply to investigative and intelligence collection activities of the FBI in foreign countries; those are governed by:

A) *(U) The Attorney General's Guidelines for Extraterritorial FBI Operations and Criminal Investigations*;

B) *(U) The Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection* (those portions which were not superseded by *The Attorney General Guidelines for Domestic FBI Operations*);

C) *(U) The Attorney General Guidelines on the Development and Operation of FBI Criminal Informants and Cooperative Witnesses in Extraterritorial Jurisdictions;*

D) *(U) The Attorney General Procedure for Reporting and Use of Information Concerning Violations of Law and Authorization for Participation in Otherwise Illegal Activity in FBI Foreign Intelligence, Counterintelligence or International Terrorism Intelligence Investigations (August 8, 1988; and*

E) *(U) Memorandum of Understanding Concerning Overseas and Domestic Activities of the Central Intelligence Agency and the Federal Bureau of Investigation* (2005).

(U//FOUO) Collectively, these guidelines and procedures are hereinafter referred to as the Extraterritorial Guidelines in the DIOG.

1.2 (U) PURPOSE

(U) The purpose of the DIOG is to standardize policies so that criminal, national security, and foreign intelligence investigative activities are consistently and uniformly accomplished whenever possible (e.g., same approval, opening/closing, notification, and reporting requirements).

(U) This policy document also stresses the importance of oversight and self-regulation to ensure that all investigative and intelligence collection activities are conducted within Constitutional and statutory parameters and that civil liberties and privacy are protected.

(U) In addition to this policy document, each FBI Headquarters (FBIHQ) operational division has a Policy Implementation Guide (PG) or several PGs that supplement the DIOG. These operational division PGs may not contradict, alter, or otherwise modify the standards established in the DIOG. As a result, numerous FBI manuals, electronic communications, letterhead memoranda, and other policy documents are incorporated into the DIOG and operational division PGs, thus, consolidating FBI policy guidance.

This Page is Intentionally Blank.

2 (U) GENERAL AUTHORITIES AND PRINCIPLES

2.1 (U) AUTHORITY OF THE ATTORNEY GENERAL'S GUIDELINES FOR DOMESTIC FBI OPERATIONS

(U) The *Attorney General's Guidelines for Domestic FBI Operations* (AGG-Dom) apply to investigative and intelligence collection activities conducted by the FBI within the United States, in the United States territories, or outside the territories of all countries. They do not apply to investigative and intelligence collection activities of the FBI in foreign countries, which are governed by the Extraterritorial Guidelines discussed in DIOG Section 13. (Reference: AGG-Dom, Part I.A.)

(U) The AGG-Dom replaces the following six guidelines:

A) *(U) The Attorney General's Guidelines on General Crimes, Racketeering Enterprise and Terrorism Enterprise Investigations (May 30, 2002);*

B) *(U) The Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection (October 31, 2003);*

C) *(U) The Attorney General's Supplemental Guidelines for Collection, Retention, and Dissemination of Foreign Intelligence (November 29, 2006);*

D) *(U) The Attorney General Procedure for Reporting and Use of Information Concerning Violations of Law and Authorization for Participation in Otherwise Illegal Activity in FBI Foreign Intelligence, Counterintelligence or International Terrorism Intelligence Investigations (August 8, 1988);*

E) *(U) The Attorney General's Guidelines for Reporting on Civil Disorders and Demonstrations Involving a Federal Interest (April 5, 1976); and*

F) *(U) The Attorney General's Procedures for Lawful, Warrantless Monitoring of Verbal Communications (May 30, 2002) [only portion applicable to FBI repealed].*

(U) Certain of the existing guidelines that are repealed by the AGG-Dom currently apply in part to extraterritorial operations, including the *Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection*, and the *Attorney General Procedure for Reporting and Use of Information Concerning Violations of Law and Authorization for Participation in Otherwise Illegal Activity in FBI Foreign Intelligence, Counterintelligence or International Terrorism Intelligence Investigations*. To ensure that there is no gap in the existence of guidelines for extraterritorial operations, these existing guidelines will remain in effect in their application to extraterritorial operations notwithstanding the general repeal of these existing guidelines by the AGG-Dom.

(U) Also, the classified *Attorney General Guidelines for Extraterritorial FBI Operation and Criminal Investigations* (1993) will continue to apply to FBI criminal investigations, pending the execution of the new guidelines for extraterritorial operations. Finally, for national security and foreign intelligence investigations, FBI investigative activities will continue to be processed as set forth in the classified *Memorandum of Understanding Concerning Overseas and Domestic Activities of the Central Intelligence Agency and the Federal Bureau of Investigation* (2005).

2.2 (U) General FBI Authorities under AGG-Dom

(U) The AGG-Dom recognizes four broad, general FBI authorities. (AGG-Dom, Part I.B.)

2.2.1 (U) Conduct Investigations and Collect Intelligence and Evidence

(U) The FBI is authorized to collect intelligence and to conduct investigations to detect, obtain information about, and prevent and protect against federal crimes and threats to the national security and to collect foreign intelligence, as provided in the DIOG (AGG-Dom, Part II).

(U) By regulation, the Attorney General has directed the FBI to investigate violations of the laws of the United States and to collect evidence in investigations in which the United States is or may be a party in interest, except in investigations in which such responsibility is by statute or otherwise specifically assigned to another investigative agency. The FBI's authority to investigate and to collect evidence involving criminal drug laws of the United States is concurrent with such authority of the Drug Enforcement Administration (DEA) (28 C.F.R. § 0.85[a]).

2.2.2 (U) Provide Investigative Assistance

(U) The FBI is authorized to provide investigative assistance to other federal, state, local, or tribal agencies, and foreign agencies as provided in Section 12 of the DIOG (AGG-Dom, Part III).

2.2.3 (U) Conduct Intelligence Analysis and Planning

(U) The FBI is authorized to conduct intelligence analysis and planning as provided in Section 15 of the DIOG (AGG-Dom, Part IV).

2.2.4 (U) Retain and Share Information

(U) The FBI is authorized to retain and to share information obtained pursuant to the AGG-Dom, as provided in Sections 12 and 14 of the DIOG (AGG-Dom, Part VI).

2.3 (U) FBI as an Intelligence Agency

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

(U) Part IV of the AGG-Dom authorizes the FBI to engage in intelligence analysis and planning, drawing on all lawful sources of information. The functions authorized under that Part includes: (i) development of overviews and analyses concerning threats to and vulnerabilities of the United States and its interests; (ii) research and analysis to produce reports and assessments (see note below) concerning matters relevant to investigative activities or other authorized FBI activities;

and (iii) the operation of intelligence systems that facilitate and support investigations through the compilation and analysis of data and information on an ongoing basis.

(U) *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 and objective (s) as discussed in the DIOG Section 5. The United States Intelligence Community (USIC), however, also uses the word "assessment" to describe written intelligence products as discussed in the DIOG Section 15.6.1.2.

2.4 (U) FBI LEAD INVESTIGATIVE AUTHORITIES

2.4.1 (U) INTRODUCTION

(U//FOUO) The FBI's primary investigative authority is derived from the authority of the Attorney General as provided in 28 U.S.C. §§ 509, 510, 533 and 534. Within this authority, the Attorney General may appoint officials to detect crimes against the United States and to conduct such other investigations regarding official matters under the control of the Department of Justice (DOJ) and the Department of State (DOS) as may be directed by the Attorney General (28 U.S.C. § 533). The Attorney General has delegated a number of his statutory authorities and granted other authorities to the Director of the FBI (28 C.F.R. § 0.85[a]). Some of these authorities apply both inside and outside the United States.

2.4.2 (U) TERRORISM AND COUNTERTERRORISM INVESTIGATIONS

(U) The Attorney General has directed the FBI to exercise Lead Agency responsibility in investigating all crimes for which DOJ has primary or concurrent jurisdiction and which involve terrorist activities or acts in preparation of terrorist activities within the statutory jurisdiction of the United States. Within the United States, this includes the collection, coordination, analysis, management and dissemination of intelligence and criminal information, as appropriate. If another federal agency identifies an individual who is engaged in terrorist activities or acts in preparation of terrorist activities, the other agency is required to promptly notify the FBI. Terrorism, in this context, includes the unlawful use of force and violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, to further political or social objectives (28 C.F.R. § 0.85[I]). For a current list of legal authorities relating to the FBI's investigative jurisdiction in terrorism investigations, see the OGC Law Library website at [redacted] b7E

(U//FOUO) DOJ guidance designates the FBI as Lead Agency for investigating explosives matters which, under the following protocol, demonstrate a possible nexus to international or domestic terrorism:

A) (U//FOUO) The following factors are strong indicia of a nexus to terrorism and lead-agency jurisdiction is assigned based on these factors alone:

1) (U//FOUO) an attack on a government building, mass transit, a power plant; or

2) (U//FOUO) the use of a chemical, biological, radiological, or nuclear agents.

B) (U//FOUO) Requires each agency to notify the other immediately when responding to an explosives incident and to share all relevant information that may serve to rule in or out a connection to terrorism; and

C) (U//FOUO) Creates a process for the FBI/Joint Terrorism Task Force (JTTF) to identify an explosives incident as connected to terrorism when there is reliable evidence supporting that claim and establishes a process for shifting lead-agency jurisdiction to the JTTF until the issue is resolved. (See DOJ Memorandum, dated August 3, 2010, on "Protocol for Assigning Lead Agency Jurisdiction in Explosives Investigations.")

2.4.2.1 (U) "FEDERAL CRIMES OF TERRORISM"

(U) Pursuant to the delegation in 28 C.F.R. § 0.85(l), the FBI exercises the Attorney General's lead investigative responsibility under 18 U.S.C. § 2332b(f) for all "federal crimes of terrorism" as identified in that statute. Many of these statutes grant the FBI extraterritorial investigative responsibility (See the cited statute for the full particulars concerning elements of the offense, jurisdiction, etc.). Under 18 U.S.C. § 2332b(g)(5), the term "federal crime of terrorism" means an offense that is: (i) calculated to influence or affect the conduct of government by intimidation or coercion or to retaliate against government conduct; and (ii) violates a federal statute relating to:

A) (U) Destruction of aircraft or aircraft facilities (18 U.S.C. § 32);

B) (U) Violence at international airports (applies to offenses occurring outside the United States in certain situations) (18 U.S.C. § 37);

C) (U) Arson within "special maritime and territorial jurisdiction (SMTJ) of the United States" (SMTJ is defined in 18 U.S.C. § 7) (18 U.S.C. § 81);

D) (U) Prohibitions with respect to biological weapons (extraterritorial federal jurisdiction if offense committed by or against a United States national) (18 U.S.C. § 175);

E) (U) Possession of biological agents or toxins by restricted persons (18 U.S.C. § 175b);

F) (U) Variola virus (includes smallpox and other derivatives of the variola major virus) (applies to offenses occurring outside the United States in certain situations) (18 U.S.C. § 175c);

G) (U) Prohibited activities regarding chemical weapons (applies to offenses occurring outside the United States in certain situations) (18 U.S.C. § 229) (E.O. 13128 directs any possible violation of this statute be referred to the FBI);

H) (U) Congressional, Cabinet, and Supreme Court assassination, kidnapping and assault (18 U.S.C. § 351[a]-[d]) (18 U.S.C. § 351[g] directs that the FBI shall investigate violations of this statute);

I) (U) Prohibited transactions involving nuclear materials (applies to offenses occurring outside the United States in certain situations) (18 U.S.C. § 831);

J) (U) Participation in nuclear and weapons of mass destruction threats to the United States (extraterritorial federal jurisdiction) (18 U.S.C. § 832);

K) (U) Importation, exportation, shipping, transport, transfer, receipt, or possession of plastic explosives that do not contain a detection agent (18 U.S.C. § 842[m] and [n]);

L) (U) Arson or bombing of government property risking or causing death (18 U.S.C. § 844[f][2] or [3]) (18 U.S.C. § 846[a] grants FBI and the Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF) concurrent authority to investigate violations of this statute). See Section

2.4.2.1.L above regarding DOJ Memorandum dated 08/03/2010 on ATF/FBI Lead Agency Jurisdiction;

M) (U) Arson or bombing of property used in or affecting interstate or foreign commerce (18 U.S.C. § 844[i]) (18 U.S.C. § 846[a] grants FBI and ATF concurrent authority to investigate violations of this statute);

N) (U) Killing or attempted killing during an attack on a federal facility with a dangerous weapon (18 U.S.C. § 930[c]);

O) (U) Conspiracy within United States jurisdiction to murder, kidnap, or maim persons at any place outside the United States (18 U.S.C. § 956[a][1]);

P) (U) Using a computer for unauthorized access, transmission, or retention of protected information (18 U.S.C. § 1030[a][1]) (18 U.S.C. § 1030[d][2] grants the FBI "primary authority" to investigate Section 1030[a][1] offenses involving espionage, foreign counterintelligence, information protected against unauthorized disclosure for reasons of national defense or foreign relations, or Restricted Data as defined in the Atomic Energy Act, except for offenses affecting United States Secret Service (USSS) duties under 18 U.S.C. § 3056[a]);

Q) (U) Knowingly transmitting a program, information, code, or command and thereby intentionally causing damage, without authorization, to a protected computer (18 U.S.C. § 1030[a][5][A][i]);

R) (U) Killing or attempted killing of officers or employees of the United States, including any member of the uniformed services (18 U.S.C. § 1114);

S) (U) Murder or manslaughter of foreign officials, official guests, or internationally protected persons (applies to offenses occurring outside the United States in certain situations) (18 U.S.C. § 1116) (Attorney General may request military assistance in the course of enforcement of this section);

T) (U) Hostage taking (applies to offenses occurring outside the United States in certain situations) (18 U.S.C. § 1203);

U) (U) Willfully injuring or committing any depredation against government property or contracts (18 U.S.C. § 1361);

V) (U) Destruction of communication lines, stations, or systems (18 U.S.C. § 1362);

W) (U) Destruction or injury to buildings or property within special maritime and territorial jurisdiction of the United States (18 U.S.C. § 1363);

X) (U) Destruction of $100,000 or more of an "energy facility" property as defined in the statute (18 U.S.C. § 1366);

Y) (U) Presidential and Presidential staff assassination, kidnapping, and assault (18 U.S.C. § 1751[a], [b], [c], or [d]) (extraterritorial jurisdiction) (Per 18 U.S.C. § 1751[i], 1751 violations must be investigated by the FBI; FBI may request assistance from any federal [including military], state, or local agency notwithstanding any statute, rule, or regulation to the contrary);

Z) (U) Terrorist attacks and other violence against railroad carriers and against mass transportation systems on land, on water, or through the air (includes a school bus, charter, or sightseeing transportation; or any means of transport on land, water, or through the air) (18 U.S.C. § 1992);

AA) (U) Destruction of national defense materials, premises, or utilities (18 U.S.C. § 2155);

BB) (U) Production of defective national defense materials, premises, or utilities (18 U.S.C. § 2156);

CC) (U) Violence against maritime navigation (18 U.S.C. § 2280);

DD) (U) Violence against maritime fixed platforms (located on the continental shelf of the United States or located internationally in certain situations) (18 U.S.C. § 2281);

EE) (U) Certain homicides and other violence against United States nationals occurring outside of the United States (18 U.S.C. § 2332);

FF) (U) Use of weapons of mass destruction (WMD) (against a national of the United States while outside the United States; against certain persons or property within the United States; or by a national of the United States outside the United States) (18 U.S.C. § 2332a) (WMD defined in 18 U.S.C. § 2332a[c][2]);

GG) (U) Acts of terrorism transcending national boundaries (includes murder, kidnapping, and other prohibited acts occurring inside and outside the United States under specified circumstances – including that the victim is a member of a uniform service; includes offenses committed in the United States territorial sea and airspace above and seabed below; includes offenses committed in special maritime and territorial jurisdiction of the United States as defined in 18 U.S.C. § 7) (18 U.S.C. § 2332b);

HH) (U) Bombings of places of public use, government facilities, public transportation systems and infrastructure facilities (applies to offenses occurring inside or outside the United States in certain situations; does not apply to activities of armed forces during an armed conflict) (18 U.S.C. § 2332f);

II) (U) Missile systems designed to destroy aircraft (applies to offenses occurring outside the United States in certain situations) (18 U.S.C. § 2332g);

JJ) (U) Radiological dispersal devices (applies to offenses occurring outside the United States in certain situations) (18 U.S.C. § 2332h);

KK) (U) Harboring or concealing terrorists (18 U.S.C. § 2339);

LL) (U) Providing material support or resources to terrorists (18 U.S.C. § 2339A);

MM) (U) Providing material support or resources to designated foreign terrorist organizations (extraterritorial federal jurisdiction) (18 U.S.C. § 2339B) ("The Attorney General shall conduct any investigation of a possible violation of this section, or of any license, order, or regulation issued pursuant to this section." 18 U.S.C. § 2339B[e][1]);

NN) (U) Prohibitions against the financing of terrorism (applies to offenses occurring outside the United States in certain situations including on board a vessel flying the flag of the United States or an aircraft registered under the laws of the United States) (18 U.S.C. § 2339C) (Memorandum of Agreement between the Attorney General and the Secretary of Homeland Security, dated May 13, 2005: FBI leads all terrorist financing investigations and operations);

OO) (U) Relating to military-type training from a foreign terrorist organization (extraterritorial jurisdiction) (18 U.S.C. § 2339D);

PP) (U) Torture applies only to torture committed outside the United States in certain situations; torture is defined in 18 U.S.C. § 2340 (18 U.S.C. § 2340A);

QQ) (U) Prohibitions governing atomic weapons (applies to offenses occurring outside the United States in certain situations) (42 U.S.C. § 2122) (FBI shall investigate alleged or suspected violations per 42 U.S.C. § 2271[b]);

RR) (U) Sabotage of nuclear facilities or fuel (42 U.S.C. § 2284) (FBI shall investigate alleged or suspected violations per 42 U.S.C. § 2271[b]);

SS) (U) Aircraft piracy (applies to offenses occurring outside the United States in certain situations) (49 U.S.C. § 46502) (FBI shall investigate per 28 U.S.C. § 538);

TT) (U) Assault on a flight crew with a dangerous weapon (applies to offenses occurring in the "special aircraft jurisdiction of the United States" as defined in 49 U.S.C. § 46501[2]); (second sentence of 49 U.S.C. § 46504) (FBI shall investigate per 28 U.S.C. § 538);

UU) (U) Placement of an explosive or incendiary device on an aircraft (49 U.S.C. § 46505[b][3]) (FBI shall investigate per 28 U.S.C. § 538);

VV) (U) Endangerment of human life on aircraft by means of weapons (49 U.S.C. § 46505[c]) (FBI shall investigate per 28 U.S.C. § 538);

WW) (U) Application of certain criminal laws to acts on aircraft (if homicide or attempted homicide is involved) (applies to offenses occurring in the "special aircraft jurisdiction of the United States" as defined in 18 U.S.C. § 46501[2]); (49 U.S.C. § 46506) (FBI shall investigate per 28 U.S.C. § 538);

XX) (U) Damage or destruction of interstate gas or hazardous liquid pipeline facility (49 U.S.C. § 60123[b]); and

YY) (U) Section 1010A of the Controlled Substances Import and Export Act (relating to narco-terrorism).

2.4.2.2 (U) Additional Offenses Not Defined as "Federal Crimes of Terrorism"

(U) Title 18 U.S.C. § 2332b(f) expressly grants the Attorney General primary investigative authority for additional offenses not defined as "Federal Crimes of Terrorism." These offenses are:

A) (U) Congressional, Cabinet, and Supreme Court assaults (18 U.S.C. § 351[e]) (18 U.S.C. § 351[g]) directs that the FBI investigate violations of this statute);

B) (U) Using mail, telephone, telegraph, or other instrument of interstate or foreign commerce to threaten to kill, injure, or intimidate any individual, or unlawfully to damage or destroy any building, vehicle, or other real or personal property by means of fire or explosive (18 U.S.C. § 844[e]); (18 U.S.C. § 846[a] grants FBI and ATF concurrent authority to investigate violations of this statute);

C) (U) Damages or destroys by means of fire or explosive any building, vehicle, or other personal or real property, possessed, owned, or leased to the United States or any agency thereof, or any institution receiving federal financial assistance (18 U.S.C. § 844[f][1]) (18 U.S.C. § 846[a] grants FBI and ATF concurrent authority to investigate violations of this statute). See Section 2.4.2.1.L above regarding DOJ Memorandum dated 08/03/2010 on ATF/FBI Lead Agency Jurisdiction;

D) (U) Conspiracy within United States jurisdiction to damage or destroy property in a foreign country and belonging to a foreign country, or to any railroad, canal, bridge, airport, airfield, or other public utility, public conveyance, or public structure, or any religious, educational, or cultural property so situated (18 U.S.C. § 956[b]);

E) (U) Destruction of $5,000 or more of an "energy facility" property as defined in 18 U.S.C. § 1366(c) (18 U.S.C. § 1366[b]); and

F) (U) Willful trespass upon, injury to, destruction of, or interference with fortifications, harbor defenses, or defensive sea areas (18 U.S.C. § 2152).

(U) Nothing in this section of the DIOG may be construed to interfere with the USSS under 18 U.S.C. § 3056.

2.4.2.3 (U//FOUO) NSPD-46/HSPD-15, "U.S. POLICY AND STRATEGY IN THE WAR ON TERROR"

(U//FOUO) Annex II (Consolidation and Updating of Outdated Presidential Counterterrorism Documents), dated January 10, 2007, to the classified National Security Presidential Directive (NSPD) 46/Homeland Security Presidential Directive (HSPD) 15, dated March 6, 2006, establishes FBI lead responsibilities, as well as those of other federal entities, in the "War on Terror."[redacted] b7E

(U//FOUO) Areas addressed in Annex II [redacted] Both NSPD-46/HSPD-15 and Annex II thereto are classified.

2.4.3 (U) COUNTERINTELLIGENCE AND ESPIONAGE INVESTIGATIONS

(U//FOUO) A representative list of federal statutes applicable to counterintelligence and espionage investigations appears below. For additional information, refer to the classified Counterintelligence Division (CD) Policy Implementation Guide (PG) and the current list of espionage and counterintelligence authorities.

2.4.3.1 (U) ESPIONAGE INVESTIGATIONS OF PERSONS IN UNITED STATES DIPLOMATIC MISSIONS ABROAD

(U) Section 603 of the Intelligence Authorization Act of 1990 (P.L. 101-193) states that, subject to the authority of the Attorney General, "the FBI shall supervise the conduct of all investigations of violations of the espionage laws of the United States by persons employed by or assigned to United States diplomatic missions abroad. All departments and agencies shall provide appropriate assistance to the FBI in the conduct of such investigations." Consult the Attorney General's extraterritorial guidelines and other applicable policy or agreements.

2.4.3.2 (U) INVESTIGATIONS OF UNAUTHORIZED DISCLOSURE OF CLASSIFIED INFORMATION TO A FOREIGN POWER OR AGENT OF A FOREIGN POWER

(U) The National Security Act of 1947, as amended, establishes procedures for the coordination of counterintelligence activities (50 U.S.C. § 402a). Part of that statute requires that, absent extraordinary circumstances as approved by the President in writing on a case-by-case basis, the head of each executive branch department or agency must ensure that the FBI is "advised immediately of any information, regardless of its origin, which indicates that

classified information is being, or may have been, disclosed in an unauthorized manner to a foreign power or an agent of a foreign power."

2.4.4 (U) CRIMINAL INVESTIGATIONS

(U//FOUO) In addition to the statutes listed above and below, refer to the appropriate program/sub-program Criminal Investigative Division (CID) PG for additional criminal jurisdiction information.

2.4.4.1.1 (U) INVESTIGATIONS OF AIRCRAFT PRIVACY AND RELATED VIOLATIONS

(U) The FBI shall investigate any violation of 49 U.S.C. § 46314 (Entering aircraft or airport areas in violation of security requirements) or chapter 465 (Special aircraft jurisdiction of the United States) of Title 49, United States Code; (28 U.S.C. § 538)

2.4.4.1.2 (U) VIOLENT CRIMES AGAINST FOREIGN TRAVELERS

(U) The Attorney General and Director of the FBI shall assist state and local authorities in investigating and prosecuting a felony crime of violence in violation of the law of any State in which the victim appears to have been selected because he or she is a traveler from a foreign nation; (28 U.S.C. § 540A[b])

2.4.4.1.3 (U) FELONIOUS KILLINGS OF STATE AND LOCAL LAW ENFORCEMENT OFFICERS

(U) The FBI shall investigate any violation of 28 U.S.C. § 540; and

2.4.4.1.4 (U) INVESTIGATIONS OF SERIAL KILLINGS

(U) The FBI shall investigate any violation of 28 U.S.C. § 540B.

2.4.5 (U) AUTHORITY OF AN FBI SPECIAL AGENT

(U) An FBI Special Agent has the authority to:

A) (U) Investigate violations of the laws, including the criminal drug laws, of the United States (21 U.S.C. § 871; 28 U.S.C. §§ 533, 534 and 535; 28 C.F.R. § 0.85);

B) (U) Collect evidence in investigations in which the United States is or may be a party in interest (28 C.F.R. § 0.85 [a]) as redelegated through exercise of the authority contained in 28 C.F.R. § 0.138 to direct personnel in the FBI;

C) (U) Make arrests (18 U.S.C. §§ 3052 and 3062);

D) (U) Serve and execute arrest warrants and seize property under warrant; issue and/or serve administrative subpoenas; serve subpoenas issued by other proper authority; and make civil investigative demands (18 U.S.C. §§ 3052, 3107; 21 U.S.C. § 876; 15 U.S.C. § 1312);

E) (U) Carry firearms (18 U.S.C. § 3052);

F) (U) Administer oaths to witnesses attending to testify or depose in the course of investigations of frauds on or attempts to defraud the United States or irregularities or misconduct of employees or agents of the United States (5 U.S.C. § 303);

G) (U) Seize property subject to seizure under the criminal and civil forfeiture laws of the United States (e.g., 18 U.S.C. §§ 981 and 982); and

H) (U) Perform other duties imposed by law.

(U) *Note*: For policy regarding Agent's authority to intervene in non-federal crimes or make non-federal arrests, see Section 19.3.3.

2.5 (U) STATUS AS INTERNAL GUIDANCE

(U) The AGG-Dom, this DIOG, and the various operational division PGs are set forth solely for the purpose of internal DOJ and FBI guidance. They are not intended to, do not, and may not be relied upon to create any rights, substantive or procedural, enforceable by law by any party in any matter, civil or criminal, nor do they place any limitation on otherwise lawful investigative and litigative prerogatives of the DOJ and the FBI. (AGG-Dom, Part I.D.2.)

2.6 (U) DEPARTURE FROM THE AGG-DOM (AGG-DOM I.D.3)

2.6.1 (U) DEFINITION

(U//FOUO) A "departure" from the AGG-Dom is a deliberate deviation from a known requirement of the AGG-Dom. The word "deliberate" means the employee was aware of the AGG-Dom requirement and affirmatively chose to depart from it for operational reasons before the activity took place. Departures from the AGG-Dom may only be made in accordance with the guidance provided in this section.

2.6.2 (U) DEPARTURE FROM THE AGG-DOM IN ADVANCE

(U//FOUO) A departure from the AGG-Dom must be approved by the Director of the FBI, by the Deputy Director of the FBI, or by an Executive Assistant Director (EAD) designated by the Director. The Director of the FBI has designated the EAD National Security Branch (NSB) and the EAD Criminal Cyber Response and Services Branch (CCRSB) to grant departures from the AGG-Dom. Notice of the departure must be provided by Electronic Communication (EC) to the General Counsel (GC) using file number 333-HQ-C1629406. The Office of the General Counsel (OGC) must provide timely written notice of departures from the AGG-Dom to either the DOJ Criminal Division or National Security Division (NSD), whichever is appropriate, or to both, and the Criminal Division or NSD must notify the Attorney General and the Deputy Attorney General. Notwithstanding this paragraph, all activities in all circumstances must be carried out in a manner consistent with the Constitution and laws of the United States. (AGG-Dom, Part I.D.3.)

2.6.3 (U) EMERGENCY DEPARTURES FROM THE AGG-DOM

(U//FOUO) If a departure from the AGG-Dom is necessary without prior approval because of the immediacy or gravity of a threat to the safety of persons or property or to the national security, an FBI employee may, at his/her discretion, depart from the requirements of the AGG-Dom when the designated approving authority for the investigative activity cannot be contacted through reasonable means. The Director, the Deputy Director, or a designated EAD, and the GC must be notified by EC of the departure as soon thereafter as practicable, but not more than 5 business days after the departure using file number 333-HQ-C1629406. The OGC must provide

timely written notice of departures from the AGG-Dom to either the DOJ Criminal Division or NSD, whichever is appropriate, or to both of them, and the Criminal Division or NSD must notify the Attorney General and the Deputy Attorney General. Notwithstanding this paragraph, all activities in all circumstances must be carried out in a manner consistent with the Constitution and laws of the United States. (AGG-Dom, Part I.D.3.)

2.6.4 (U) Records of Departures from the AGG-Dom

(U//FOUO) The OGC is responsible for maintaining records of all requests and approvals or denials of departures from the AGG-Dom. Records will be maintained in file number 333-HQ-C1629406.

2.7 (U) Departures from the DIOG

2.7.1 (U) Definition

(U//FOUO) A "departure" from the DIOG is a deliberate deviation from a known requirement of the DIOG. The word "deliberate" means the employee was aware of the DIOG requirement and affirmatively chose to depart from it for operational reasons before the activity took place. Departures from the DIOG may only be made in accordance with the guidance provided in this section.

2.7.2 (U) Departure from the DIOG

(U//FOUO) A request for a departure from the DIOG must be submitted with an EC using file number 333-HQ-C1629406 and approved by the appropriate operational program Assistant Director (AD) with notice to the GC. Notwithstanding this paragraph, all activities in all circumstances must be carried out in a manner consistent with the Constitution and laws of the United States.

(U//FOUO) OGC will review all departures from the DIOG. If OGC determines the departure from the DIOG also involves a departure from the AGG-Dom, OGC must provide timely written notice to DOJ in accordance with the provisions of Section I.D.3 of the AGG-Dom.

2.7.3 (U) Emergency Departures from the DIOG

(U//FOUO) FBI employees may conduct or engage in investigative activity that deviates from the requirements of the DIOG, including utilizing investigative methods, without prior approval, when the designated approving authority for the investigative activity (if any) cannot be contacted through reasonable means and in the judgment of the employee one of the following factors is present:

A) (U//FOUO) an immediate or grave threat to the safety of persons or property exists, or

B) (U//FOUO) an immediate or grave threat to the national security exists, or

C) (U//FOUO) a substantial likelihood exists that a delay will result in the loss of a significant investigative opportunity.[1]

(U//FOUO) The appropriate operational program AD and the GC must be notified of the emergency departure by EC using file number 333-HQ-C1629406 as soon as practicable, but no later than 5 business days after engaging in the activity or utilizing the investigative method. This documentation must also be filed in the applicable investigative file in which the activity or method was taken. OGC will review all departures from the DIOG. If OGC determines the departure from the DIOG also involves a departure from the AGG-Dom, OGC must provide timely written notice to DOJ in accordance with the provisions of Section I.D.3 of the AGG-Dom. Notwithstanding this paragraph, all activities in all circumstances must be carried out in a manner consistent with the Constitution and laws of the United States.

2.7.4 (U) RECORDS OF DEPARTURES FROM THE DIOG

(U//FOUO) The OGC is responsible for maintaining records of all requests and approvals or denials of departures from the DIOG. Records will be maintained in file number 333-HQ-C1629406.

2.8 (U) DISCOVERY OF NON-COMPLIANCE WITH DIOG REQUIREMENTS AFTER-THE-FACT

2.8.1 (U) SUBSTANTIAL NON-COMPLIANCE WITH THE DIOG

2.8.1.1 (U) SUBSTANTIAL NON-COMPLIANCE

(U//FOUO) "Substantial non-compliance" means non-compliance that is of significance to the matter and is more than a minor deviation from a DIOG requirement.[2] Non-compliance that relates solely to administrative or peripheral requirements is not substantial. Substantial non-compliance specifically includes the following:

A) (U//FOUO) the unauthorized use of an investigative method;

B) (U//FOUO) the failure to obtain required supervisory approval;[3] *and*

C) (U//FOUO) non-compliance that has a potential adverse effect upon a member of the public's individual rights or liberties.

(U//FOUO) **Example A:** During an Assessment [redacted] b7E to conduct surveillance. Because the approval was not obtained in advance nor was it done pursuant to an emergency

[1] (U//FOUO) This is not a permissible factor for departing from the AGG-Dom. Thus, this factor may only provide a basis for a departure from the DIOG that does not require a departure from the AGG-Dom.
[2] (U//FOUO) Departures from the AGG-Dom and the DIOG do not fall within the definition of "non-compliance" as used in this section. Departures are to be handled as described Sections 2.6 and 2.7 and should not be reported as "non-compliance" matters.
[3] (U//FOUO) If supervisory approval was obtained pursuant to Section 2.7.3 (Emergency Departure from the DIOG), the failure to document this approval within 5 business days is a reportable "substantial non-compliance" matter.

situation as described in 2.7.3, this would be "substantial" non-compliance with DIOG sections 18.5.8.3.3 and 18.5.8.3.4 and must be reported to OIC as set forth in 2.8.2 below.

(U//FOUO) **Example B:** A new SSA arrives in a squad and discovers that his predecessor did not conduct file reviews in several of the squad's Predicated Investigations for several months. This is "substantial non-compliance" and must be reported.

2.8.1.2 (U) OTHER NON-COMPLIANCE

(U//FOUO) Non-compliance with the DIOG that is not "substantial" may be reported, but it is not mandatory to do so. If there is uncertainty regarding whether a particular matter is substantial or not, the matter should be reported. Nevertheless, whenever non-compliance is discovered (whether reported or not), appropriate remedial action must be taken by the relevant employee(s) to correct the non-compliance, including implementing any preventative measures that would help eliminate possible future non-compliance.

(U//FOUO) **Example:** An SSA discovers that she conducted a file review 20 days late. This relates to an administrative requirement and, without more, is not "substantial" noncompliance; this does not have to be reported to OIC. The SSA should, however, take appropriate preventative measures to avoid recurrence.

2.8.2 (U) DOCUMENTATION OF SUBSTANTIAL NON-COMPLIANCE

(U//FOUO) Substantial non-compliance with the DIOG must be reported by EC or subsequent form. The EC must include the following information:

A) (U//FOUO) The relevant DIOG provision(s) involved;

B) (U//FOUO) Description of the facts and circumstances (including dates) of the substantial non-compliance;

C) (U//FOUO) The date the substantial non-compliance was discovered;

D) (U//FOUO) Circumstances leading to the discovery of the substantial non-compliance;

E) (U//FOUO) If the substantial non-compliance was the result of the failure to obtain appropriate supervisory approval (e.g., failure to comply with the requirements of section 2.7.4) in the context of an emergency departure from the DIOG, a statement as to whether that official, or the current official in the appropriate supervisory position, would have approved the action if a timely request had been made based on the facts and circumstances then known;

F) (U//FOUO) Known adverse consequences, if any, attributable to the substantial non-compliance; and

G) (U//FOUO) Corrective or remedial action(s) taken or planned to be taken to mitigate the substantial non-compliance, as well as to help prevent such occurrences in the future.

(U//FOUO) **Example:** An ASAC discovers that a Preliminary Investigation (PI) was extended without obtaining the proper approvals. The failure to obtain appropriate supervisory approval to extend the Preliminary Investigation must be reported, and the report must address all of the seven areas in A-G listed above.

2.8.3 (U) REPORTING AUTHORITIES

(U//FOUO) If the substantial non-compliance occurred in a field office, the EC must be addressed to the ADIC/SAC. If the substantial non-compliance occurred at FBI Headquarters (FBIHQ), the EC must be addressed to the employee's Assistant Director. A copy of the EC must be provided to the Office of Integrity and Compliance (OIC) and to the Office of the General Counsel (OGC) using file number 319O-HQ-A1561245-OIC. A copy of the EC should also be sent to the investigative file in which the incident occurred. In addition, if the ADIC/SAC or AD assesses that the non-compliance appears to reflect intentional or willful misconduct, it must be reported separately by EC to the Internal Investigations Section of the Inspection Division.

2.8.4 (U) ROLE OF OIC AND OGC

(U//FOUO) OGC will review all reports of substantial non-compliance to determine whether any further action is required in the particular matter. OIC will analyze substantial non-compliance reports to determine whether any trends exist in the data and will develop strategies to reduce the occurrences of substantial non-compliance. Based upon OIC's analysis of these reports, if OIC discovers a systemic problem of non-compliance with the AGG-Dom or DIOG involving intelligence activities, either division or FBI wide, OIC must notify OGC/NSLB of this systemic problem.

(U//FOUO) **Example A:** An IA discovers that a mail cover was used in an Assessment. Because mail covers are not permitted to be used in Assessments, this must be reported as a "substantial" non-compliance with the DIOG.

(U//FOUO) **Example B:** A supervisor determines that a Type 1 & 2 Assessment was opened based solely on the exercise of First Amendment rights. While no supervisory approval was required to open the Type 1 & 2 Assessment, this must be reported as "substantial" non-compliance because opening an Assessment based solely on First Amendment activity affects an individual's rights and liberties.

2.8.5 (U) POTENTIAL IOB MATTERS INVOLVING THE REPORTS OF SUBSTANTIAL NON-COMPLIANCE

(U//FOUO) If the substantial non-compliance is also a potential IOB matter, the matter must be reported in accordance with the requirements and procedures for reporting potential IOB matters to OGC/NSLB. See Corporate Policy Directive 0188D: Guidance on Intelligence Oversight Board Matters (See 0188D); the Policy Implementation Guide 0188PG; and see DIOG Section 4. No additional reporting of the incident needs to be made to OIC under this section.

2.8.6 (U) REPORTING NON-COMPLIANCE WITH POLICY IMPLEMENTATION GUIDES

(U//FOUO) Substantial non-compliance with DIOG-related Policy/Program Guides must be reported by EC or subsequent form to the SAC/ADIC, with a copy to the pertinent Headquarters Program Manager, and to the OIC and OGC using file number 319O-HQ-A1561245-OIC.

2.8.7 (U) *REPORTING NON-COMPLIANCE WITH OTHER FBI POLICIES AND PROCEDURES (OUTSIDE THE DIOG)*

(U//FOUO) Nothing in this section is intended to alter, limit, or restrict existing policies that require non-compliance to be reported in areas not covered by the DIOG. Employees remain responsible to report those other matters. Additional information can be found on the Office of Integrity and Compliance's webpage.

2.9 (U) OTHER FBI ACTIVITIES NOT LIMITED BY AGG-DOM

(U) The AGG-Dom apply to FBI domestic investigative activities and do not limit other authorized activities of the FBI. The authority for such other activities may be derived from the authority of the Attorney General as provided in federal statutes, guidelines, or Executive Orders. The scope and approval of these other authorized activities are addressed in the policies that govern the activity and these policies must be relied on when engaging in such activities. Examples of authorized FBI activities not governed by the AGG-Dom include, but are not limited to, the FBI's responsibilities to conduct background checks and inquiries concerning applicants and employees under federal personnel security programs (e.g., background investigations), FBI physical building security issues, Office of Professional Responsibility/personnel issues, certain administrative claims/civil actions, the FBI's maintenance and operation of national criminal records systems and preparation of national crime statistics, and the forensic assistance and administration functions of the FBI Laboratory. (AGG-Dom, Part I.D.4.)

(U) FBI employees may incidentally obtain information relating to matters outside of the FBI's primary investigative responsibility. For example, information relating to violations of state or local law or foreign law may be incidentally obtained in the course of investigating federal crimes or threats to the national security or in collecting foreign intelligence. Neither the AGG-Dom nor the DIOG bar the acquisition of such information in the course of authorized investigative activities, the retention of such information, or its dissemination as appropriate to the responsible authorities in other jurisdictions. (See Section 14; AGG-Dom, Part II and Part VI.B)

2.10 (U) USE OF CLASSIFIED INVESTIGATIVE TECHNOLOGIES

(U) Inappropriate use of classified investigative technologies may risk the compromise of such technologies. Hence, in an investigation relating to activities in violation of federal criminal law that does not concern a threat to the national security or foreign intelligence, the use of such technologies must be in conformity with the Procedures for the Use of Classified Investigative Technologies in Criminal Cases (AGG-Dom, Part V.B.2), Operational Technology Division (OTD) Domestic Technical Assistance (DTA) Policy Implementation Guide (PG), and any other FBI policies concerning such technology use.

2.11 (U) APPLICATION OF AGG-DOM AND DIOG

(U//FOUO) The AGG-Dom and DIOG apply to all FBI domestic investigations and operations conducted by an "FBI employee" or an FBI confidential human source (CHS), when operating

pursuant to the tasking or instructions of an FBI employee. The term "FBI employee" includes, but is not limited to, an operational/administrative professional support person, intelligence analyst, special agent, task force officer (TFO), task force member (TFM), task force participant (TFP), detailee, and FBI contractor. Both an "FBI employee" and a CHS, when operating pursuant to the tasking or instructions of an FBI employee, are bound by the AGG-Dom and DIOG. In the DIOG, "FBI employee" includes all personnel descriptions, if not otherwise prohibited by law or policy. For example, if the DIOG states that the "FBI employee" is responsible for a particular investigative activity, the supervisor has the flexibility to assign that responsibility to any person bound by the AGG-Dom and DIOG (e.g., agent, intelligence analyst, task force officer), if not otherwise prohibited by law or policy.

(U//FOUO) TFOs, TFMs, TFPs, detailees, and FBI contractors are defined as "FBI employees" for purposes of application of the AGG-Dom and DIOG. However, for overt representational purposes, TFOs, TFMs, TFPs, detailees and FBI contractors should identify themselves as employees of their parent agency and, if appropriate and necessary, affiliated with a particular FBI investigative entity, such as the JTTF, etc. A CHS is likewise bound by the AGG-Dom, DIOG, AGG-CHS, and other applicable CHS policies when operating pursuant to the tasking or instructions of an FBI employee; however, the FBI CHS is not an employee of the FBI.

(U//FOUO) TFOs, TFMs, TFPs, detailees, and FBI contractors are defined as "FBI employees" only for purposes of the AGG-Dom and DIOG. This inclusive definition does not define federal employment for purposes of the Federal Tort Claims Act, 28 U.S.C. §§ 1346(b), 2401, and 2671 et seq.; the Federal Employees Compensation Act, 5 U.S.C. § 8101 et seq.; the Intergovernmental Personnel Act, 5 U.S.C. § 3374 et seq, or any other law.

(U//FOUO) FBIHQ division PGs may not contradict, alter or otherwise modify the standards established in the DIOG.

3 (U) CORE VALUES, ROLES, AND RESPONSIBILITIES

3.1 (U) THE FBI'S CORE VALUES

(U) The FBI's core values guide and further our mission and help us achieve our many goals. The values do not exhaust the many goals we wish to achieve, but they capsulate the goals as well as can be done in a few words. The FBI's core values must be fully understood, practiced, shared, vigorously defended, and preserved. The values are:

A) (U) Rigorous obedience to the Constitution of the United States

B) (U) Respect for the dignity of all those we protect

C) (U) Compassion

D) (U) Fairness

E) (U) Uncompromising personal integrity and institutional integrity

F) (U) Accountability by accepting responsibility for our actions and decisions and their consequences

G) (U) Leadership, by example, both personal and professional

(U) By observing these core values, we achieve a high level of excellence in performing the FBI's national security and criminal investigative functions as well as the trust of the American people. Our individual and institutional rigorous obedience to constitutional principles and guarantees is more important than the outcome of any single interview, search for evidence, or investigation. Respect for the dignity of all reminds us to wield law enforcement powers with restraint and to avoid placing our self interest above that of those we serve. Fairness and compassion ensure that we treat everyone with the highest regard for constitutional, civil, and human rights. Personal and institutional integrity reinforce each other and are owed to our Nation in exchange for the sacred trust and great authority conferred upon us.

(U) We who enforce the law must not merely obey it. We have an obligation to set a moral example that those whom we protect can follow. Because the FBI's success in accomplishing its mission is directly related to the support and cooperation of those we protect, these core values are the fiber that holds together the vitality of our institution.

3.1.1 (U) COMPLIANCE

(U) All FBI personnel must fully comply with all laws, rules, and regulations governing FBI investigations, operations, programs and activities, including those set forth in the AGG-Dom. We cannot, do not, and will not countenance disregard for the law for the sake of expediency in anything we do. The FBI expects its personnel to ascertain the laws and regulations that govern the activities in which they engage and to acquire sufficient knowledge of those laws, rules, and regulations to understand their requirements, and to conform their professional and personal conduct accordingly. Under no circumstances will expediency justify disregard for the law. FBI policy must be consistent with Constitutional, legal, and regulatory requirements. Additionally,

the FBI must provide sufficient training to affected personnel and ensure that appropriate oversight monitoring mechanisms are in place.

(U//FOUO) In general, the FBI requires employees to report known or suspected failures to adhere to the law, rules or regulations by themselves or other employees, to any supervisor in the employees' chain of command; any Division Compliance Officer; any Office of the General Counsel (OGC) Attorney; any Inspection Division personnel; any FBI Office of Integrity and Compliance (OIC) staff; or any person designated to receive disclosures pursuant to the FBI Whistleblower Protection Regulation (28 Code of Federal Regulations § 27.1), including the Department of Justice (DOJ) Inspector General. For specific requirements and procedures for reporting "departures" and "non-compliance" with the AGG-Dom on the DIOG, see DIOG Section 2.

3.2 (U) INVESTIGATIVE AUTHORITY, ROLES AND RESPONSIBILITY OF THE DIRECTOR'S OFFICE

3.2.1 (U) DIRECTOR'S AUTHORITY, ROLES AND RESPONSIBILITY

(U//FOUO) The Director's authority is derived from a number of statutory and regulatory sources. For example, Sections 531 through 540a of Title 28, United States Code (U.S.C.), provide for the appointment of the Director and enumerate some of his powers. More importantly, with regard to promulgation of the DIOG, Section 301 of Title 5, U.S.C., authorizes the head of an Executive department to "prescribe regulations for the government of his department, the conduct of its employees, the distribution and performance of its business, and the custody, use, and preservation of its records, papers, and property." The Attorney General, as head of the DOJ, has delegated the authority in Section 301 to the Director in a variety of orders and regulations. Foremost among these delegations are Subpart P and Section 0.137 of Title 28, Code of Federal Regulations (C.F.R.). This DIOG is promulgated under the authority thus delegated.

(U//FOUO) The Director's role and responsibilities under the AGG-Dom and DIOG, include, among others, the approval or denial of departures from the AGG-Dom, Undisclosed Participation (UDP) (see DIOG Section 16) and Sensitive Operations Review Committee (SORC) matters (see DIOG Section 10).

3.2.2 (U) DEPUTY DIRECTOR'S AUTHORITY, ROLES AND RESPONSIBILITY

(U//FOUO) The Deputy Director is the proponent of the DIOG, and in that position has oversight regarding compliance with the DIOG and subordinate implementing procedural directives and divisional specific PGs. The Deputy Director is also responsible for the development and the delivery of necessary training and the execution of the monitoring and auditing processes.

(U//FOUO) The Deputy Director works through the Corporate Policy Office (CPO) to ensure the following:

A) (U//FOUO) The DIOG is updated as necessary to comply with changes in the law, rules, or regulations;

B) (U//FOUO) The DIOG is reviewed every three years after the effective date of the 2011 revision, and revised as appropriate. This mandatory review schedule, however, does not restrict the CPO, which is responsible for all corporate policy matters, from working with FBI Headquarters (FBIHQ) divisions and field offices in the meantime to make policy revisions to the DIOG and the PGs whenever necessary and appropriate during the three year period. The CPO may also make technical or non-substantive language or formatting changes to the DIOG, as necessary, provided those changes clarify the meaning without altering the substance of the DIOG;

C) (U//FOUO) Existing and proposed investigative and administrative policies and PGs comply with the standards established in the AGG-Dom and DIOG. On behalf of the Deputy Director, the CPO has the authority, following coordination with the OIC and OGC, to modify or remove any provision of existing or proposed investigative or administrative policies or PGs determined to violate, contradict, or otherwise modify the intent or purpose of any provision or standard established in the AGG-Dom or DIOG; and

D) (U//FOUO) If the CPO makes any changes to the DIOG or other policy pursuant to DIOG Sections 3.2.2.B and/or 3.2.2.C above, the CPO will immediately advise by e-mail all FBIHQ and field office Division Policy Officers (DPO) of such changes and all DPOs must further advise their respective FBI employees of such changes. The electronic version of the DIOG maintained in the CPO's Policy and Guidance Library is the official current policy of the FBI.

3.3 (U) Special Agent/Intelligence Analyst/Task Force Officer (TFO)/Task Force Member (TFM)/Task Force Participant (TFP)/FBI Contractor/Others - Roles and Responsibilities

3.3.1 (U) Roles and Responsibilities

(U//FOUO) Special Agents, analysts, TFO, TFM, TFP, FBI contractors and others bound by the AGG-Dom and DIOG must:

3.3.1.1 (U) Training

(U//FOUO) Obtain training on the DIOG standards relevant to his/her position and perform activities consistent with those standards;

3.3.1.2 (U) Investigative Activity

(U//FOUO) Ensure all investigative activity complies with the Constitution, Federal law, executive orders, Presidential Directives, AGG-Dom, other Attorney General Guidelines (AGG), Treaties, Memoranda of Agreement/Understanding, the DIOG, and any other applicable legal and policy requirements (if an agent, analyst, TFO, or other individual is unsure of the legality of any action, he/she must consult with his/her supervisor, the Chief Division Counsel (CDC) or OGC);

3.3.1.3 (U) Privacy and Civil Liberties

(U//FOUO) Ensure that civil liberties and privacy are protected throughout the Assessment or investigative process;

3.3.1.4 (U) PROTECT RIGHTS

(U//FOUO) Conduct no investigative activity based solely on the exercise of First Amendment activities (i.e., the free exercise of speech, religion, assembly, press or petition) or on the race, ethnicity, national origin or religion of the subject (See DIOG Section 4);

3.3.1.5 (U) COMPLIANCE

(U//FOUO) Ensure compliance with the DIOG, including standards for opening, conducting, and closing an investigative activity; collection activity; or use of an investigative method, as provided in the DIOG;

3.3.1.6 (U) REPORT NON-COMPLIANCE

(U//FOUO) Comply with the law, rules, or regulations, and report any non-compliance concern to the proper authority. For specific requirements and procedures for reporting departures and non-compliance with the AGG-Dom and the DIOG, see DIOG Sections 2.6 - 2.8;

3.3.1.7 (U) ASSIST VICTIMS

(U//FOUO) Identify victims who have suffered direct physical, emotional, or financial harm as result of the commission of Federal crimes, offer the FBI's assistance to victims of these crimes and provide victims' contact information to the responsible FBI Victim Specialist (VS). The VS is thereafter responsible for keeping victims updated on the status of the investigation to the extent permitted by law, regulation, or policy, unless the victim has opted not to receive assistance. The FBI's responsibility for assisting victims is continuous as long as there is an open investigation (see the Office of Victim Assistance PG);

3.3.1.8 (U) OBTAIN APPROVAL

(U//FOUO) Ensure appropriate supervisory approval is obtained for investigative activity as required in the DIOG. Obtain and document oral approval as specified in Section 3.4.2.2 below. Self-approval of DIOG activities is not permitted. See "No Self-Approval Rule" set forth in Section 3.4.2.3 below;

3.3.1.9 (U) ATTRIBUTE INFORMATION TO ORIGINATOR IN REPORTS

(U//FOUO) Ensure that if the originator of information reported to the FBI characterizes an individual, group, or activity in a certain way, FBI records (i.e., 302s, ECs, LHMs, etc.) reflect that another party, and not the FBI, is the originator of the characterization. Example: An FBI document should state: "The complainant advised that the subject was prejudiced and motivated by ethnic bias" rather than "The subject was prejudiced and motivated by ethnic bias;"

3.3.1.10 (U) SERVE AS INVESTIGATION ("CASE") MANAGER

(U//FOUO) If assigned responsibility for an investigation, manage all aspects of that investigation, until it is assigned to another person. It is the employee's responsibility to ensure compliance with all applicable laws, rules, regulations, and guidelines, both

investigative and administrative, from the opening of the investigation through disposition of the evidence, until the investigation is assigned to another person;

3.3.1.11 (U) CREATE AND MAINTAIN RECORDS/FILES

(U//FOUO) Create and maintain authentic, reliable, and trustworthy records, establish files, set leads, supervise investigations, index documents, and retain and share information, as specified in DIOG Section 14 and Appendix J;

3.3.1.12 (U) INDEX DOCUMENTS

(U//FOUO) If assigned responsibility for an investigation, index information in documents. Current guidance for indexing documents may be found in DIOG Appendix J and on the RMD website: [redacted] b7E

3.3.1.13 (U) SEEK FEDERAL PROSECUTION

(U//FOUO) Prefer Federal prosecution rather than state/local prosecution. An FBI employee may protect the FBI's resources and interests when discussing investigations with the United States Attorney's Office (USAO) by accurately representing the time and effort spent on an investigation. The USAO should be aware of this information prior to deciding whether he/she will decline prosecution in favor of handling by local authorities. Criminal investigations conducted by the FBI are designed to obtain evidence for prosecution in Federal court and not in state or local courts; and

3.3.1.14 (U) RETAIN NOTES MADE DURING AN INVESTIGATION

(U//FOUO) Retain in the investigative file (1A envelope) the following types of material developed when interviewing witnesses:

A) (U) Statements signed by the witness.

B) (U) Written statements, unsigned by the witness, but approved or adopted in any manner by the witness.

C) (U) Original notes of interview with prospective witnesses and/or suspects and subjects. That is, in any interview where preparation of an FD-302 is required (an interview where it is anticipated the results will become the subject of court testimony) the handwritten notes must be retained.

D) (U) Dictating interview notes on audio tape in lieu of handwritten notes may be viewed by a court as "original notes" and, therefore, must be retained. Dictation on audio tape of the results of an interview for transcription to a final FD-302 is not "original note" material and need not be retained.

E) (U) An FBI employee's notes made to record his/her own finding, must always be retained. Such notes include, but are not limited to, accountant's work papers and notes covering matters such as crime scene searches, laboratory examinations, and fingerprint examinations. If there is a question whether notes must be retained, resolve the question in favor of retaining the notes.

3.3.2 (U) DEFINITIONS OF TASK FORCE OFFICER (TFO), TASK FORCE MEMBER (TFM), AND TASK FORCE PARTICIPANT (TFP)

(U//FOUO) It is required in some situations for the sponsoring agency of the TFO, TFM and TFP to enter into an MOU with the FBI that governs the activities of the Task Force. For purposes of the DIOG, TFO, TFM, and TFP are defined as follows:

3.3.2.1 (U) TASK FORCE OFFICER (TFO)

(U//FOUO) An individual is a TFO when all of the following apply:

A) (U//FOUO) The individual is a certified Federal, state, local, or tribal law enforcement officer;

B) (U//FOUO) The individual is authorized to carry a firearm;

C) (U//FOUO) The individual is currently deputized under either Title 21 or Title 18 of the U.S.C.;

D) (U//FOUO) The individual has been issued Federal law enforcement credentials;

E) (U//FOUO) The individual is assigned to the supervision of an FBI led task force;

F) (U//FOUO) The individual has a security clearance recognized by the FBI that is currently active; and

G) (U//FOUO) The individual is authorized to have access to FBI facilities.

(U//FOUO) An FBI TFO is mandated to attend all DIOG related training, and is bound by all rules, regulations, and policies set forth in the DIOG when acting in the capacity as an FBI TFO.

3.3.2.2 (U) TASK FORCE MEMBER (TFM)

(U//FOUO) An individual is a TFM when all of the following apply:

A) (U//FOUO) The individual is an employee of a Federal, state, local, or tribal agency;

B) (U//FOUO) The individual is assigned to the supervision of an FBI led task force;

C) (U//FOUO) The individual has a security clearance recognized by the FBI that is currently active; and

D) (U//FOUO) The individual is authorized to have access to FBI facilities.

(U//FOUO) An FBI TFM is mandated to attend all DIOG related training, and is bound by all rules, regulations, and policies set forth in the DIOG when acting in the capacity as an FBI TFM.

3.3.2.3 (U) TASK FORCE PARTICIPANT (TFP) (I.E., TASK FORCE LIAISON)

(U//FOUO) An individual is a TFP when he/she participates on an FBI-led task force and does not otherwise qualify as a TFO or TFM. A TFP is bound by all rules, regulations, and policies set forth in the DIOG when acting in the capacity as an FBI TFP. DIOG related training for an FBI TFP may be required by the head of the office/division that governs the activities of the Task Force.

3.4 (U) SUPERVISOR ROLES AND RESPONSIBILITIES

3.4.1 (U) SUPERVISOR DEFINED

(U) The term "supervisor" as used in the DIOG includes (whether in a Field Office or FBIHQ) the following positions, or a person acting in such capacity:

A) (U) Supervisory Special Agent (SSA),

B) (U) Supervisory Senior Resident Agent (SSRA),

C) (U) Supervisory Intelligence Analyst (SIA),

D) (U) Legal Attache (Legat),

E) (U) Deputy Legal Attache (DLAT),

F) (U) Unit Chief (UC),

G) (U) Assistant Special Agent in Charge (ASAC),

H) (U) Assistant Section Chief (ASC),

I) (U) Section Chief (SC),

J) (U) Special Agent in Charge (SAC),

K) (U) Deputy Assistant Director (DAD),

L) (U) Assistant Director (AD),

M) (U) Assistant Director in Charge (ADIC),

N) (U) Associate Executive Assistant Director (A/EAD),

O) (U) Executive Assistant Director (EAD),

P) (U) Associate Deputy Director (ADD), and

Q) (U) Deputy Director (DD).

(U) The term "supervisor" is also intended to include any other FBI supervisory or managerial position that is not specifically listed above but is equal in rank and/or responsibility to these listed positions. (Note: TFOs/TFMs cannot be supervisors.)

3.4.2 (U) SUPERVISOR RESPONSIBILITIES

3.4.2.1 (U) APPROVAL/REVIEW OF INVESTIGATIVE OR COLLECTION ACTIVITIES

(U//FOUO) Anyone in a supervisory role who approves/reviews investigative or collection activity must determine whether the standards for opening, approving, conducting, and closing an investigative activity, collection activity or investigative method, as provided in the DIOG, have been satisfied.

3.4.2.2 (U) ORAL AUTHORITY / APPROVAL

(U//FOUO) Unless otherwise specified by the AGG–Dom or FBI policy, any authority/approval required in the DIOG necessary to conduct investigative activities may be granted orally by the appropriate approving official. Should such oral authorization be

granted, appropriate written documentation of the oral authorization must be documented by the FBI employee to the authorizing official as soon as practicable, but not more than five business days after the oral authorization. The effective date of any such oral authorization is the date on which the oral authority was granted, and that date and the name of the approving official must be included in the subsequent written documentation.

(U//FOUO) Supervisors are not permitted to self-approve investigative or intelligence collection activity or methods in assessments or investigations assigned to them as case agents or analysts. An independent evaluation and approval of these activities must be obtained including the opening and closing of any Assessment or Predicated Investigation. See Section 3.4.2.3 below.

3.4.2.3 (U) No Self-Approval Rule

(U//FOUO) When approval/authority is required in the DIOG to open, utilize an investigative method, close, or perform any administrative requirement (i.e. initial paperwork to a file, perform a file review, etc.), an approving official (supervisor) may not "self-approve" his/her own work or activity. An independent evaluation and approval of these activities must be obtained, including the opening and closing of any Assessment or Predicated Investigation.

(U//FOUO) Example: An SSA/SIA properly designates a relief supervisor on the squad to act as the SSA/SIA while the supervisor is on leave. The relief SSA/SIA may not approve anything related to his/her own investigations/work because supervisors are not permitted to self-approve investigative or intelligence collection activity or methods in files assigned to themselves.

3.4.2.4 (U) Ensure Compliance with U.S. Regulations and other Applicable Legal and Policy Requirements

(U//FOUO) Supervisors must monitor and take reasonable steps to ensure that all investigative activity, collection activity and the use of investigative methods comply with the Constitution, Federal law, Executive Orders, Presidential Directives, AGG-Dom, other AGG, Treaties, Memoranda of Agreement/Understanding, the DIOG, and any other applicable legal and policy requirements.

3.4.2.5 (U) Training

(U//FOUO) Supervisors must obtain training on the DIOG standards relevant to his/her position and then conform decisions to those standards. Supervisors must also take reasonable steps to ensure that all subordinates have received the required training on the DIOG standards and requirements relevant to the subordinate's position.

3.4.2.6 (U) Protect Civil Liberties and Privacy

(U//FOUO) All supervisors must take reasonable steps to ensure that civil liberties and privacy are protected throughout the investigative process.

3.4.2.7 (U) REPORT COMPLIANCE CONCERNS

(U//FOUO) If a supervisor encounters a practice that does not comply, or appears not to comply, with the law, rules, or regulations, the supervisor must report that compliance concern to the proper authority and, when necessary, take action to maintain compliance. For specific requirements and procedures for reporting departures and non-compliance with the AGG-Dom and the DIOG, see Sections 2.6 - 2.8.

3.4.2.8 (U) NON-RETALIATION POLICY

(U//FOUO) Supervisors must not retaliate or take adverse action against persons who raise compliance concerns. (See CPD 0032D, 02/11/2008 for non-retaliation policy)

3.4.2.9 (U) CREATE AND MAINTAIN RECORDS/FILES

(U//FOUO) Supervisors must ensure that FBI employees create and maintain authentic, reliable, and trustworthy records, establish files, set leads, supervise investigations, index documents, and retain and share information, as specified in DIOG Section 14.

3.4.3 (U) DELEGATION AND SUCCESSION IN THE FBI

(U//FOUO) The ability to exercise legal authority within the FBI through delegations of legal authority and orderly succession to positions of authority is set forth in the Succession and Delegation Policy.

3.4.3.1 (U) DELEGATION

(U//FOUO) As used in the DIOG, the term "delegation" refers to the conveyance of authority to another official (either by position or to a named individual). FBI legal authority is generally delegable one supervisory level unless expressly permitted, prohibited, or restricted by law, regulation, or policy. For example, an SAC may delegate his/her authority to approve Sensitive Investigative Matters (SIMs) to an ASAC, but the ASAC cannot further delegate this authority to an SSA. Delegations will continue in effect until modified, revoked, superseded, the position no longer exists, or the named individual vacates the position.

(U//FOUO) A supervisor may only delegate authority to another supervisor one level junior to himself or herself, unless specified otherwise (e.g., an ASAC may delegate authority to an SSA). SACs may, however, restrict delegations within their field offices, i.e., an SAC may prohibit ASACs from further delegating authorities that have been assigned to them.

(U//FOUO) SSAs and Supervisory Intelligence Analysts (SIA) cannot "delegate" their authority because they are the first level of supervisory responsibility; however, a relief supervisor may exercise the SSA's authority when serving as the "acting" SSA (e.g., when the SSA is absent or unavailable). In the absence of the immediate approval authority, a supervisor at the same or higher level than that required may approve a particular activity (e.g., an Special Agent requests that his/her ASAC or SAC approve a Preliminary Investigation because the Agent's SSA is on a temporary duty assignment).

3.4.3.2 (U) SUCCESSION: ACTING SUPERVISORY AUTHORITY

(U//FOUO) As used in the DIOG, the term "succession" refers to the process by which an official assumes the authorities and responsibilities of an existing position, typically when the incumbent is absent, unavailable, unable to carry out official responsibilities, or has vacated the position. A person who temporarily succeeds to a position is referred to as "acting" in that position.

(U//FOUO) The FBI follows the general rule, recognized in law, that employees properly designated as "acting" in a position exercise the full legal authorities of that position, unless specifically precluded by higher authority or by an applicable law, regulation, or policy. Accordingly, unless expressly precluded, any authority vested in an FBI supervisor pursuant to the DIOG may be exercised by someone who occupies that position in an acting status. An employee may be designated to an acting position either through a succession plan or ad hoc designation. See the FBI Succession and Delegation Policy for additional details.

3.4.3.3 (U) DOCUMENTATION

(U//FOUO) Delegations of authority as well as succession plans and ad hoc designations must be documented in writing and maintained in an appropriate administrative file whenever practicable, unless specifically required by the DIOG. An administrative file has been created to maintain documentation of delegations of authority and ad hoc designations (319W-HQ-A1487698-xx with the last two alpha characters designating particular field office, FBIHQ Division or Legat). An administrative file has also been created to maintain documentation of succession plans (319X-HQ-A1538387-XX with the last two alpha characters designating the particular field office, FBIHQ Division or Legat). Documentation of acting authority may take place subsequent to the actual ad hoc designation. For example, an SSA orally advises his principal relief supervisor that he/she has an emergency and will not be able to come into the office. The ad hoc designation of the relief supervisor as acting SSA can be documented upon the SSA's return to the office. Failure to document an ad hoc designation does not invalidate the designation but may result in difficulty proving the appropriate exercise of authority if required to do so. (See Section 3.4.2.2 above concerning oral authorizations and related documentation requirements).

3.4.4 (U) FILE REVIEWS AND JUSTIFICATION REVIEWS

3.4.4.1 (U) OVERVIEW

(U//FOUO) The file review is designed to ensure investigative and intelligence activities are progressing adequately and conducted in compliance with applicable statutes, regulations, and FBI/DOJ policies and procedures. As a management tool, the file review process has proven effective for operational program oversight, tracking investigative and intelligence collection progress, ensuring investigative focus, and reduction of risk.

(U//FOUO) Supervisory review of investigative files is especially important with regard to tracking the progress and development of new employees. It provides an opportunity for supervisors to guide employees on how properly to manage and document investigation files, and to use and document investigative methods, while emphasizing the importance of

compliance and recognition of risk. In addition, the file review process is an opportunity to begin to evaluate an employee's level of performance and to identify his/her strengths and weaknesses.

(U//FOUO) File reviews help supervisors to ensure their office is effectively supervising activities in its own territory and monitoring investigative activity carried out on their behalf in other field offices. For example, a supervisor may use a file review as a reasonable step to ensure the employee assigned an investigation has addressed all logical investigation in a timely manner, or to ensure the employee has successfully set necessary leads for other offices or other employees within his/her own office.

3.4.4.2 (U) Types of Files/Investigations Requiring File Reviews and Justification Reviews

(U//FOUO) File reviews must be conducted for all Predicated Investigations, including investigations placed in "pending inactive" status, unaddressed work files, and Types 3 through 6 Assessments. Type 1 & 2 Assessments must have a 30 day justification reviews, as specified below.

3.4.4.3 (U) Frequency of File Reviews

(U//FOUO) Supervisors must adhere to the following timeframes for file reviews:

A) **(U//FOUO) 90 Days** – The supervisor must review the files for all investigations (including pending Predicated Investigations, pending inactive investigations, unaddressed work files, and Type 3 - 6 Assessments) assigned to each agent, Resident Agent, TFO, and IA every 90 calendar days.

1) **(U//FOUO) 30 Additional Days:** All documentation of the required reviews must be completed within 30 calendar days of the file review date.

B) **(U//FOUO) 60 Days** - The supervisor must review the files for all investigations (including pending Predicated Investigations, pending inactive investigations, unaddressed work files, and Type 3 - 6 Assessments) assigned to each probationary employee (agent and IA) every 60 calendar days.

1) **(U//FOUO) 30 Additional Days:** All documentation of the required reviews must be completed within 30 calendar days of the file review date.

3.4.4.4 (U) Frequency of Justification Reviews

(U//FOUO) In addition to file reviews, every 30 days supervisors must complete "justification reviews" for Type 1 & 2 Assessments, as specified below.

3.4.4.5 (U) Delegation of File Reviews

(U//FOUO) Thorough, complete and well conducted file reviews are an important part of the compliance regime, provide valuable and needed information for purposes of evaluating the performance of employees, and are critical to the effective management of a squad. For those reasons, file reviews are an important duty and responsibility for Supervisors, and Supervisors are discouraged from routinely delegating these reviews. Because, however, conducting a file review is an important developmental opportunity for primary relief supervisors, file reviews

may be conducted by a duly designated acting supervisor or duly designated primary relief supervisor. Acting supervisors may conduct file reviews just as they would conduct any other supervisory duty while functioning in an acting capacity. Primary relief supervisors may conduct file reviews; however, when they do so, the next required file review must be conducted by a supervisor or duly designated acting supervisor. In other words, every other file review of any given investigative file must be conducted by a supervisor or duly designated acting supervisor. Acting supervisors may not review their own files under any circumstances. Acting supervisors must either reassign their investigations or have their investigations reviewed by another supervisor or an ASAC.

3.4.4.6 (U) File Review Requirements for Predicated Investigations & Assessments

(U//FOUO) A file review or justification review must be: conducted in person or by telephone when necessary (e.g., FBI employee is TDY or in a remote Resident Agency (RA)); conducted in private; and documented as specified below.

(U//FOUO) The file review process requires the supervisor to review the investigative files assigned to the employee, discuss past progress and future objectives, and document that information on the Investigative Case Management (ICM) Case Review Sheet generated by ACS (commonly referred to as the "file review sheet"). Discussion and documentation must also include the progress of the investigation/Assessment since the previous file review and the projected work for the time period until the next file review.

(U//FOUO) When reviewing the employee's assigned investigative files, the supervisor should consider the following:

A) (U//FOUO) Whether subject(s) have been indexed in compliance with indexing guidelines;

B) (U//FOUO) Whether statistical accomplishments, i.e., FD-515 and FD-542, have been entered within established timeframes;

C) (U//FOUO) Whether evidence has been stored and disposed of properly and whether documentation has been completed according to evidence control policies;

D) (U//FOUO) Whether leads have been covered within established deadlines;

E) (U//FOUO) Whether any National Security Letters have been issued in accordance with policy, including whether responsive materials have been appropriately examined (e.g., examined for overproduction);

F) (U//FOUO)Whether any Federal Grand Jury Subpoenas have been issued in accordance with policy, including whether responsive materials have been appropriately examined (e.g., examined for overproduction);

G) (U//FOUO) Whether any Administrative Subpoenas have been issued in accordance with policy, including whether responsive materials have been appropriately examined (e.g., examined for overproduction);

H) (U//FOUO) Whether any Federal Grand Jury Materials covered by Rule 6e are properly marked and handled, including being appropriately restricted in ACS;

I) (U//FOUO) Whether the Watchlist status of any subject(s) has been appropriately documented;

J) (U//FOUO) Whether the status of the Preliminary Investigation is current (e.g., has not expired or will not expire before the next file review);

K) (U//FOUO) Whether any Potential Intelligence Oversight Board (IOB) violations have been reported in accordance with policy; and

L) (U//FOUO) Whether relevant asset forfeiture statutes have been applied and their use documented.

(U//FOUO) Supervisors must evaluate the proper use of investigative methods and ensure they are appropriately documented in the file. Leads and administrative actions must be documented in ECs. When evidence has been recovered, the supervisor must review all FD-192s to ensure the evidence was handled appropriately. The supervisor should use the file review process as an opportunity to determine whether the employee has adequately used liaison and external contacts to further the investigation/Assessment. In addition, the supervisor must assess whether the employee needs additional assistance, training, guidance, or other resources to successfully advance the investigation/Assessment.

(U//FOUO) The intelligence aspect of every investigation must be scrutinized during the file review process. The supervisor must determine whether the employee understands his/her responsibilities relative to intelligence collection and reporting and has ensured that investigative and intelligence aspects of each investigation complement each other. This includes examining whether the employee has adequately collaborated with the field office's intelligence component and exploited his/her investigations to obtain information relevant to standing intelligence collection requirements. The supervisor must review the files for potential intelligence collection and sharing opportunities, both cross-programmatic and interagency. The file review must document whether applicable intelligence products such as intelligence reports, bulletins and assessments, etc., have been or should be drafted based on investigative and intelligence information collected during the investigation.

(U//FOUO) The supervisor must also evaluate whether the employee has been in communication with FBIHQ division entities, if appropriate, with respect to his/her investigative/intelligence activities. The supervisor must also evaluate whether the employee has coordinated with FBIHQ to obtain any special authorities/concurrences needed from DOJ/FBI components and other governmental agencies (e.g., CIA, DOS, and DOD).

(U//FOUO) The supervisor must consider and take into account the employee's collateral duties, such as SWAT, ERT, HAZMAT, Hostage Negotiator, training, TDY assignments and other activities constituting official business that could limit his/her ability to address his/her assigned caseload. The supervisor must take into account planned annual and sick leave, holidays and similar time constraints when estimating the employee's overall work responsibilities for the next 90 day period.

(U//FOUO) The supervisor must evaluate whether the employee is acting within all applicable statutes, regulations, and FBI/DOJ policies and procedures. Supervisors must keep in mind that how the employee accomplishes his or her tasks is just as important as whether he or she accomplishes them. Any compliance concerns must be immediately referred to the field office's compliance officer for discussion regarding what additional actions should be taken. For specific requirements and procedures for reporting departures and non-compliance with the AGG-Dom and the DIOG, see Sections 2.6 - 2.8.

(U//FOUO) At the conclusion of the file review, the supervisor must ensure that the employee understands the objectives to be accomplished over the next 90 calendar days and must document specifically those expectations on the file review sheets. At this time the supervisor must also prepare an FD-865 (Performance Summary Assessment) for Special Agents per Corporate Policy Notice (CPN) 0043N. For all other employees, the supervisor has the option to prepare an FD-865.

(U//FOUO) The supervisor must be diligent about documenting all aspects of the file review on the file review sheet and setting appropriate ticklers.

3.4.4.7 (U) Type 1 & 2 Assessments - Justification Reviews

(U//FOUO) Supervisors must conduct 30-day justification reviews for Type 1 & 2 Assessments. Following the end of the 30-day period, the agent, TFO, or IA and the supervisor have up to 10 calendar days to complete all aspects of the justification review and to document the review. These justification reviews must address the following Assessment Review Standards (ARS):

A) (U//FOUO) has progress been made toward achieving the authorized purpose and clearly defined objective(s);

B) (U//FOUO) were the activities that occurred in the prior 30 calendar days appropriate and in compliance with applicable DIOG requirements;

C) (U//FOUO) is it reasonably likely that information will be obtained that is relevant to the authorized purpose and clearly defined objective(s), thereby warranting an extension for another 30 calendar days;

D) (U//FOUO) has adequate predication been developed to open a Predicated Investigation; and

E) (U//FOUO) should the Assessment be terminated.

(U//FOUO) The justification review, including the ARS requirements, must be documented in the FD-71 or the FD-71a (Guardian).

3.4.4.8 (U) Type 3, 4, and 6 Assessments - Assessment Review Standards (ARS)

(U//FOUO) In addition to the file review procedures documented on the File Review Sheet set forth above, supervisors are required to evaluate Type 3, 4 and 6 Assessments using the below- listed ARS during the file review every 90 calendar days (60 calendar days for probationary employees):

A) (U//FOUO) has progress been made toward achieving the authorized purpose and clearly defined objective(s);

B) (U//FOUO) were the activities that occurred in the prior 60 or 90 calendar days appropriate and in compliance with applicable DIOG requirements;

C) (U//FOUO) is it reasonably likely that information may be obtained that is relevant to the authorized purpose and clearly defined objective(s), thereby warranting an extension for another 60/90 calendar days;

D) (U//FOUO) has adequate predication been developed to open a Predicated Investigation on specific individuals identified during the Assessment; and

E) (U//FOUO) should the Assessment be terminated.

(U//FOUO) The ARS must be documented in an EC and uploaded to the Assessment file.

(U//FOUO) The EC utilized to document the review of Type 3, 4 and 6 Assessments must be made part of the Assessment file. Therefore, the EC must not be used to memorialize other information, such as performance measures, investigative steps, possible outcomes, or compliance matters that are historically documented on the File Review Sheet.

3.4.4.9 (U) Type 5 Assessments - Assessment Review Standards (ARS)

(U//FOUO) In addition to the applicable file review procedures discussed above, supervisors are required to evaluate Type 5 Assessments using the below-listed ARS during the file review every 90 calendar days (60 days for probationary employees):

A) (U//FOUO) whether authorized investigative methods have been used properly in all phases of the Assessment;

B) (U//FOUO) whether, in the identification phase, the Assessment has successfully narrowed the field to a group of individuals who are likely to have appropriate placement and access;

C) (U//FOUO) whether reimbursable expenses incurred by an SA, if any, were reasonable, properly authorized, and properly documented;

D) (U//FOUO) whether the Potential CHS was "tasked" to provide information or paid for his/her services or expenses (activities which are not permitted prior to opening the person as a CHS);

E) (U//FOUO) whether there is a reasonable likelihood that the Potential CHS can and should be recruited or, if the Assessment is in the Identification Phase, the plan has a reasonable likelihood of generating a group of Potential CHSs; and

F) (U//FOUO) whether the Type 5 Assessment should continue for an additional 90 days (60 days for probationary employees). If continuation is justified, the SIA/SSA must document the rationale for keeping the Type 5 Assessment open.

(U//FOUO) The review must be documented in an EC or successor form [redacted] and uploaded to the Assessment file. Because Type 5 Assessments are confidential, a Case Review Sheet is not available in ACS. b7E

(U//FOUO) The EC (or successor form [redacted] utilized to document the evaluation of the ARSs for Type 5 Assessments must be made part of the Assessment file. Therefore, the EC (or successor form [redacted] must not be used to memorialize other information, such as performance measures, investigative steps, possible outcomes, or compliance matters. b7E

3.4.4.10 (U) Documentation of File Reviews

(U//FOUO) Investigative Case Management (ICM) Case Review Sheets (also known as File Review Sheets) are currently generated by ACS. These must be completed by the supervisor as part of the file review process and maintained as a part of the employee's performance folder to be used as a tool in determining an employee's performance rating. Documents maintained for evaluations, including copies of File Review Sheets, must be destroyed within 30 calendar days after the expiration of the previous PAR year. The original File Review Sheets are to be maintained for inspection and other purposes not related to the performance appraisal process (FBI Corporate Policy Notice 0043N).

(U//FOUO) Performance Summary Assessments (PSA) are required to be completed by the supervisor as part of the file review process (see FBI Corporate Policy Notice 0043N). The FD-865 must be used to memorialize the PSA. The form must be signed and dated by the supervisor. The original FD-865 must be submitted to the field office's executive management, which is responsible for ensuring that PSAs are conducted. One completed copy of the FD-865 must be placed in the employee's performance folder maintained by the rating official for inspection, mid-year progress reviews, development worksheets, and annual performance appraisal purposes (this provision does not apply to TFOs). A second completed copy must be given to the employee. FD-865s maintained for performance evaluation must be destroyed within 30 calendar days after the expiration of the previous Performance Annual Review (PAR) year.

3.4.4.11 (U) Records Retention

(U//FOUO) Supervisors must conduct, document and retain file reviews as specified above. Supervisors must maintain appropriate documentation and review it periodically with particular attention to documenting an employee's ability to successfully complete his or her investigative assignments and to documenting a probationary employee's success or failure during the probationary period.

3.5 (U) Chief Division Counsel (CDC) Roles and Responsibilities

(U//FOUO) The CDC must review all Assessments and Predicated Investigations involving sensitive investigative matters as discussed in DIOG Section 10 as well as review the use of certain investigative methods as discussed in Section 18. The primary purpose of the CDC's review is to ensure the legality of the actions proposed. Review, in this context, includes a determination that the investigative activity is: (i) not legally objectionable (e.g., that it is not based solely on the exercise of First Amendment rights (i.e., the free exercise of speech, religion, assembly, press or petition) or on the race, ethnicity, national origin or religion of the subject); and (ii) founded upon an authorized purpose and/or adequate factual predication and meets the standard specified in the DIOG. The CDC should also include in his or her review and recommendation, if appropriate, a determination of the wisdom of the proposed action (e.g., the CDC may have no legal objection but may recommend denial because the value of the proposal is outweighed by the intrusion into legitimate privacy interests). The CDC's determination that an investigative activity is: (i) not legally objectionable; and (ii) warranted from a mission standpoint is based on facts known at the time of the review and recommendation. Often, these facts are not verified or otherwise corroborated until the investigative activity commences. As a result, the CDC may require additional CDC reviews or provide guidance to supervisory personnel with regard to monitoring the results of the investigative activity to ensure that the authorized purpose and/or factual predication remains intact after the facts are developed. The regularity of such review is within the CDC's discretion. Activities found to be legally objectionable by the CDC may not be approved unless and until the CDC's determination is countermanded by the FBI General Counsel or a delegated designee.

(U//FOUO) For investigative activities involving a sensitive investigative matter, the CDC must also independently consider the factors articulated in Section 10 and provide the approving

authority with a recommendation as to whether, in the CDC's judgment, the investigative activity should be approved.

(U//FOUO) Throughout the DIOG, any requirement imposed on the CDC may be performed by an Associate Division Counsel (ADC) or a designated Acting CDC.

3.6 (U) OFFICE OF THE GENERAL COUNSEL (OGC) ROLES AND RESPONSIBILITIES

(U//FOUO) The mission of the FBI's Office of the General Counsel (OGC) is to provide comprehensive legal advice to the Director, other FBI officials and divisions, and field offices on a wide array of national security, investigative, and administrative operations. In addition to providing legal advice as requested, OGC reviews the legal sufficiency of sensitive Title III affidavits and a wide variety of operational documents relating to foreign counterintelligence/ international terrorism investigations, including requests for surveillance and physical searches pursuant to the Foreign Intelligence Surveillance Act (FISA) and undercover proposals, and manages the physical flow of FISA requests, applications, orders, and returns. OGC maintains liaison with the intelligence community on legal issues and reviews for legal sufficiency proposals to share information or form partnerships with other federal, state, local, and international agencies. OGC also supports federal criminal prosecutions by assisting in criminal discovery and by conducting reviews of personnel files, coordinates the defense of the FBI and its employees in civil actions which arise out of the FBI's investigative mission and personnel matters, and responds to Congressional requests for FBI documents. OGC addresses legal issues associated with the impact of communication and information technology on the ability of the FBI and other law-enforcement and intelligence agencies to execute their public safety and national security missions, including their ability to conduct authorized electronic surveillance.

(U//FOUO) In coordination with the DOJ NSD, the OGC is responsible for conducting regular reviews of all aspects of FBI national security and foreign intelligence activities. The primary purpose of the OGC's review is to ensure the legality of the actions proposed. These reviews, conducted at FBI field offices and FBIHQ' units, broadly examine such activities for compliance with the AGG-Dom and other applicable requirements. Review, in this context, includes a determination that the investigative activity is: (i) not legally objectionable (e.g., that it is not based solely on the exercise of First Amendment rights or on the race, ethnicity, national origin or religion of the subject); and (ii) founded upon an authorized purpose and/or adequate factual predication and meets the standard specified in the DIOG. The OGC should also include in its review and recommendation, if appropriate, a determination of the wisdom of the proposed action (e.g., the OGC may have no legal objection but may recommend denial because the value of the proposal is outweighed by the intrusion into legitimate privacy interests). The OGC's determination that an investigative activity is: (i) not legally objectionable; and (ii) warranted from a mission standpoint is based on facts known at the time of the review and recommendation. Often these facts are not verified or otherwise corroborated until the investigative activity commences. As a result, the OGC may require additional OGC reviews or provide guidance to supervisory personnel with regard to monitoring the results of the investigative activity to ensure that the authorized purpose and/or factual predication remains intact after the facts are developed. The regularity of such review is within the discretion of OGC.

(U//FOUO) For those investigative activities involving a sensitive investigative matter requiring OGC review, the OGC must independently consider the factors articulated in Section 10 and provide the approving authority with a recommendation as to whether, in the OGC's judgment, the investigative activity should be approved.

(U//FOUO) Throughout the DIOG, any requirement imposed on the General Counsel may be delegated and performed by a designated OGC attorney. All delegations must be made as set forth in Section 3.4.3 above.

3.7 (U) Corporate Policy Office (CPO) Roles and Responsibilities

(U//FOUO) Subject to the guidance of the Deputy Director, the CPO has oversight of the implementation of the DIOG. Working with the Deputy Director's office, the CPO may make revisions to the DIOG as necessary, following appropriate coordination with the OIC, OGC and other FBIHQ or field office entities. In the process of implementing and analyzing the DIOG, the CPO should report any apparent compliance risk areas directly to the OIC. Additionally, the CPO will work directly with the OIC to ensure that the policies, training and monitoring are adequate to meet compliance monitoring procedures.

(U//FOUO) The CPO is responsible for ensuring the following:

A) (U//FOUO) The DIOG is updated as necessary to comply with changes in the law, rules, or regulations;

B) (U//FOUO) The DIOG is reviewed every three years from the effective date of the 2011 revision, and revised as appropriate. This mandatory review schedule, however, does not restrict the CPO, which is responsible for all corporate policy matters, from working with FBIHQ divisions and field offices to make policy revisions to the DIOG and the PGs whenever necessary and appropriate during the three year period. The CPO may also make technical or non-substantive language or formatting changes to the DIOG, as necessary, provided those changes clarify the meaning without altering the substance;

C) (U//FOUO) Existing and proposed investigative and administrative policies and PGs comply with the standards established in the AGG-Dom and DIOG. On behalf of the Deputy Director, the CPO has the authority, following coordination with the OIC and OGC, to modify or remove any provision of existing or proposed investigative or administrative policies or PGs determined to violate, contradict, or otherwise modify the intent or purpose of any provision or standard established in the AGG-Dom or the DIOG; and

D) (U//FOUO) If the CPO makes any changes to the DIOG or other policy pursuant to 3.7.B and/or C above, the CPO will immediately advise by e-mail all FBIHQ and field office Division Policy Officers (DPO) of such changes and all DPO must further advise their respective FBI employees of such changes. The electronic version of the DIOG maintained in the CPO's Policy and Guidance Library is the official current policy of the FBI.

3.8 (U) Office of Integrity and Compliance (OIC) Roles and Responsibilities

(U//FOUO) OIC is responsible for reviewing the DIOG and working with each FBIHQ division and the CPO to identify compliance risk areas and to ensure the adequacy of policy statements, training and monitoring. When compliance risk areas are identified, OIC must work with the

divisions, field offices, and/or programs affected by the risk and develop programs to review the adequacy of policy statements, training, and monitoring in order to mitigate those concerns appropriately.

3.9 (U) OPERATIONAL PROGRAM MANAGER ROLES AND RESPONSIBILITIES

(U//FOUO) In addition to managing national level programs, coordinating investigations, training, and providing guidance and oversight to the field, the FBIHQ Operational Program Managers are responsible for identifying, prioritizing, and analyzing potential compliance risks within their programs regarding implementation of the DIOG and developing mitigation plans where warranted.

(U//FOUO) Operational Program Managers must proactively identify and take appropriate action to resolve potential compliance concerns. In identifying possible compliance concerns, Program Managers should consider the following indicators of possible compliance issues:

A) (U//FOUO) Similar activities being handled differently from squad-to-squad / unit-to-unit / field office-to-field office;

B) (U//FOUO) Unusually high level of contact with FBIHQ' division for basic information on how to conduct an activity;

C) (U//FOUO) Apparent confusion over how to conduct a certain activity;

D) (U//FOUO) Policy conflict;

E) (U//FOUO) Non-existent/inaccurate/wrongly targeted training;

F) (U//FOUO) Monitoring mechanisms that do not exist or do not test the right information (e.g. file reviews/program management); and

G) (U//FOUO) Inadequate processes in place to audit for compliance.

(U//FOUO) Operational Program Managers may not retaliate or take adverse action against persons who raise compliance concerns.

3.10 (U) DIVISION COMPLIANCE OFFICER ROLES AND RESPONSIBILITIES

(U//FOUO) Each FBIHQ division and field office must have a Division Compliance Officer (DCO). The DCO will proactively identify potential risk of non-compliance in the implementation of the DIOG and report them to the proper authority and the OIC. The DCO must always be aware that the focus of a compliance program is the identification and resolution of a compliance problem using non-punitive and non-retaliatory means.

3.11 (U) POSITION EQUIVALENTS - FBI HEADQUARTERS (FBIHQ) APPROVAL LEVELS

(U//FOUO) The official position equivalents between the field offices and FBIHQ are outlined below. In general, an equivalent position at either the field or FBIHQ may exercise DIOG authority, unless the DIOG specifically limits a given authority. The equivalent positions are:

A) (U//FOUO) Field Office Analyst or Special Agent = FBIHQ Analyst or Special Agent;

B) (U//FOUO) Field Office SIA = FBIHQ SIA;

C) (U//FOUO) CDC = FBIHQ OGC General Attorney;

D) (U//FOUO) Field Office SSA = FBIHQ SSA;

E) (U//FOUO) Field Office ASAC = FBIHQ UC;

F) (U//FOUO) SAC = FBIHQ SC; and

G) (U//FOUO) ADIC = FBIHQ AD.

4 (U) PRIVACY AND CIVIL LIBERTIES, AND LEAST INTRUSIVE METHODS

4.1 (U) CIVIL LIBERTIES AND PRIVACY

4.1.1 (U) OVERVIEW

(U) The FBI is responsible for protecting the security of our nation and its people from crime and terrorism while maintaining rigorous obedience to the Constitution. *The Attorney General's Guidelines for Domestic FBI Activities* (AGG-Dom) establish a set of basic principles that serve as the foundation for all FBI mission-related activities. When these principles are applied, they demonstrate respect for civil liberties and privacy as well as adherence to the Constitution and laws of the United States. These principles are as follows:

A) **(U) Protecting the public includes protecting their rights and liberties.** FBI investigative activity is premised upon the fundamental duty of government to protect the public, which must be performed with care to protect individual rights and to ensure that investigations are confined to matters of legitimate government interest.

B) **(U) Only investigate for a proper purpose.** All FBI investigative activity must have an authorized law enforcement, national security, or foreign intelligence purpose.

C) **(U) Race, ethnicity, religion, or national origin alone can never constitute the sole basis for initiating investigative activity.** Although these characteristics may be taken into account under certain circumstances, there must be an independent authorized law enforcement or national security purpose for initiating investigative activity.

D) **(U) Only perform authorized activities in pursuit of investigative objectives.** Authorized activities conducted as part of a lawful assessment or investigation include the ability to: collect criminal and national security information, as well as foreign intelligence; provide investigative assistance to federal, state, local, tribal, and foreign agencies; conduct intelligence analysis and planning; and retain and share information.

E) **(U) Employ the least intrusive means that do not otherwise compromise FBI operations.** Assuming a lawful intelligence or evidence collection objective, i.e., an authorized purpose, strongly consider the method (technique) employed to achieve that objective that is the least intrusive available (particularly it there is the potential to interfere with protected speech and association, damage someone's reputation, intrude on privacy, or interfere with the sovereignty of foreign governments) while still being operationally sound and effective.

F) **(U) Apply best judgment to the circumstances at hand to select the most appropriate investigative means to achieve the investigative goal.** The choice of which investigative method to employ is a matter of judgment, but the FBI must not hesitate to use any lawful method consistent with the AGG-Dom when the degree of intrusiveness is warranted in light of the seriousness of the matter concerned.

4.1.2 (U) PURPOSE OF INVESTIGATIVE ACTIVITY

(U) One of the most important safeguards in the AGG-Dom—one that is intended to ensure that FBI employees respect the constitutional rights of Americans—is the threshold requirement that

all investigative activities be conducted for an authorized purpose. Under the AGG-Dom that authorized purpose must be an authorized national security, criminal, or foreign intelligence collection purpose.

(U) Simply stating such a purpose, however, is not sufficient to ensure compliance with this requirement. The authorized purpose must be well-founded and well-documented. In addition, the information sought and the investigative method used to obtain it must be focused in scope, time, and manner to achieve the underlying purpose. Furthermore, the Constitution sets limits on what that purpose may be. It may not be solely to monitor the exercise of constitutional rights, such as the free exercise of speech, religion, assembly, press and petition, and, equally important, the authorized purpose may not be based solely on the race, ethnicity, national origin or religious beliefs of an individual, group, or organization or a combination of only those factors.

(U) It is important to understand how the "authorized purpose" requirement and these constitutional limitations relate to one another. For example, individuals or groups who communicate with each other or with members of the public in any form in pursuit of social or political causes—such as opposing war or foreign policy, protesting government actions, or promoting certain religious beliefs—have a First Amendment right to do so. No investigative activity may be conducted for the sole purpose of monitoring the exercise of these rights. If a well-founded basis to conduct investigative activity exists, however, and that basis is not solely activity that is protected by the First Amendment or on the race, ethnicity, national origin or religion of the participants—FBI employees may assess or investigate these activities, subject to other limitations in the AGG-Dom and the DIOG. In such a situation, the investigative activity would not be based solely on constitutionally-protected conduct or on race, ethnicity, national origin or religion. Finally, although investigative activity would be authorized in this situation, it is important that it be conducted in a manner that does not materially interfere with the ability of the individuals or groups to engage in the exercise of constitutionally-protected rights.

4.1.3 (U) OVERSIGHT AND SELF-REGULATION

(U) Every FBI employee has the responsibility to ensure that the activities of the FBI are lawful, appropriate and ethical as well as effective in protecting the civil liberties and privacy of individuals in the United States. Strong oversight mechanisms are in place to assist the FBI in carrying out this responsibility. Department of Justice (DOJ) oversight is provided through provisions of the AGG-Dom, other Attorney General Guidelines, and oversight by other DOJ components. DOJ and the FBI's Inspection Division, and the FBI's Office of Integrity and Compliance (OIC) and Office of the General Counsel (OGC), also provide substantial monitoring and guidance. In the criminal investigation arena, prosecutors and district courts exercise oversight of FBI activities. In the national security and foreign intelligence arenas, the DOJ National Security Division (NSD) exercises that oversight. The DOJ NSD's Oversight Section and the FBI's OGC are responsible for conducting regular reviews of all aspects of FBI national security and foreign intelligence activities. These reviews, conducted at FBI field offices and FBI Headquarters (FBIHQ) divisions, broadly examine such activities for compliance with the AGG-Dom and other applicable requirements. In addition, the AGG-Dom creates additional requirements, including:

A) (U) Required notification by the FBI to the DOJ NSD concerning a Full Investigation that involves foreign intelligence collection, a Full Investigation of a United States person

(USPER) in relation to a threat to the national security, or a national security investigation involving a "sensitive investigative matter" (SIM) (see DIOG Section 10).

B) (U) An annual report by the FBI to the DOJ NSD concerning the FBI's foreign intelligence collection program, including information reflecting the scope and nature of foreign intelligence collection activities in each FBI field office.

C) (U) Access by the DOJ NSD to information obtained by the FBI through national security or foreign intelligence activities.

D) (U) General authority for the Assistant Attorney General for National Security to obtain reports from the FBI concerning these activities. (AGG-Dom, Intro. C)

(U) Further examples of oversight mechanisms include the involvement of both FBI and prosecutorial personnel in the review of undercover operations involving sensitive circumstances; notice requirements for investigations involving sensitive investigative matters; and notice and oversight provisions for Enterprise Investigations, which involve a broad examination of groups implicated in criminal and national security threats. These requirements and procedures help to ensure that the rule of law is respected in the FBI's activities and that public confidence is maintained in these activities. (AGG-Dom, Intro. C)

(U) In addition to the above-described oversight mechanisms, the FBI is subject to a regime of oversight, legal limitations, and self-regulation designed to ensure strict adherence to the Constitution. This regime is comprehensive and has many facets, including the following:

A) (U) The Foreign Intelligence Surveillance Act of 1978, as amended, and Title III of the Omnibus Crime Control and Safe Streets Act of 1968. These laws establish the processes for obtaining judicial approval of electronic surveillance and physical searches for the purpose of collecting foreign intelligence and electronic surveillance for the purpose of collecting evidence of crimes.

B) (U) The Whistleblower Protection Acts of 1989 and 1998. These laws protect whistleblowers from retaliation.

C) (U) The Freedom of Information Act of 1966. This law provides the public with access to FBI documents not covered by a specific statutory exemption.

D) (U) The Privacy Act of 1974. This law balances the government's need to maintain information about United States citizens and legal permanent resident aliens with the rights of those individuals to be protected against unwarranted invasions of their privacy stemming from the government's collection, use, maintenance, and dissemination of that information. The Privacy Act forbids the FBI and other federal agencies from collecting information about how individuals exercise their First Amendment rights, unless that collection is expressly authorized by statute or by the individual, or is pertinent to and within the scope of an authorized law enforcement activity (5 U.S.C. § 552a[e][7]). Activities authorized by the AGG-Dom – with the exception of Positive Foreign Intelligence collection (see DIOG Section 9.3) - are authorized law enforcement activities or activities for which there is otherwise statutory authority for purposes of the Privacy Act.

E) (U) Documents describing First Amendment activity that are subsequently determined to have been collected or retained in violation of the Privacy Act must be destroyed as set forth in Records Management Division (RMD) Policy Notice 0108N.

(U) Congress, acting primarily through the Judiciary and Intelligence Committees, exercises regular, vigorous oversight into all aspects of the FBI's operations. To this end, the National

Security Act of 1947 requires the FBI to keep the intelligence committees (for the Senate and House of Representatives) fully and currently informed of substantial intelligence activities. This oversight has significantly increased in breadth and intensity since the 1970's, and it provides important additional assurance that the FBI conducts its investigations according to the law and the Constitution. Advice on what activities fall within the supra of required congressional notification can be obtained from OCA [A Corporate Policy Directive is forthcoming].

(U) The FBI's intelligence activities (as defined in Section 3.4(e) of Executive Order (EO) 12333 [see DIOG Appendix B]) are subject to significant self-regulation and oversight beyond that conducted by Congress. The Intelligence Oversight Board (IOB), comprised of members from the President's Intelligence Advisory Board (PIAB), also conducts oversight of the FBI's intelligence activities. Among its responsibilities, the IOB must inform the President of intelligence activities the IOB believes: (i)(a) may be unlawful or contrary to EO or Presidential Decision Directive (PDD), and (b) are not being adequately addressed by the Attorney General, the Director of National Intelligence (DNI), or the head of the department concerned; or (ii) should be immediately reported to the President. The requirements and procedures for reporting potential IOB matters to OGC/NSLB can be found in Corporate Policy Directive 0188D (Guidance on IOB Matters), and the Policy Implementation Guide (PG) 0188PG.

(U) Internal FBI safeguards include:

A) (U) the OGC's Privacy and Civil Liberties Unit (PCLU), which reviews plans for any proposed FBI record system for compliance with the Privacy Act and related privacy protection requirements and policies and which provides legal advice on civil liberties questions;

B) (U) the criminal and national security undercover operations review committees, comprised of senior DOJ and FBI officials, which review all proposed undercover operations that involve sensitive circumstances;

C) (U) the Sensitive Operations Review Committee (SORC), comprised of senior DOJ and FBI officials, which provides oversight of those investigative activities that may impact civil liberties and privacy and that are not otherwise subject to high level FBI and DOJ review;

D) (U) the FBI requirement that all FBI employees report departures from and non-compliance with the DIOG to their supervisor, other management officials, or appropriate authorities as set forth in DIOG Sections 2.6 – 2.8 and 3.1.1; and

E) (U) training new FBI employees on privacy and periodic training for all FBI employees to maintain currency on the latest guidelines, changes to laws and regulations, and judicial decisions related to constitutional rights and liberties.

4.2 (U) PROTECTION OF FIRST AMENDMENT RIGHTS

(U) A fundamental principle of the Attorney General's Guidelines for FBI investigations and operations since the first guidelines were issued in 1976 has been that investigative activity may not be based solely on the exercise of rights guaranteed by the First Amendment to the United States Constitution. This principle carries through to the present day in the AGG-Dom. The Privacy Act contains a corollary principle – the government is prohibited from retaining information describing how a person exercises rights under the First Amendment, unless that

information is pertinent to or within the scope of an authorized law enforcement activity. 5 U.S.C. § 552a(e)(7).

(U) The First Amendment states:

> *(U) Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or of the right of the people peaceably to assemble, and to petition the Government for a redress of grievances.*

(U) Although the amendment appears literally to apply only to Congress, the Supreme Court made clear long ago that it also applies to activities of the Executive Branch, including law enforcement agencies. Therefore, for FBI purposes, it would be helpful to read the introduction to the first sentence as: "The FBI shall take no action respecting…" In addition, the word "abridging" must be understood. "Abridging," as used here, means "diminishing." Thus, it is not necessary for a law enforcement action to destroy or totally undermine the exercise of First Amendment rights for it to be unconstitutional; significantly diminishing or lessening the ability of individuals to exercise these rights without an authorized investigative purpose is sufficient.

(U) This is not to say that any diminution of First Amendment rights is unconstitutional. The Supreme Court has never held that the exercise of these rights is absolute. In fact, the Court has realistically interpreted the level and kind of government activity that violates a First Amendment right. For example, taken to an extreme, one could argue that the mere possibility of an FBI agent being present at an open forum (or as an on-line presence) would diminish the right of free speech by a participant in the forum because he/she would be afraid to speak freely. The Supreme Court, however, has never found an "abridgement" of First Amendment rights based on such a subjective fear. Rather, the Court requires an action that, from an objective perspective, truly diminishes the speaker's message or his/her ability to deliver it (e.g., pulling the plug on the sound system). For another example, requiring protestors to use a certain parade route may diminish their ability to deliver their message in a practical sense, but the Court has made it clear, that for legitimate reasons (e.g., public safety), the government may impose reasonable limitations in terms of time, place and manner on the exercise of such rights, as long as the ability to deliver the message remains.

(U) While the language of the First Amendment prohibits action that would abridge the enumerated rights, the implementation of that prohibition in the AGG-Dom reflects the Supreme Court's opinions on the constitutionality of law enforcement action that may impact the exercise of First Amendment rights. As stated above, the AGG-Dom prohibits investigative activity for the sole purpose of monitoring the exercise of First Amendment rights. The importance of the distinction between this language and the actual text of the First Amendment is two-fold: (i) the line drawn by the AGG-Dom prohibits even "monitoring" the exercise of First Amendment rights (far short of abridging those rights) as the sole purpose of FBI activity; and (ii) the requirement of an authorized purpose for all investigative activity provides additional protection for the exercise of constitutionally protected rights.

(U) The AGG-Dom classifies investigative activity that involves a religious or political organization (or an individual prominent in such an organization) or a member of the news media as a "sensitive investigative matter." That designation recognizes the sensitivity of conduct that traditionally involves the exercise of First Amendment rights by groups, e.g., who

associate for political or religious purposes or by the press. The requirements for opening and pursuing a "sensitive investigative matter" are set forth in DIOG Section 10. It should be clear, however, from the discussion below just how pervasive the exercise of First Amendment rights is in American life and that not all protected First Amendment activity will fall within the definition of a "sensitive investigative matter." Therefore, it is essential that FBI employees recognize when investigative activity may have an impact on the exercise of these fundamental rights and be especially sure that any such investigative activity has a valid law enforcement or national security purpose, even if it is not a "sensitive investigative matter" as defined in the AGG-Dom and the DIOG.

(U) Finally, it is important to note that individuals in the United States (and organizations comprised of such individuals) do not forfeit their First Amendment rights simply because they also engage in criminal activity or in conduct that threatens national security. For example, an organization suspected of engaging in acts of domestic terrorism may also pursue legitimate political goals and may also engage in lawful means to achieve those goals. The pursuit of these goals through constitutionally protected conduct does not insulate them from legitimate investigative focus for unlawful activities—but the goals and the pursuit of their goals through lawful means remain protected from unconstitutional infringement.

(U) When allegations of First Amendment violations are brought to a court of law, it is usually in the form of a civil suit in which a plaintiff has to prove some actual or potential harm. See, *e.g., Presbyterian Church v. United States,* 870 F.2d 518 (9th Cir. 1989) (challenging INS surveillance of churches). In a criminal trial, a defendant may seek either or both of two remedies as part of a claim that his or her First Amendment rights were violated: suppression of evidence gathered in the alleged First Amendment violation, a claim typically analyzed under the "reasonableness" clause of the Fourth Amendment, and dismissal of the indictment on the basis of "outrageous government conduct" in violation of the Due Process Clause of the Fifth Amendment.

(U) The scope of First Amendment rights and their impact on FBI investigative activity are discussed below. The First Amendment's "establishment clause"—the prohibition against the government establishing or sponsoring a specific religion—has little application to the FBI and, therefore, is not discussed here.

4.2.1 (U) FREE SPEECH

(U) The exercise of free speech includes far more than simply speaking on a controversial topic in the town square. It includes such activities as carrying placards in a parade, sending letters to a newspaper editor, posting information on the Internet, wearing a tee shirt with a political message, placing a bumper sticker critical of the President on one's car, and publishing books or articles. The common thread in these examples is conveying a public message or an idea through words or deeds. Law enforcement activity that diminishes a person's ability to communicate in any of these ways may interfere with his or her freedom of speech—and thus may not be undertaken by the FBI solely for that purpose.

(U) It is important to understand the line between constitutionally protected speech and advocacy of violence or of conduct that may lead to violence or other unlawful activity. In *Brandenburg v. Ohio, 395 U.S. 444 (1969)*, the Supreme Court established a two-part test to determine whether

such speech is constitutionally protected: the government may not prohibit advocacy of force or violence except when such advocacy (i) is intended to incite imminent lawless action, and (ii) is likely to do so. Therefore, even heated rhetoric or offensive provocation that could conceivably lead to a violent response in the future is usually protected. Suppose, for example, a politically active group advocates on its web site taking unspecified "action" against persons or entities it views as the enemy, who thereafter suffer property damage and/or personal injury. Under the *Brandenburg* two-part test, the missing specificity and imminence in the message may provide it constitutional protection. For that reason, law enforcement may take no action that, in effect, blocks the message or punishes its sponsors.

(U) Despite the high standard for interfering with free speech or punishing those engaged in it, the law does not preclude FBI employees from observing and collecting any of the forms of protected speech and considering its content—as long as those activities are done for a valid law enforcement or national security purpose and are conducted in a manner that does not unduly infringe upon the ability of the speaker to deliver his or her message. To be an authorized purpose it must be one that is authorized by the AGG-Dom—i.e., to further an FBI Assessment, Predicated Investigation, or other authorized function such as providing assistance to other agencies. Furthermore, by following the standards for opening or approving an Assessment or Predicated Investigation as contained in the DIOG, the FBI will ensure that there is a rational relationship between the authorized purpose and the protected speech to be collected such that a reasonable person with knowledge of the circumstances could understand why the information is being collected.

(U) Returning to the example posed above, because the group's advocacy of action could be directly related by circumstance to property damage suffered by one of the group's known targets, collecting the speech—although constitutionally protected—can lawfully occur. Similarly, listening to and documenting the public talks by a religious leader, who is suspected of raising funds for a terrorist organization, may yield clues as to his motivation, plan of action, and/or hidden messages to his followers. FBI employees should not, therefore, avoid collecting First Amendment protected speech if it is relevant to an authorized AGG-Dom purpose— as long as FBI employees do so in a manner that does not inhibit the delivery of the message or the ability of the audience to hear it, and so long as the collection is done in accordance with the discussion of least intrusive means or method in Section 4.4.

(U) In summary, during the course of lawful investigative activities, the FBI may lawfully collect, retain, and consider the content of constitutionally protected speech, so long as: (i) the collection is logically related to an authorized investigative purpose; (ii) the collection does not actually infringe on the ability of the speaker to deliver his or her message; and (iii) the method of collection complies with the least intrusive method policy.

4.2.2 (U) EXERCISE OF RELIGION

(U) Like the other First Amendment freedoms, the "free exercise of religion" clause is broader than commonly believed. First, it covers any form of worship of a deity—even forms that are commonly understood to be cults or fringe sects, as well as the right not to worship any deity. Second, protected religious exercise also extends to dress or food that is required by religious edict, attendance at a facility used for religious practice (no matter how unlikely it appears to be intended for that purpose), observance of the Sabbath, raising money for evangelical or

missionary purposes, and proselytizing. Even in controlled environments like prisons, religious exercise must be permitted—subject to reasonable restrictions as to time, place, and manner. Another feature of this First Amendment right is that religion is a matter of heightened sensitivity to some Americans—especially to devout followers. For this reason, religion is a matter that is likely to provoke an adverse reaction if the right is violated—regardless of which religion is involved. Therefore, when essential investigative activity may impact this right, the investigative activity must be conducted in a manner that avoids the actual—and the appearance of—interference with religious practice to the maximum extent possible.

(U) While there must be an authorized purpose for any investigative activity that could have an impact on religious practice, this does not mean religious practitioners or religious facilities are completely free from being examined as part of an Assessment or Predicated Investigation. If such practitioners are involved in—or such facilities are used for—activities that are the proper subject of FBI-authorized investigative or intelligence collection activities, their religious affiliation does not "immunize" them to any degree from these efforts. It is paramount, however, that the authorized purpose of such efforts be properly documented. It is also important that investigative activity directed at religious leaders or at conduct occurring within religious facilities be focused in time and manner so as not to infringe on legitimate religious practice by any individual but especially by those who appear unconnected to the activities under investigation.

(U) Furthermore, FBI employees may take appropriate cognizance of the role religion may play in the membership or motivation of a criminal or terrorism enterprise. If, for example, affiliation with a certain religious institution or a specific religious sect is a known requirement for inclusion in a violent organization that is the subject of an investigation, then whether a person of interest is a member of that institution or sect is a rational and permissible consideration. Similarly, if investigative experience and reliable intelligence reveal that members of a terrorist or criminal organization are known to commonly possess or exhibit a combination of religion-based characteristics or practices (e.g., group leaders state that acts of terrorism are based in religious doctrine), it is rational and lawful to consider such a combination in gathering intelligence about the group—even if any one of these, by itself, would constitute an impermissible consideration. By contrast, solely because prior subjects of an investigation of a particular group were members of a certain religion and they claimed a religious motivation for their acts of crime or terrorism, other members' mere affiliation with that religion, by itself, is not a basis to assess or investigate—absent a known and direct connection to the threat under Assessment or investigation. Finally, the absence of a particular religious affiliation can be used to eliminate certain individuals from further investigative consideration in those scenarios where religious affiliation is relevant.

4.2.3 (U) FREEDOM OF THE PRESS

(U) Contrary to what many believe, this well-known First Amendment right is not owned by the news media; it is a right of the American people. Therefore, this right covers such matters as reasonable access to news-making events, the making of documentaries, and various other forms of publishing the news. Although the news media typically seek to enforce this right, freedom of the press should not be viewed as a contest between law enforcement or national security, on the one hand, and the interests of news media, on the other. That said, the news gathering function is

the aspect of freedom of the press most likely to intersect with law enforcement and national security investigative activities.

(U) The interest of the news media in protecting confidential sources and the interest of agencies like the FBI in gaining access to those sources who may have evidence of a crime or national security intelligence often clash. The seminal case in this area is *Branzburg v. Hayes,* 408 U.S. 665 (1972), in which the Supreme Court held that freedom of the press does not entitle a news reporter to refuse to divulge the identity of his source to a federal grand jury. The Court reasoned that, as long as the purpose of law enforcement is not harassment or vindictiveness against the press, any harm to the news gathering function of the press (by revealing source identity) is outweighed by the need of the grand jury to gather evidence of crime.

(U) Partially in response to *Branzburg*, the Attorney General promulgated regulations that govern the issuance of subpoenas for reporter's testimony and telephone toll records, the arrest of a reporter for a crime related to news gathering, and the interview of a reporter as a suspect in a crime arising from the news gathering process. In addition, an investigation of a member of the news media in his official capacity, the use of a reporter as a source, and posing as a member of the news media are all sensitive circumstances in the AGG-Dom, DIOG and other applicable AGGs.

(U) These regulations are not intended to insulate reporters and other news media from FBI Assessments or Predicated Investigations. They are intended to ensure that investigative activity that seeks information from or otherwise involves members of the news media:

A) (U) Is appropriately authorized;

B) (U) Is necessary for an important law enforcement or national security objective;

C) (U) Is the least intrusive means to obtain the information or achieve the goals; and

D) (U) Does not unduly infringe upon the news gathering aspect of the constitutional right to freedom of the press.

4.2.4 (U) FREEDOM OF PEACEFUL ASSEMBLY AND TO PETITION THE GOVERNMENT FOR REDRESS OF GRIEVANCES

(U) Freedom of peaceful assembly, often called the right to freedom of association, presents unique issues for law enforcement agencies, including the FBI. Individuals who gather with others to protest government action, or to rally or demonstrate in favor of, or in opposition to, a social cause sometimes present a threat to public safety by their numbers, by their actions, by the anticipated response to their message, or by creating an opportunity for individuals or other groups with an unlawful purpose to infiltrate and compromise the legitimacy of the group for their own ends. The right to peaceful assembly includes more than just public demonstrations—it includes, as well, the posting of group web sites on the Internet, recruiting others to a cause, marketing a message, and fund raising. All are protected First Amendment activities if they are conducted in support of the organization or political, religious or social cause.

(U) The right to petition the government for redress of grievances is so linked to peaceful assembly and association that it is included in this discussion. A distinction between the two is that an individual may exercise the right to petition the government by himself whereas assembly

necessarily involves others. The right to petition the government includes writing letters to Congress, carrying a placard outside city hall that delivers a political message, recruiting others to one's cause, and lobbying Congress or an executive agency for a particular result.

(U) For the FBI, covert presence or action within associations or organizations, also called "undisclosed participation," has the greatest potential to impact this constitutional right. The Supreme Court addressed this issue as a result of civil litigation arising from one of the many protests against the Vietnam War. In *Laird v. Tatum,* 408 U.S. 1 (1972), the Court found that the mere existence of an investigative program—consisting of covert physical surveillance in public areas, infiltration of public assemblies by government operatives or sources, and the collection of news articles and other publicly available information—for the purpose of determining the existence and scope of a domestic threat to national security does not, by itself, violate the First Amendment rights of the members of the assemblies. The subjective "chill" to the right to assembly, based on the suspected presence of government operatives, did not by itself give rise to legal "standing" for plaintiffs to argue that their constitutional rights had been abridged. Instead, the Court required a showing that the complained-of government action would reasonably deter the exercise of that right.

(U) Since *Laird v. Tatum* was decided, the lower courts have examined government activity on many occasions to determine whether it gave rise to a "subjective chill" or an "objective deterrent." The basic standing requirement establish by *Laird* remains unchanged today. The lower courts, however, have often imposed a very low threshold of objective harm to survive a motion to dismiss the case. For example, plaintiffs who have shown a loss of membership in an organization, loss of financial support, loss to reputation and status in the community, and loss of employment by members have been granted standing to sue.

(U) More significant for the FBI than the standing issue has been the lower courts' evaluation of investigative activity into First Amendment protected associations since *Laird.* The courts have held the following investigative activities to be constitutionally permissible under First Amendment analysis:

A) (U) Undercover participation in group activities;

B) (U) Physical and video surveillance in public areas;

C) (U) Properly authorized electronic surveillance;

D) (U) Recruitment and operation of sources;

E) (U) Collection of information from government, public, and private sources (with consent); and

F) (U) The dissemination of information for a valid law enforcement purpose.

(U) However, these decisions were not reached in the abstract. In every case in which the courts have found government action to be proper, the government proved that the action was conducted for an authorized law enforcement or national security purpose and that the action was conducted in substantial compliance with controlling regulations. In addition, in approving these techniques, the courts have often considered whether a less intrusive technique was available to the agency, and the courts have balanced the degree of intrusion or impact against the importance of the law enforcement or national security objective.

(U) By contrast, since *Laird*, the courts have found these techniques to be legally objectionable:

A) (U) Opening an investigation solely because of the group's social or political agenda (even if the agenda made the group susceptible to subversive infiltration);

B) (U) Sabotaging or neutralizing the group's legitimate social or political agenda;

C) (U) Disparaging the group's reputation or standing;

D) (U) Leading the group into criminal activity that otherwise probably would not have occurred; and

E) (U) Undermining legitimate recruiting or funding efforts.

(U) In every such case, the court found the government's purpose was not persuasive, was too remote, or was too speculative to justify the intrusion and the potential harm to the exercise of First Amendment rights.

(U) Once again, the message is clear that investigative activity that involves assemblies or associations of individuals in the United States exercising their First Amendment rights must have an authorized purpose under the AGG-Dom—and one to which the information sought and the technique to be employed are rationally related. Less intrusive techniques should always be explored first and those authorizing such activity (which, as discussed above, will almost always constitute a sensitive investigative matter) should ensure that the investigative activity is focused as narrowly as feasible and that the purpose is thoroughly documented.

4.3 (U) EQUAL PROTECTION UNDER THE LAW

4.3.1 (U) INTRODUCTION

(U) The Equal Protection Clause of the United States Constitution provides in part that: "No State shall make or enforce any law which shall deny to any person within its jurisdiction the equal protection of the laws." The Supreme Court and the lower courts have made it clear that the Equal Protection Clause applies to the official acts of United States government law enforcement agents. See, *e.g., Whren v. United States,* 517 U.S. 806 (1996); see also *Chavez v. Illinois State Police,* 251 F.3d 612 (7th Cir. 2001).

Specifically, government employees are prohibited from engaging in invidious discrimination against individuals on the basis of race, ethnicity, national origin, or religious affiliation. This principle is further reflected and implemented for federal law enforcement in the United States Department of Justice's *Guidance Regarding the Use of Race by Federal Law Enforcement Agencies* (hereinafter "DOJ Guidance on the Use of Race").

(U) Investigative and intelligence collection activities must not be based solely on race, ethnicity, national origin, or religious affiliation. Any such activities that are based solely on such considerations are invidious by definition, and therefore, unconstitutional. This standard applies to all investigative and collection activity, including collecting and retaining information, opening investigations, disseminating information, and indicting and prosecuting defendants. It is particularly applicable to the retention and dissemination of personally identifying information about an individual—as further illustrated in the examples enumerated below.

(U) The constitutional prohibition against invidious discrimination based on race, ethnicity, national origin or religion is relevant to both the national security and criminal investigative programs of the FBI. National security investigations often have ethnic aspects; members of a foreign terrorist organization may be primarily or exclusively from a particular country or area of the world. Similarly, ethnic heritage is frequently the common thread running through violent gangs or other criminal organizations. It should be noted that this is neither a new nor isolated phenomenon. Ethnic commonality among criminal and terrorist groups has been relatively constant and widespread across many ethnicities throughout the history of the FBI.

4.3.2 (U) POLICY PRINCIPLES

(U) To ensure that Assessment and investigative activities and strategies consider racial, ethnic, national origin and religious factors properly and effectively and to help assure the American public that the FBI does not engage in invidious discrimination, the DIOG establishes the following policy principles:

A) (U) The prohibition on basing investigative activity solely on race or ethnicity is not avoided by considering it in combination with other prohibited factors. For example, a person of a certain race engaging in lawful public speech about his religious convictions is not a proper subject of investigative activity based solely on any one of these factors—or by their combination. Before collecting and using information on race, religion or other prohibited factors, a well-founded and authorized investigative purpose must exist beyond these prohibited factors.

B) (U) When race or ethnicity is a relevant factor to consider, it should not be the dominant or primary factor. Adherence to this standard will not only ensure that it is never the sole factor—it will also preclude undue and unsound reliance on race or ethnicity in investigative analysis. It reflects the recognition that there are thousands and, in some cases, millions of law abiding people in American society of the same race or ethnicity as those who are the subjects of FBI investigative activity, and it guards against the risk of sweeping them into the net of suspicion without a sound investigative basis.

C) (U) The FBI will not collect or use behavior or characteristics common to a particular racial or ethnic community as investigative factors unless the behavior or characteristics bear clear and specific relevance to a matter under Assessment or investigation. This policy is intended to prevent the potential that collecting ethnic characteristics or behavior will inadvertently lead to individual identification based solely on such matters, as well as to avoid the appearance that the FBI is engaged in ethnic or racial profiling.

4.3.3 (U) GUIDANCE ON THE USE OF RACE AND ETHNIC IDENTITY IN ASSESSMENTS AND PREDICATED INVESTIGATIONS

(U) Considering the reality of common ethnicity or race among many criminal and terrorist groups, some question how the prohibition against racial or ethnic profiling is to be effectively applied—and not violated—in FBI Assessments and Predicated Investigations. The question arises generally in two contexts: (i) with respect to an individual or a group of individuals; and (ii) with respect to ethnic or racial communities as a whole.

4.3.3.1 (U) Individual Race or Ethnicity as a Factor

(U) The DOJ Guidance on the Use of Race permits the consideration of ethnic and racial identity information based on specific reporting—such as from an eyewitness. As a general rule, race or ethnicity as an identifying feature of a suspected perpetrator, subject, and in some cases, a victim, is relevant if it is based on reliable evidence or information—not conjecture or stereotyped assumptions. In addition, the DOJ Guidance on the Use of Race permits consideration of race or ethnicity in other investigative or collection scenarios if it is relevant. These examples illustrate:

A) (U) The race or ethnicity of suspected members, associates, or supporters of an ethnic-based gang or criminal enterprise may be collected and retained when gathering information about or investigating the organization.

B) (U) Ethnicity may be considered in evaluating whether a subject is—or is not—a possible associate of a criminal or terrorist group that is known to be comprised of members of the same ethnic grouping—as long as it is not the dominant factor for focusing on a particular person. It is axiomatic that there are many members of the same ethnic group who are not members of the criminal or terrorist group; for that reason, there must be other information beyond race or ethnicity that links the individual to the terrorist or criminal group or to the other members of the group. Otherwise, racial or ethnic identity would be the sole criterion, and that is impermissible.

4.3.3.2 (U) Community Race or Ethnicity as a Factor

4.3.3.2.1 (U) Collecting and Analyzing Demographics

(U) The DOJ Guidance on the Use of Race and FBI policy permit the FBI to identify locations of concentrated ethnic communities in the field office's domain, if these locations will reasonably aid the analysis of potential threats and vulnerabilities, and, overall, assist domain awareness for the purpose of performing intelligence analysis. If, for example, intelligence reporting reveals that members of certain terrorist organizations live and operate primarily within a certain concentrated community of the same ethnicity, the location of that community is clearly valuable—and properly collectible—data. Similarly, the locations of ethnic-oriented businesses and other facilities may be collected if their locations will reasonably contribute to an awareness of threats and vulnerabilities, and intelligence collection opportunities. Also, members of some communities may be potential victims of civil rights crimes and, for this reason, community location may aid enforcement of civil rights laws. Information about such communities should not be collected, however, unless the communities are sufficiently concentrated and established so as to provide a reasonable potential for intelligence collection that would support FBI mission programs (e.g., where identified terrorist subjects from certain countries may relocate to blend in and avoid detection).

4.3.3.2.2 (U) Geo-Mapping Ethnic/Racial Demographics

(U) As a general rule, if information about community demographics may be collected, it may be "mapped." Sophisticated computer geo-mapping technology visually depicts lawfully collected information and can assist in showing relationships among disparate data. By itself,

mapping raises no separate concerns about racial or ethnic profiling, assuming the underlying information that is mapped was properly collected. It may be used broadly - e.g., for domain awareness of all relevant demographics in the field office's area of responsibility or to track crime trends – or narrowly to identify specific communities or areas of interest to inform a specific Assessment or investigation. In each case, the relevance of the ethnic or racial information mapped to the authorized purpose of the Assessment or investigation must be clearly demonstrated and documented.

4.3.3.2.3 (U) General Ethnic/Racial Behavior

(U) The authority to collect ethnic community location information does not extend to the collection of cultural and behavioral information about an ethnic community that bears no rational relationship to a valid investigative or analytical need. Every ethnic community in the Nation that has been associated with a criminal or national security threat has a dominant majority of law-abiding citizens, resident aliens, and visitors who may share common ethnic behavior but who have no connection to crime or terrorism (as either subjects or victims). For this reason, a broad-brush collection of racial or ethnic characteristics or behavior is not helpful to achieve any authorized FBI purpose and may create the appearance of improper racial or ethnic profiling.

4.3.3.2.4 (U) Specific and Relevant Ethnic Behavior

(U) On the other hand, knowing the behavioral and life style characteristics of known individuals who are criminals or who pose a threat to national security may logically aid in the detection and prevention of crime and threats to the national security within the community and beyond. Focused behavioral characteristics reasonably believed to be associated with a particular criminal or terrorist element of an ethnic community (not with the community as a whole) may be collected and retained. For example, if it is known through intelligence analysis or otherwise that individuals associated with an ethnic-based terrorist or criminal group conduct their finances by certain methods, travel in a certain manner, work in certain jobs, or come from a certain part of their home country that has established links to terrorism, those are relevant factors to consider when investigating the group or assessing whether it may have a presence within a community. It is recognized that the "fit" between specific behavioral characteristics and a terrorist or criminal group is unlikely to be perfect—that is, there will be members of the group who do not exhibit the behavioral criteria as well as persons who exhibit the behaviors who are not members of the group. Nevertheless, in order to maximize FBI mission relevance and to minimize the appearance of racial or ethnic profiling, the criteria used to identify members of the group within the larger ethnic community to which they belong must be as focused and as narrow as intelligence reporting and other circumstances permit. If intelligence reporting is insufficiently exact so that it is reasonable to believe that the criteria will include an unreasonable number of people who are not involved, then it would be inappropriate to use the behaviors, standing alone, as the basis for FBI activity.

4.3.3.2.5 (U) EXPLOITIVE ETHNIC BEHAVIOR

(U) A related category of information that can be collected is behavioral and cultural information about ethnic or racial communities that is reasonably likely to be exploited by criminal or terrorist groups who hide within those communities in order to engage in illicit activities undetected. For example, the existence of a cultural tradition of collecting funds from members within the community to fund charitable causes in their homeland at a certain time of the year (and how that is accomplished) would be relevant if intelligence reporting revealed that, unknown to many donors, the charitable causes were fronts for terrorist organizations or that terrorist supporters within the community intended to exploit the unwitting donors for their own purposes.

4.4 (U) LEAST INTRUSIVE METHOD

4.4.1 (U) OVERVIEW

(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 a more intrusive method. This principle is also reflected in See Appendix B: Executive Order 12333, which governs the activities of the United States Intelligence Community. The concept of least intrusive method applies to the collection of all information. Regarding the collection of foreign intelligence that is not collected as part of the FBI's traditional national security or criminal missions, the AGG-Dom further requires that open and overt collection activity must be used with USPERs, if feasible.

(U) By emphasizing the use of the least intrusive means to obtain information, FBI employees can effectively execute their duties while mitigating potential negative impact on the privacy and civil liberties of all people encompassed within the investigation, including targets, witnesses, and victims. This principle is not intended to discourage FBI employees from seeking relevant and necessary information, but rather is intended to encourage investigators to choose the least intrusive—but still reasonable—means from the available options to obtain the information.

(U) This principle is embodied in statutes and DOJ policies on a variety of topics including electronic surveillance, the use of tracking devices, the temporary detention of suspects, and forfeiture. In addition, the concept of least intrusive method can be found in case law as a factor to be considered in assessing the reasonableness of an investigative method in the face of a First Amendment or due process violation claim. See *Clark v. Library of Congress*, 750 F.2d 89, 94-5 (D.C. Cir. 1984); *Alliance to End Repression v. City of Chicago*, 627 F. Supp. 1044, 1055 (N.D. Ill. 1985), citing *Elrod v. Burns*, 427 U.S. 347, 362-3 (1976).

4.4.2 (U) GENERAL APPROACH TO LEAST INTRUSIVE METHOD CONCEPT

(U) Determining what constitutes the least intrusive method in an investigative or intelligence collection scenario is both a logical process and an exercise in judgment. It is logical in the sense that the FBI employee must first confirm that the selected technique will:

A) (U) Gather information that is relevant to the Assessment or Predicated Investigation;

B) (U) Acquire the information within the time frame required by the assessment or Predicated Investigation;

C) (U) Gather the information consistent with operational security and the protection of sensitive sources and methods; and

D) (U) Gather information in a manner that provides confidence in its accuracy.

(U) Determining the least intrusive method also requires sound judgment because the factors discussed above are not fixed points on a checklist. They require careful consideration based on a thorough understanding of investigative objectives and circumstances.

4.4.3 (U) DETERMINING INTRUSIVENESS

(U) The degree of procedural protection that established law and the AGG-Dom provide for the use of the method helps to determine its intrusiveness. Using this factor, search warrants, wiretaps, and undercover operations are very intrusive. By contrast, investigative methods with limited procedural requirements, such as checks of government and commercial data bases and communication with established sources, are less intrusive.

(U) The following guidance is designed to assist FBI personnel in judging the relative intrusiveness of different methods:

A) (U) ***Nature of the information sought:*** Investigative objectives generally dictate the type of information required and from whom it should be collected. This subpart is not intended to address the situation where the type of information needed and its location are so clear that consideration of alternatives would be pointless. When the option exists to seek information from any of a variety of places, however, it is less intrusive to seek information from less sensitive and less protected places. Similarly, obtaining information that is protected by a statutory scheme (e.g., financial records) or an evidentiary privilege (e.g., attorney/client communications) is more intrusive than obtaining information that is not so protected. In addition, if there exists a reasonable expectation of privacy under the Fourth Amendment (i.e., private communications), obtaining that information is more intrusive than obtaining information that is knowingly exposed to public view as to which there is no reasonable expectation of privacy.

B) (U) ***Scope of the information sought:*** Collecting information regarding an isolated event—such as a certain phone number called on a specific date or a single financial transaction—is less intrusive or invasive of an individual's privacy than collecting a complete communications or financial "profile." Similarly, a complete credit history is a more intrusive view into an individual's life than a few isolated credit charges. In some cases, of course, a complete financial and credit profile is exactly what the investigation requires (for example, investigations of terrorist financing or money laundering). If so, FBI employees should not hesitate to use appropriate legal process to obtain such information if the predicate requirements are satisfied. Operational security—such as source protection—may also dictate seeking a wider scope of information than is absolutely necessary for the purpose of protecting a specific target or source. When doing so, however, the concept of least intrusive method still applies. The FBI may obtain more data than strictly needed, but it should obtain no more data than is needed to accomplish the investigative or operational security purpose.

C) (U) ***Scope of the use of the method:*** Using a method in a manner that captures a greater picture of an individual's or a group's activities are more intrusive than using the same method or a different one that is focused in time and location to a specific objective. For example, it is

less intrusive to use a tracking device to verify point-to-point travel than it is to use the same device to track an individual's movements over a sustained period of time. Sustained tracking on public highways would be just as lawful but more intrusive because it captures a greater portion of an individual's daily movements. Similarly, surveillance by closed circuit television that checks a discrete location within a discrete time frame is less intrusive than 24/7 coverage of a wider area. For another example, a computer intrusion device that captures only host computer identification information is far less intrusive than one that captures file content.

D) (U) ***Source of the information sought:*** It is less intrusive to obtain information from existing government sources (such as state, local, tribal, international, or federal partners) or from publicly-available data in commercial data bases, than to obtain the same information from a third party (usually through legal process) that has a confidential relationship with the subject—such as a financial or academic institution. Similarly, obtaining information from a reliable confidential source who is lawfully in possession of the information and lawfully entitled to disclose it (such as obtaining an address from an employee of a local utility company) is less intrusive than obtaining the information from an entity with a confidential relationship with the subject. It is recognized in this category that the accuracy and procedural reliability of the information sought is an important factor in choosing the source of the information. For example, even if the information is available from a confidential source, a grand jury subpoena, national security letter, ex parte order, or other process may be required in order to ensure informational integrity and accuracy.

E) (U) ***The risk of public exposure:*** Seeking information about an individual or group under circumstances that create a risk that the contact itself and the information sought will be exposed to the individual's or group's detriment and/or embarrassment—particularly if the method used carries no legal obligation to maintain silence—is more intrusive than information gathering that does not carry that risk. Interviews with employers, neighbors, and associates, for example, or the issuance of grand jury subpoenas at a time when the investigation has not yet been publicly exposed are more intrusive than methods that gather information covertly. Similarly, interviews of a subject in a discrete location would be less intrusive than an interview at, for example, a place of employment or other location where the subject is known.

(U) There is a limit to the utility of this list of intrusiveness factors. Some factors may be inapplicable in a given investigation and, in many cases, the choice and scope of the method will be dictated wholly by investigative objectives and circumstances. The foregoing is not intended to provide a comprehensive checklist or even an overall continuum of intrusiveness. It is intended instead to identify the factors involved in a determination of intrusiveness and to attune FBI employees to select, within each applicable category, a less intrusive method if operational circumstances permit. In the end, selecting the least intrusive method that will accomplish the objective is a matter of sound judgment. In exercising such judgment, however, consideration of these factors should ensure that the decision to proceed is well founded.

4.4.4 (U) STANDARD FOR BALANCING INTRUSION AND INVESTIGATIVE REQUIREMENTS

(U) Once an appropriate method and its deployment have been determined, reviewing and approving authorities should balance the level of intrusion against investigative requirements. This balancing test is particularly important when the information sought involves clearly established constitutional, statutory, or evidentiary rights or sensitive circumstances (such as obtaining information from religious or academic institutions or public fora where First

Amendment rights are being exercised), but should be applied in all circumstances to ensure that the least intrusive method if reasonable based upon the circumstances of the investigation is being utilized.

(U) Balancing the factors discussed above with the considerations discussed below will help determine whether the method and the extent to which it intrudes into privacy or threatens civil liberties are proportionate to the significance of the case and the information sought.

(U) Considerations on the investigative side of the balancing scale include the:

A) (U) Seriousness of the crime or national security threat;

B) (U) Strength and significance of the intelligence/information to be gained;

C) (U) Amount of information already known about the subject or group under investigation; and

D) (U) Requirements of operational security, including protection of sources and methods.

(U) If, for example, the threat is remote, the individual's involvement is speculative, and the probability of obtaining probative information is low, intrusive methods may not be justified, and, in fact, they may do more harm than good. At the other end of the scale, if the threat is significant and possibly imminent (e.g., a bomb threat), aggressive measures would be appropriate regardless of intrusiveness.

(U) In addition, with respect to the investigation of a group, if the terrorist or criminal nature of the group and its membership is well established (e.g., al Qaeda, Ku Klux Klan, Colombo Family of La Cosa Nostra), there is less concern that pure First Amendment activity is at stake than there would be for a group whose true character is not yet known (e.g., an Islamic charity suspected of terrorist funding) or many of whose members appear to be solely exercising First Amendment rights (anti-war protestors suspected of being infiltrated by violent anarchists). This is not to suggest that investigators should be less aggressive in determining the true nature of an unknown group that may be engaged in terrorism or other violent crime. Indeed, a more aggressive and timely approach may be in order to determine whether the group is violent or to eliminate it as a threat. Nevertheless, when First Amendment rights are at stake, the choice and use of investigative methods should be focused in a manner that minimizes potential infringement of those rights. Finally, as the investigation progresses and the subject's or group's involvement becomes clear, more intrusive methods may be justified. Conversely, if reliable information emerges refuting the individual's involvement or the group's criminal or terrorism connections, the use of any investigative methods must be carefully reconsidered.

(U) Another consideration to be balanced is operational security: if a less intrusive but reasonable method were selected, would the subject detect its use and alter his activities—including his means of communication—to thwart the success of the operation? Operational security—particularly in national security investigations—should not be undervalued and may, by itself, justify covert tactics which, under other circumstances, would not be the least intrusive.

4.4.5 (U) Conclusion

(U) The foregoing guidance is offered to assist FBI employees in navigating the often unclear course to select the least intrusive investigative method that effectively accomplishes the operational objective at hand. In the final analysis, choosing the method that must appropriately

balances the impact on privacy and civil liberties with operational needs, is a matter of judgment, based on training and experience. Pursuant to the AGG-Dom, other applicable laws and policies, and this guidance, FBI employees may use any lawful method allowed, even if intrusive, where the intrusiveness is warranted by the threat to the national security or to potential victims of crime and/or the strength of the information indicating the existence of that threat.

This Page is Intentionally Blank.

5 (U) ASSESSMENTS

5.1 (U) OVERVIEW AND ACTIVITIES AUTHORIZED PRIOR TO OPENING AN ASSESSMENT

(U//FOUO) The AGG-Dom combines "threat assessments" under the former *Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection* and the "prompt and extremely limited checking out of initial leads" under the former Attorney *General's Guidelines on General Crimes, Racketeering Enterprise and Terrorism Enterprise Investigations* into a new investigative category entitled "Assessments."

(U//FOUO) All Assessments must be documented in the appropriate form, to include an FD-71, Guardian (FD-71a), or EC, and the form must be placed in one of the following files:

A) (U//FOUO) *investigative classification as an Assessment file* (e.g., 415A-WF-xxxxxx);

B) (U//FOUO) *zero sub-assessment file* (e.g., 91-0-ASSESS-D; 15-0-ASSESS; 315-0-ASSESS-D);

C) (U//FOUO) *zero classification file* (e.g. 196-WF-0). This file may be used if information is entered in the FD-71 or FD-71a and an Assessment is not opened based on that information;

D) (U//FOUO) *800 series (801-807) classification file*, as discussed in greater detail below;

E) (U//FOUO) *unaddressed work file*; or

F) (U//FOUO) *existing open or closed file*.

(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 this section of the DIOG. The USIC, however, also uses the word "assessment" to describe written intelligence products, as discussed in DIOG Sections 15.2.3 and 15.6.1.2.

(U) Assessments authorized under the AGG-Dom do not require a particular factual predication but do require an authorized purpose and clearly defined objective(s). Assessments may be carried out to detect, obtain information about, or prevent or protect against Federal crimes or threats to the national security or to collect foreign intelligence. (AGG-Dom, Part II and Part II.A)

(U//FOUO) Although "no particular factual predication" is required, the basis of an Assessment cannot be arbitrary or groundless speculation, nor can an Assessment be based solely on the exercise of First Amendment protected activities or on the race, ethnicity, national origin or religion of the subject. Although difficult to define, "no particular factual predication" is less than "information or allegation" as required for the initiation of a preliminary investigation (PI). For example, an Assessment may be conducted when: (i) there is reason to collect information or facts to determine whether there is a criminal or national security threat; and (ii) there is a rational and articulable relationship between the stated authorized purpose of the Assessment on the one hand and the information sought and the proposed means to obtain that information on the other. An FBI employee must be able to explain the authorized purpose and the clearly

defined objective(s), and reason the particular investigative methods were used to conduct the Assessment. FBI employees who conduct Assessments are responsible for ensuring that Assessments are not pursued for frivolous or improper purposes and are not based solely on First Amendment activity or on the race, ethnicity, national origin, or religion of the subject of the Assessment, or a combination of only such factors. (AGG-Dom, Part II)

(U//FOUO) When employees undertake activities authorized in DIOG Section 5.1.1below prior to opening an Assessment they must have a reason to undertake these activities that is tied to an authorized FBI criminal or national security purpose.

5.1.1 (U) ACTIVITIES AUTHORIZED PRIOR TO OPENING AN ASSESSMENT

(U//FOUO) When initially processing a complaint, observation, or information, an FBI employee can use the following investigative methods:

5.1.1.1 (U) PUBLIC INFORMATION

(U//FOUO) See DIOG section 18.5.1.

(U//FOUO) Prior to opening an Assessment, consent searches are not authorized. However, if in the course of processing a complaint or conducting a clarifying interview of the complainant, the complainant volunteers to provide access to his personal or real property, an agent may accept and conduct a search of the item(s) or property voluntarily provided.

5.1.1.2 (U) RECORDS OR INFORMATION - FBI AND DOJ

(U//FOUO) See DIOG section 18.5.2.

5.1.1.3 (U) RECORDS OR INFORMATION – OTHER FEDERAL, STATE, LOCAL, TRIBAL, OR FOREIGN GOVERNMENT AGENCY

(U//FOUO) See DIOG Section 18.5.3.

5.1.1.4 (U) ON-LINE SERVICES AND RESOURCES

(U//FOUO) See DIOG Section 18.5.4.

5.1.1.5 (U) CLARIFYING INTERVIEW

(U//FOUO) Conduct a voluntary clarifying interview of the complainant or the person who initially furnished the information.

(U//FOUO) See DIOG Section 18.5.6.

5.1.1.6 (U) INFORMATION VOLUNTARILY PROVIDED BY GOVERNMENTAL OF PRIVATE ENTITIES

(U//FOUO) See DIOG Section 18.5.7.

(U//FOUO) With the benefit of a clarifying interview, checking records (existing/historical information), and/or asking an existing CHS about something that he or she already knows, an

FBI employee may be able to answer the following question when evaluating the initial complaint, observation, or information: Does the complaint, observation, or information appear to represent a credible basis to open an Assessment, with an authorized purpose and clearly defined objective(s), or to open a Predicated Investigation consistent with the standards set forth in the DIOG?

(U//FOUO) **Intelligence Analysis and Planning:** These activities may allow the FBI employee to resolve a matter without the need to conduct new investigative activity, for which an Assessment or a Predicated Investigation must be opened. When conducting clarifying interviews and checking records as described above, FBI employees must always adhere to the core values and principles articulated in DIOG Sections 3 and 4.

5.1.2 (U) DOCUMENTATION REQUIREMENTS FOR RECORD CHECKS: (EXISTING /HISTORICAL INFORMATION REFERRED TO IN SECTION 5.1.1 ABOVE)

(U//FOUO) FBI employees must document and retain records checks in an FD-71, FD-71a or successor intake form or other system of records if, in the judgment of the FBI employee, there is a law enforcement, intelligence or public safety purpose to do so. If such record checks are documented, they must also be retained in one of the following files:

A) (U//FOUO) zero classification file when no further investigative activity is warranted;

B) (U//FOUO) relevant open or closed zero sub-assessment file;

C) (U//FOUO) relevant open or closed Predicated Investigation file;

D) (U//FOUO) new Assessment or Predicated Investigation file, when further investigative activity is warranted; or

E) (U//FOUO) unaddressed work file.

(U//FOUO) Additionally, through analysis of existing information, the FBI employee may produce products that include, but are not limited to: an Intelligence Assessment, Intelligence Bulletin and Geospatial Intelligence (mapping). If, while conducting analysis, the FBI employee finds a gap in intelligence that is relevant to an authorized FBI activity, then the FBI employee can identify the gap for possible development of a "collection requirement." The FBI employee must document this analysis in the applicable 801-807 classification file (or other 800-series classification file as directed in the Intelligence Policy Implementation Guide (IPG)). See the IPG for file classification guidance.

5.1.3 (U) LIAISON ACTIVITIES AND TRIPWIRES

(U) Some FBI activities are not traditional investigative or intelligence activities. Activities such as liaison, tripwires, and other community outreach represent relationship-building efforts or other pre-cursors to developing and maintaining good partnerships. These activities are critical to the success of the FBI's mission. DIOG Section 11 addresses liaison activities and tripwires.

5.2 (U) PURPOSE AND SCOPE

(U//FOUO) The FBI cannot be content to wait for leads to come in through the actions of others; rather, we must be vigilant in detecting criminal or national security threats to the full extent

permitted by law, with an eye towards early intervention and prevention of criminal or national security incidents before they occur. For example, to carry out the central mission of protecting the national security, the FBI must proactively collect information from available sources in order to identify threats and activities and to inform appropriate intelligence analysis. Collection required to inform such analysis will appear as FBI National Collection Requirements and FBI Field Office Collection Requirements. Likewise, in the exercise of its protective functions, the FBI is not constrained to wait until information is received indicating that a particular event, activity or facility has drawn the attention of would-be perpetrators of crime or terrorism. The proactive authority conveyed to the FBI is designed for, and may be used by, the FBI in the discharge of these responsibilities. The FBI may also conduct Assessments as part of its special events management responsibilities. (AGG-Dom, Part II)

(U) More broadly, detecting and interrupting criminal activities at their early stages, and preventing crimes from occurring in the first place, is preferable to allowing criminal plots to come to fruition. Hence, Assessments may also be undertaken proactively with such purposes as detecting criminal activities; obtaining information on individuals, groups, or organizations of possible investigative interest, either because they may be involved in criminal or national security-threatening activities or because they may be targeted for attack or victimization in such activities; and identifying and assessing individuals who may have value as confidential human sources. (AGG-Dom, Part II).

(U//FOUO) As described in the scenarios below, Assessments may be used when an "allegation or information" or an "articulable factual basis" (the predicates for Predicated Investigations) concerning crimes or threats to the national security is obtained and the matter can be checked out or resolved through the relatively non-intrusive methods authorized in Assessments (use of least intrusive means). The checking of investigative leads in this manner can avoid the need to proceed to more formal levels of investigative activity (Predicated Investigation), if the results of an Assessment indicate that further investigation is not warranted. (AGG-Dom, Part II) Hypothetical fact patterns are discussed below:

5.2.1 (U) SCENARIOS

(U/FOUO) Scenario 1: [redacted] b7E

(U//FOUO) [redacted] b7E

b7E

(U//FOUO)

b7E

(U/FOUO) Scenario 2:

b7E

(U//FOUO)

b7E

(U/FOUO) Scenario 3:

b7E

(U//FOUO)

b7E

(U/FOUO) Scenario 4

b7E

(U//FOUO)

b7E

(U//FOUO)

b7E

(U/FOUO) Scenario 5: b7E

(U//FOUO) b7E

b7E

(U//FOUO)

(U/FOUO) Scenario 6: b7E

(U//FOUO) b7E

(U/FOUO) Scenario 7: b7E

(U//FOUO) b7E

(U/FOUO) Scenario 8 b7E

(U//FOUO) b7E

5.3 (U) CIVIL LIBERTIES AND PRIVACY

(U) The pursuit of legitimate goals without infringing upon the exercise of constitutional freedoms is a challenge that the FBI meets through the application of sound judgment and discretion. In order to ensure civil liberties are not infringed upon through Assessments, every Assessment must have an authorized purpose and clearly defined objective(s). The authorized purpose and clearly defined objective(s) of the Assessment must be documented and retained as described in this section and in DIOG Section 14.

(U) Even when an authorized purpose is present, an Assessment could create the appearance that it is directed at or activated by constitutionally-protected activity, race, ethnicity, national origin or religion—particularly under circumstances where the link to an authorized FBI mission is not readily apparent. In these situations, it is vitally important that the authorized purpose and the clearly defined objective(s), as well as the use of any investigative methods, are well documented.

(U) No investigative activity, including Assessments, may be taken solely on the basis of activities that are protected by the First Amendment or on the race, ethnicity, national origin or religion of the subject, or a combination of only such factors. If an Assessment touches on or is partially motivated by First Amendment activities, or by race, ethnicity, national origin or religion, or a combination of only such factors, it is particularly important to identify and document the basis for the Assessment with clarity.

(U//FOUO) *Example:* Individuals or groups who communicate with each other or with members of the public in any form in pursuit of social or political causes—such as opposing war or foreign policy, protesting government actions, promoting certain religious beliefs, championing particular local, national, or international causes, or advocating a change in government through non-criminal means, and actively recruiting others to join their causes—have a fundamental constitutional right to do so. An Assessment may not be opened based solely on the exercise of these First Amendment rights. If, however, a group exercising its First Amendment rights also threatens or advocates violence or destruction of property, an Assessment would be appropriate.

(U) The AGG-Dom require that the "least intrusive" means or method be considered and—if reasonable based upon the circumstances of the investigation—used in lieu of more intrusive methods to obtain information, intelligence and/or evidence. This principle is also reflected in Executive Order 12333 (see Appendix B), which governs the activities of the USIC. Executive Order 12333 lays out the goals, directions, duties and responsibilities of the USIC. The concept of least intrusive means applies to the collection of all information, intelligence and evidence, not just that collected by those aspects of the FBI that are part of the intelligence community.

(U) By emphasizing the use of the least intrusive means to obtain information, intelligence, and/or evidence, FBI employees can effectively execute their duties while mitigating the potential negative impact on the privacy and civil liberties and the damage to the reputation of all people encompassed within the investigation or Assessment, including targets, witnesses, and victims. This principle is not intended to discourage FBI employees from seeking relevant and necessary intelligence, information, or evidence, but rather is intended to encourage FBI employees to choose the least intrusive—but still reasonable based upon the circumstances of the

investigation—means from the available options to obtain the information. (AGG-Dom, Part I.C.2)

5.4 (U) Five Types of Assessments (AGG-Dom, Part II.A.3.)

5.4.1 (U) Assessment Types

(U) There are five (5) authorized types of Assessments that may be carried out for the purposes of detecting, obtaining information about, or preventing or protecting against Federal crimes or threats to the national security or to collect foreign intelligence. The types of Assessments are:

A) (U) ***Type 1 & 2 Assessment***[4]***:*** Seek information, proactively or in response to investigative leads, relating to activities – or the involvement or role of individuals, groups, or organizations relating to those activities – constituting violations of Federal criminal law or threats to the national security;

B) (U) ***Type 3 Assessment:*** Identify, obtain and utilize information about actual or potential national security threats or Federal criminal activities, or the vulnerability to such threats or activities;

C) (U) ***Type 4 Assessment:*** Obtain and retain information to inform or facilitate intelligence analysis and planning;

D) (U) ***Type 5 Assessment:*** Seek information to identify potential human sources, assess their suitability, credibility, or value of individuals as human sources; and

E) (U) ***Type 6 Assessment:*** Seek information, proactively or in response to investigative leads, relating to matters of foreign intelligence interest responsive to foreign intelligence requirements.

5.5 (U) Standards for Opening or Approving an Assessment

(U//FOUO) Before opening or approving an Assessment, an FBI employee or approving official must determine whether:

A) (U//FOUO) An authorized purpose and clearly defined objective(s) exists for the conduct of the Assessment;

B) (U//FOUO) The Assessment is not based solely on the exercise of First Amendment activities or on the race, ethnicity, national origin or religion of the subject, or a combination of only such factors; and

C) (U//FOUO) The Assessment is an appropriate use of personnel and financial resources.

[4] (U//FOUO) In the original DIOG (12/16/2008), types I and 2 were considered to be separate Assessment types. Because they, however, have many commonalities, they were merged into one type (named a "Type 1 & 2 Assessment") for purposes of this version of the DIOG. Hence, there are now five, not six, types of Assessments.

5.6 (U) Position Equivalents, Effective Date, Duration, Documentation, Approval, Notice, File Review and Responsible Entity

5.6.1 (U) Field Office and FBIHQ Position Equivalents

(U//FOUO) FBIHQ and FBI field offices have the authority to conduct all Assessment activities as authorized in Section 5.4 above. Position equivalents for field office and FBIHQ personnel when FBIHQ opens, conducts, or closes an Assessment are specified in DIOG Section 3.11.

5.6.2 (U) Effective Date of Assessments

(U//FOUO) For all Assessments, the effective date of the Assessment is the date the final approval authority approves the FD-71, Guardian (FD-71a) or EC. Documenting the effective date of an Assessment is important for many reasons, including establishing time frames for justification and file reviews, and extensions. The effective date of the final approval authority occurs when:

A) (U//FOUO) **For Type 1 & 2 Assessments:** the SSA or SIA opens and assigns the FD-71 or Guardian (FD-71a) to the employee;

(U//FOUO) Note: In Type 1 & 2 Assessments only, employees do not need to obtain supervisory approval prior to opening the Assessment. If, however, oral approval is obtained, employees must memorialize the oral approval date in the body of the FD-71 or Guardian (FD-71a).

B) (U//FOUO) **For Type 3 – 6 Assessments:** the SSA, SIA, or the DI opens and assigns the Assessment [redacted] (ii) handwriting his/her initials and date on the EC; or b5

C) (U//FOUO) **For Sensitive Investigative Matters (SIM) Assessments:** the SAC (or SC) authorizes the Assessment to be opened and assigned to an FBI employee [redacted] FD-71 or Guardian (FD-71a) [redacted] (iii) handwriting his/her initials and date on the EC. (See DIOG Sections 5.7 and 10).

5.6.3 (U) Assessment Types

(U//FOUO) The applicable duration, documentation, approval level, notice, justification/file review, and responsible entity requirements for each of the five (5) types of Assessments are discussed below.

(U//FOUO) In all types of Assessments, investigative leads, either Action Required or Information Only, may only be set by EC, FD-71 or Guardian (FD-71a).

5.6.3.1 (U) Type 1 & 2 Assessments

(U) Type 1 & 2 Assessment defined: Seek information, proactively or in response to investigative leads, relating to activities – or the involvement or role of individuals, groups, or organizations in those activities – constituting violations of Federal criminal law or threats to the national security (i.e., the prompt checking of leads on individuals, activity, groups or organizations).

b7E

(U//FOUO) See Section 5.11 below for intelligence collection (i.e., incidental collection) and documentation requirements

5.6.3.1.1 (U) DURATION

(U//FOUO) There is no time limit for a Type 1 & 2 Assessment, but it is anticipated that such Assessments will be relatively short.

5.6.3.1.2 (U) DOCUMENTATION

(U//FOUO) FD-71 or Guardian. Guardian (FD-71a) The electronic FD-71, as discussed below,

b7E

(U//FOUO) FD-71 or Guardian (FD-71a) the FD-71 or Guardian, or by exception, in an EC. The completed FD-71 or Guardian requires supervisor approval before being uploaded.

b7E

(U//FOUO) FD-71 or Guardian consistent with the instructions in the FD-71 and Guardian

b7E

(U//FOUO)

b7E

5.6.3.1.3 (U) APPROVAL TO OPEN

(U//FOUO) An FBI employee may open a Type 1 & 2 Assessment without supervisor approval. an FD-71 or Guardian the FD-71 or Guardian The opening date for Type 1 & 2 Assessments is the date the SSA or SIA assigns an FBI employee to conduct the Assessment. The FBI employee and SSA or SIA must apply the standards for opening or approving a Type 1 & 2 Assessment contained in DIOG Section 5.5.

b7E

5.6.3.1.4 (U) SENSITIVE INVESTIGATIVE MATTERS (SIM)

(U//FOUO) As soon as practicable, but not more than five (5) business days after determining the Type 1 & 2 Assessment involves a sensitive investigative matter (SIM), the matter must be reviewed by the CDC and approved by the SAC. The term "sensitive investigative matter" is defined in DIOG Section 5.7 and DIOG Section 10. The FD-71 or Guardian [redacted] b7E

5.6.3.1.5 (U) NOTICE

(U//FOUO) There is no requirement to provide notice to FBIHQ or DOJ of opening or closing Type 1 & 2 Assessments.

5.6.3.1.6 (U) JUSTIFICATION REVIEW

(U//FOUO) If a Type 1 & 2 Assessment is not concluded within 30 days, the SSA or SIA must conduct a justification review every 30 days (recurring until the Assessment is closed) in accordance with DIOG Section 3.4.4.

5.6.3.1.7 (U) RESPONSIBLE ENTITY

(U//FOUO) A Type 1 & 2 Assessment may be conducted by an investigative field office squad or FBIHQ operational division.

5.6.3.1.8 (U) EXAMPLES/SCENARIOS OF TYPE 1 & 2 ASSESSMENTS

5.6.3.1.8.1 (U) EXAMPLE 1

(U//FOUO) [redacted] b7E

(U//FOUO) [redacted] b7E

(U//FOUO) The FBI employee can conduct record checks (search FBI/ DOJ records, USIC records, any other US government records, state or local records), and Internet searches [redacted] b7E (See Section 5.1.1) If an employee does not establish an authorized purpose to open an Assessment (or Predicated Investigation) after conducting these records checks or

Internet searches, the FBI employee should refer to Section 5.1.2 above for documenting these activities.

(U//FOUO)

b7E

and complete an FD-71.

5.6.3.1.8.2 (U) EXAMPLE 2

(U//FOUO)

b7E

(U//FOUO)

b7E

5.6.3.2 (U) TYPE 3 ASSESSMENTS

(U) Type 3 Assessment defined: Identify, obtain and utilize information about actual or potential national security threats or Federal criminal activities, or the vulnerability to such threats or activities. [See AGG-Dom, Part II.A.3.b]

(U//FOUO) Type 3 Assessments may be used to analyze or determine whether particular national security or criminal threats exist within the AOR and whether there are victims or targets within the AOR who are vulnerable to any such actual or potential threats. The

authorized purpose and clearly defined objective(s) of a Type 3 Assessment must be based on or related to actual or potential Federal criminal or national security targets, threats, or vulnerabilities. While no particular factual predication is required, the basis of the Assessment cannot be arbitrary or groundless speculation, nor can the Assessment be based solely on the exercise of First Amendment protected activities or on race, ethnicity, national origin or religion, or a combination of only such factors.

(U//FOUO) Whenever a Type 3 Assessment identifies and begins to focus on a specific individual(s), group(s) or organization(s), whose activities may constitute a violation of Federal criminal law or a threat to the national security, a separate Type 1 & 2 Assessment or a Predicated Investigation must be opened on that individual, group or organization.

(U//FOUO) A Type 3 Assessment may not be opened based solely upon the existence of a collection requirement, and addressing a collection requirement cannot be the authorized purpose of a Type 3 Assessment. Information obtained during the course of this type of assessment (or any other Assessment or Predicated Investigation) may, however, be responsive to collection requirements and collection requirements may be used to inform and help focus a Type 3 Assessment (or any other Assessment or Predicated Investigation) while also providing information about potential targets, threats and/or vulnerabilities.

(U//FOUO) Investigative activity undertaken during [redacted] must be documented using a Type 3 Assessment opened under the relevant investigative classification (e.g., [redacted] etc) or the [redacted] Opening a Type 3 Assessment for these events does not eliminate the requirement to use the [redacted] b7E

(U//FOUO) A Type 3 Assessment may not be used for the purpose of collecting positive foreign intelligence, although such intelligence may be incidentally collected. Positive foreign intelligence can only be intentionally collected pursuant to DIOG Sections 5.6.3.5 (Type 6 Assessment) and/or Section 9.

(U//FOUO) See Section 5.11 below for intelligence collection (i.e., incidental collection) and documentation requirements. [redacted] b7E

5.6.3.2.1 (U) DURATION

(U//FOUO) A Type 3 Assessment may only be opened with prior supervisor approval. The effective date of the Assessment is the date the final approval authority approves the EC as specified in Section 5.6.2 above. A Type 3 Assessment may continue for as long as necessary to achieve its authorized purpose and clearly defined objective(s). Although a Type 3 Assessment is not limited in duration, when the clearly defined objective(s) have been met, the Assessment must be closed with an EC approved by the supervisor.

5.6.3.2.2 (U) DOCUMENTATION

(U//FOUO)

b7E

(U//FOUO)

(U//FOUO)

b7E

5.6.3.2.3 (U) APPROVAL

(U//FOUO) All Type 3 Assessments must be approved in advance by a supervisor and opened by EC. Notwithstanding any other provision in the DIOG, a Type 3 Assessment cannot be opened based on oral approval. The supervisor must review and approve a Type 3 Assessment in accordance with the standards set forth in Section 5.5. Additional approval requirements apply to SIMs, as described below.

5.6.3.2.4 (U) SENSITIVE INVESTIGATIVE MATTERS (SIM)

(U//FOUO) If the Assessment involves a sensitive investigative matter, the CDC must review and the SAC must approve the Assessment prior to opening. If a SIM arises after the opening of a Type 3 Assessment, Assessment activity may continue, but the matter must be documented in an EC reviewed by the CDC and approved by the SAC as soon as practicable but not more than five (5) business days after the SIM arises. The term "sensitive investigative matter" is defined in DIOG Sections 5.7.1 and Section 10.

(U//FOUO) Investigative methods that may be used in Assessments are set forth in DIOG Section 18.

(U//FOUO) As specified in division PGs, there may be agreements (e.g., Memoranda of Understanding, Treaties) that require additional coordination and approval prior to conducting certain activities.

5.6.3.2.5 (U) NOTICE

(U//FOUO) There is no requirement to provide notice to FBIHQ or DOJ of opening or closing Type 3 Assessments.

5.6.3.2.6 (U) FILE REVIEW

(U//FOUO) A Type 3 Assessment requires file reviews in accordance with DIOG Section 3.4.4.

5.6.3.2.7 (U) RESPONSIBLE ENTITY

(U//FOUO) A Type 3 Assessment may be opened and conducted by FIGs, RIGs, the DI, field office investigative squads, and FBIHQ operational divisions. The nature of the Assessment dictates the file classification into which the Type 3 Assessment is opened. Assessments conducted by the DI, FIGs or RIGs must be opened in the appropriate [redacted] All other Assessments must be opened in the appropriate investigative file classification. b7E

5.6.3.2.8 (U) EXAMPLES OF TYPE 3 ASSESSMENTS

5.6.3.2.8.1 (U) EXAMPLE 1

(U/FOUO) [redacted] b7E

(U//FOUO) [redacted] b5 b7E

5.6.3.2.8.2 (U) EXAMPLE 2

(U/FOUO) [redacted] b7E

(U//FOUO)

b5
b7E

5.6.3.2.8.3 (U) EXAMPLE 3

(U/FOUO)

b7E

(U//FOUO)

b5
b7E

5.6.3.2.8.4 (U) EXAMPLE 4

(U/FOUO)

b7E

(U//FOUO)

b5
b7E

(U//FOUO)

b5
b7E

[redacted]

b5
b7E

5.6.3.2.8.5 (U) EXAMPLE 5

(U/FOUO) [redacted]

b7E

(U//FOUO) [redacted]

b5
b7E

5.6.3.3 (U) TYPE 4 ASSESSMENTS

(U) Type 4 Assessment defined: Obtain and retain information to inform or facilitate intelligence analysis and planning. [AGG-Dom, Part IV]

(U//FOUO) A Type 4 Assessment may be opened to obtain information that informs or facilitates the FBI's intelligence analysis and planning functions. The authorized purpose and clearly defined objective(s) of a Type 4 Assessment must be based on, or related to, the need to collect or acquire information for current or future intelligence analysis and planning purposes. An Assessment under this section, oftentimes referred to as a "domain Assessment," may lead to the identification of intelligence gaps, the development of FBI collection requirements, or the opening of new Assessments or Predicated Investigations.

(U//FOUO) A Type 4 Assessment is not threat specific; threat-based Assessments are opened and governed by DIOG Section 5.6.3.2 (Type 3 Assessment). While no particular factual predication is required for a Type 4 Assessment, the Assessment cannot be based solely on the exercise of First Amendment protected activities or on race, ethnicity, national origin or religion, or a combination of only such factors.

(U//FOUO) Whenever a Type 4 Assessment identifies and begins to focus on specific individual(s), group(s), or organization(s), whose activities may constitute a violation of Federal criminal law or a threat to the national security, a separate Type 1 & 2 Assessment or a Predicated Investigation must be opened. Similarly, if a Type 4 Assessment identifies a particular national security or criminal threat within the AOR, or identifies victims or targets within an AOR who are vulnerable to any actual or potential threat, a separate Type 3 Assessment or Predicated Investigation must be opened.

(U//FOUO) A Type 4 Assessment may not be used for the purpose of collecting positive foreign intelligence (PFI), although such intelligence may be incidentally collected. Positive

foreign intelligence can only be intentionally collected pursuant to DIOG Sections 5.6.3.5 (Type 6 Assessment) and/or Section 9.

(U//FOUO) See Section 5.11 below for intelligence collection, (i.e., incidental collection) and documentation requirements. [redacted] b7E

[redacted]

5.6.3.3.1 (U) DURATION

(U//FOUO) A Type 4 Assessment may only be opened with prior supervisor approval. The effective date of the Assessment is the date the final approval authority approves the EC as specified in Section 5.6.2 above. A Type 4 Assessment may continue for as long as necessary to achieve its authorized purpose and clearly defined objective(s). Although a Type 4 Assessment is not limited in duration, when the clearly defined objective(s) have been met, the Assessment must be closed with an EC approved by the supervisor.

5.6.3.3.2 (U) DOCUMENTATION

(U//FOUO) [redacted] b7E

[redacted]

(U//FOUO) [redacted]

[redacted]

(U//FOUO) This type of Assessment must be documented in the appropriate [redacted] b7E

[redacted]

5.6.3.3.3 (U) APPROVAL

(U//FOUO) All Type 4 Assessments must be approved in advance by a supervisor and opened by an EC. Notwithstanding any other provision in the DIOG, a Type 4 Assessment cannot be opened based on oral approval. The supervisor must approve a Type 4 Assessment in accordance with the standards discussed in DIOG Section 5.5. Additional approval requirements apply to SIMs, as described below.

5.6.3.3.4 (U) SENSITIVE INVESTIGATIVE MATTERS (SIM)

(U//FOUO) If the Assessment involves a sensitive investigative matter (SIM), the CDC must review and the SAC must approve the Assessment prior to opening. If a SIM arises after the opening of a Type 4 Assessment, Assessment activity may continue, but the matter must be

documented in an EC reviewed by the CDC and approved by the SAC as soon as practicable, but not more than five (5) business days after the SIM arises. The term "sensitive investigative matter" is defined in DIOG Section 5.7 and Section 10.

5.6.3.3.5 (U) NOTICE

(U//FOUO) There is no requirement to provide notice to FBIHQ or DOJ of opening or closing Type 4 Assessments.

5.6.3.3.6 (U) FILE REVIEW

(U//FOUO) A Type 4 Assessment requires file reviews in accordance with DIOG Section 3.4.4.

5.6.3.3.7 (U) RESPONSIBLE ENTITY

(U//FOUO) A Type 4 Assessment may only be opened by the DI, field office FIGs or Regional Intelligence Groups (RIG).

5.6.3.3.8 (U) EXAMPLES OF TYPE 4 ASSESSMENTS

5.6.3.3.8.1 (U) EXAMPLE 1

(U/FOUO)

b7E

(U//FOUO)

b5
b7E

5.6.3.3.8.2 (U) EXAMPLE 2

(U/FOUO)

b7E

(U//FOUO)

b5
b7E

5.6.3.3.8.3 (U) EXAMPLE 3

(U/FOUO)

b7E

(U//FOUO)

b5
b7E

5.6.3.3.8.4 (U) EXAMPLE 4

(U/FOUO)

b7E

(U//FOUO)

b5
b7E

5.6.3.4 (U) TYPE 5 ASSESSMENTS

(U) Type 5 Assessment defined: Seek information to identify potential human sources, assess their suitability, credibility, or value of individuals as human sources.

(U//FOUO) A Type 5 Assessment provides the authority and a mechanism to identify, evaluate and recruit a Potential Confidential Human Source (CHS) prior to opening and operating them as a CHS in A Type 5 Assessment is not a prerequisite to opening an individual as an operational CHS in if the necessary information for opening has been obtained through other methods (e.g., following arrest, an individual agrees to become as CHS).

b7E

(U//FOUO) A Type 5 Assessment may be opened:

A) (U//FOUO) on a specific named individual who is a potential CHS; or

B) (U//FOUO) without a specific named individual, if the goal is to identify individuals with placement and access to particular information.

(U//FOUO) A Type 5 Assessment may not be opened on a subject of a Predicated Investigation. A previously opened CHS cannot be opened as a Type 5 Assessment.

(U//FOUO) Type 5 Assessment activities may not be based solely on race, ethnicity, national origin, religion, or activities protected by the First Amendment, or a combination of only such factors.

(U//FOUO) There are three phases of a Type 5 Assessment. The phases are: (1) Identification Phase, (2) Evaluation Phase, and (3) Recruitment Phase. A Type 5 Assessment opened on a specific named individual may only use the Evaluation and Recruitment phases as described below. A Type 5 Assessment opened without a specific named individual is limited to the Identification Phase only. Once the Identification Phase has succeeded in identifying specific individuals who might have appropriate placement and access, the FBI employee must open a new separate Type 5 Assessment on any individual the employee wishes to further evaluate and possibly recruit as a CHS. The original Type 5 Assessment without a specific named individual may remain open in the Identification Phase, if the authorized purpose and clearly defined objective(s) still exist.

5.6.3.4.1 (U) PHASES OF TYPE 5 ASSESSMENTS

5.6.3.4.1.1 (U//FOUO) IDENTIFICATION PHASE

(U//FOUO) This phase may be used by an SA assigned to either a HUMINT or investigative squad or by an IA assigned to the field office or FBIHQ to identify potential CHSs who seem likely to have placement and access to information or intelligence related to criminal or national security threats, investigations, or collection requirements without naming a specific individual. The goal of this phase is to identify individuals with CHS potential, who may then be evaluated and recruited under the Evaluation and Recruitment Phases of a Type 5 Assessment.

(U//FOUO) This phase is initiated with the approval of a CHS identification plan. The plan, which must be based on a thorough review of available intelligence regarding the threat, investigation or collection requirement at issue, must specify characteristics of individuals likely to have CHS potential, and the investigative methods (e.g., database searches, surveillance of specific locations, attendance at specific events) that will be used to identify individuals with those characteristics. Selection of characteristics/search criteria must have a logical connection to intelligence or known facts, and may not be based merely on conjecture. In addition, selected characteristics may not be based solely on race, ethnicity, national origin, religion or activities protected under the First Amendment or a combination of only such factors. See DIOG Section 4 for further explanation on the permissible use of race, ethnic identity or activities protected under the First Amendment. The investigative methods that may be used to identify individuals

with the specified characteristics needed must also be based on existing intelligence and be reasonably likely to yield individuals with the specified characteristics.

(U//FOUO) If necessary, after a CHS identification plan has been approved, and a group of individuals who potentially have placement and access to the relevant information have been identified, the SA or IA may, with authorization set forth in Section 5.6.3.4.8, use additional characteristics to narrow the group of individuals to those most likely to have the desired placement and access.

(U//FOUO) Once an SA or IA has narrowed the field to one or more known persons who appear to have potential as CHSs, in order to gather additional information regarding background and authenticity or, in order for an SA to undertake efforts to recruit the individual, a Type 5 Assessment must be opened on the specific named individual(s) in accordance with subsection 5.6.3.4.1.2, below.

5.6.3.4.1.2 (U//FOUO) EVALUATION PHASE

(U//FOUO) This phase may be used by an SA assigned to either a HUMINT or investigative squad or by an IA assigned to the field office or FBIHQ to evaluate a known individual believed to have placement and access so that the individual, if successfully recruited, can provide the FBI with information of value. The goal of this phase of a Type 5 Assessment is to gather information, through the use of the investigative methods set forth in Section 8, below regarding background, authenticity, and suitability of a particular Potential CHS (specific named individual). An IA who develops information during this phase that indicates a Potential CHS is worthy of recruitment should prepare a [redacted] for use by an SA on the appropriate HUMINT or investigative squad to recruit the individual. If information developed during this phase indicates the individual should not be recruited as a CHS, the Type 5 Assessment must be closed. b7E

5.6.3.4.1.3 (U//FOUO) RECRUITMENT PHASE

(U//FOUO) This phase may only be used by an SA assigned to a HUMINT or investigative squad. The goal of this phase of a Type 5 Assessment is to recruit the potential CHS to become an operational CHS, and therefore, the recruitment phase may focus only on a specific named individual. Information from [redacted] or other information/intelligence available to the SA may be used during the recruitment phase. If the recruitment is successful, the Type 5 Assessment must be closed (See Section 5.6.3.4.9, below) and the individual opened as a CHS in [redacted] The Type 5 Assessment must also be closed if the recruitment is not successful, either because the individual declines to become a CHS or a determination is made not to continue the recruitment. b7E

5.6.3.4.2 (U) DURATION

(U//FOUO) The effective date of a Type 5 Assessment is the date the highest level of authority required approves the opening EC (or [redacted] A Type 5 Assessment may continue for as long as necessary to achieve its authorized purpose and b7E

clearly defined objective(s) as set forth in the three phases above or when it is determined that the individual named subject cannot or should not be recruited as a CHS.

5.6.3.4.3 (U) DOCUMENTATION

5.6.3.4.3.1 (U//FOUO) IDENTIFICATION PHASE

(U//FOUO) [redacted] b7E

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

(U//FOUO) [redacted] b7E

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

(U//FOUO) [redacted] b7E

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

(U//FOUO) [redacted] b7E

[redacted] b7E

(U//FOUO) If a Type 5 Assessment has already been opened and an IA or SA wishes to utilize additional characteristics/search criteria or investigative methods in the Identification Phase that were not documented in the opening EC, the additional characteristics/search criteria and/or investigative methods must be documented by EC

[redacted] b7E

5.6.3.4.3.2 (U//FOUO) EVALUATION/RECRUITMENT PHASES

(U//FOUO) A Type 5 Assessment opened to evaluate and/or recruit a specific person as a CHS must be opened with an EC (or [redacted] using the appropriate

[redacted] b7E

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

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

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

5.6.3.4.4 (U) APPROVAL

(U//FOUO) A Type 5 Assessment must be approved by the appropriate supervisor and opened with an EC (or [redacted]. Notwithstanding any other provision in the DIOG, a Type 5 Assessment cannot be opened on oral approval. For SAs, a Type 5 Assessment must be approved by their SSA. For IAs, a Type 5 Assessment must be approved by the SIA and the SSA on the HUMINT or investigative squad that will potentially recruit the individual. An SSA and/or SIA must use the standards provided in DIOG Section 5.5 when deciding whether to approve a Type 5 Assessment. Additional approval requirements apply to Sensitive Potential CHSs, as described below. b7E

5.6.3.4.4.1 (U//FOUO) SENSITIVE POTENTIAL CHSs AND GROUPS

(U//FOUO) CDC review and SAC approval is required before a Type 5 Assessment may be opened on a Sensitive Potential CHS or if, during the Identification Phase, a sensitive characteristic is at least one aspect being used to identify individuals with potential placement and access to information of interest. If it is determined after opening a Type 5 Assessment that a Potential CHS is Sensitive or that a sensitive characteristic must be added to the Potential CHS Identification Plan, the Assessment activity may continue, but the matter must be documented in an EC (or [redacted] and reviewed by the CDC and approved by the SAC as soon as practicable, but not more than 5 business days of this determination. A Sensitive Potential CHS or sensitive characteristic (as part of an Identification Plan) is defined as follows: b7E

A) (U//FOUO) A domestic public official (other than a member of the U.S. Congress or White House Staff – which requires higher approval authority, see [redacted] for additional details); b7E

B) (U//FOUO) A domestic political candidate;

C) (U//FOUO) An individual prominent within a religious organization;

D) (U//FOUO) An individual prominent within a domestic political organization;

E) (U//FOUO) A member of the news media; or

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

(U//FOUO) DIOG Section 10 should be consulted for a definition of these terms.

(U//FOUO) For additional information regarding Sensitive Potential CHSs, see [redacted] b7E Part 2, & DIOG Section 18.5.3.

5.6.3.4.5 (U) NOTICE

(U//FOUO) There is no requirement to provide notice to FBIHQ or DOJ of opening or closing Type 5 Assessments.

5.6.3.4.6 (U) FILE REVIEW

(U//FOUO) A supervisory file review must be conducted every 90 days (60 days for probationary employees). In addition to the requirements of section 3.4.4.9, the purpose of the file review is to determine the following:

A) (U//FOUO) Whether authorized investigative methods have been used properly in all phases of the Assessment;

B) (U//FOUO) Whether, in the Identification Phase, the Assessment has successfully narrowed the field to a group of individuals who are likely to have appropriate placement and access;

C) (U//FOUO) Whether reimbursable expenses incurred by an SA, if any, were reasonable, properly authorized, and properly documented;

D) (U//FOUO) Whether the Potential CHS was tasked to provide information or paid for his/her services or expenses (activities which are not permitted prior to opening the person as a CHS);

E) (U//FOUO) Whether there is a reasonable likelihood the Potential CHS can and should be recruited or, if the Assessment is in the Identification Phase, the plan has a reasonable likelihood of generating a group of Potential CHSs; and

F) (U//FOUO) Whether the Type 5 Assessment should continue for an additional 90 days (60 days for probationary employees). If continuation is justified, SIA/SSA must document the rationale for keeping the Type 5 Assessment open.

5.6.3.4.7 (U) RESPONSIBLE ENTITY

(U//FOUO) A Type 5 Assessment without a specific named individual may be opened by SAs on HUMINT squads or IAs assigned the field office FIG or to FBIHQ. A Type 5 Assessment on specific named individual may be opened by SAs on HUMINT or investigative squads, and by IAs assigned to the field office FIG, investigative squads, or to FBIHQ.

5.6.3.4.8 (U) AUTHORIZED INVESTIGATIVE METHODS IN TYPE 5 ASSESSMENTS

(U//FOUO) Only the following investigative methods may be used in a Type 5 Assessment, whether in the identification, evaluation, or recruitment phase. All of these investigative methods may be used by SAs. IA's may only use investigative methods (A) through (E).

A) (U//FOUO) Public information;

B) (U//FOUO) Records or information – FBI and DOJ;

C) (U//FOUO) Records or information – Other Federal, state, local, tribal, or foreign government agencies;

D) (U//FOUO) On-line services and resources;

E) (U//FOUO) Information voluntarily provided by governmental or private entities; b7E

F) (U//FOUO) Use of AFID – with certain approvals required (see [redacted]

G) (U//FOUO) CHS use and recruitment;

H) (U//FOUO) Interview or request information from the public or private entities;

I) (U//FOUO) Physical surveillance (not requiring a court order); b7E

J) (U//FOUO) Polygraph examinations (see [redacted] and

K) (U//FOUO) Trash Covers (Searches that do not require a warrant or court order).

(U//FOUO) ***Note:*** Consent Searches are authorized in Assessments.[5]

(U//FOUO) Some investigative methods used during Assessments that may require higher supervisory approval are set forth in DIOG Section 18.5.

(U//FOUO) In addition, as specified in division PGs, there may be agreements (e.g., Memoranda of Understanding, etc.) that require additional coordination and approval prior to conducting certain activities.

[5] (U//FOUO) The DOJ has opined that Consent Searches are authorized in Assessments, as well as in Predicated Investigations.

(U//FOUO [redacted] b7E

5.6.3.4.9 (U) CLOSING TYPE 5 ASSESSMENTS

(U//FOUO) A Type 5 Assessment must be closed with SIA and SSA approval if it was opened by an IA; or with SSA approval if it was opened by an SA, when:

A) (U//FOUO) In a Type 5 Assessment opened without a specific named individual, it is determined that the characteristics/search criteria used to identify individuals with placement and access to needed information have not succeeded in identifying such individuals, or the FBI no longer has a need for a CHS with the specified placement and access;

B) (U//FOUO) The Identification Phase has succeeded in identifying specific named individuals who might have appropriate placement and access. If the FBI wishes to further evaluate and possibly recruit any such identified individuals, a separate Type 5 Assessment must be opened on that person. The original Type 5 Assessment may remain open in the identification phase if the authorized purpose and clearly defined objective still exist;

C) (U//FOUO) In a Type 5 Assessment opened on a specific named individual, it is determined that the Potential CHS is not a suitable candidate for further evaluation and/or recruitment efforts;

D) (U//FOUO) In a Type 5 Assessment opened on a specific named individual, SA recruitment efforts are successful and the potential CHS has been opened as a CHS in [redacted] or b7E

E) (U//FOUO) In a Type 5 Assessment opened on a specific named individual, SA efforts to recruit the potential CHS have been unsuccessful or it is determined that further recruitment efforts are not likely to be successful.

5.6.3.4.10 (U) EXAMPLES OF TYPE 5 ASSESSMENTS

5.6.3.4.10.1 (U//FOUO) EXAMPLES OF A TYPE 5 ASSESSMENT OPENED WITHOUT A SPECIFIC NAMED INDIVIDUAL

(U//FOUO) [redacted] b7E

(U//FOUO) [redacted] b5 b7E

b5
b7E

(U//FOUO)

b7E

(U//FOUO)

b5
b7E

5.6.3.4.10.2 (U//FOUO) EXAMPLES OF TYPE 5 ASSESSMENTS OPENED ON SPECIFIC NAMED POTENTIAL CHSS

(U/FOUO)

b7E

(U//FOUO)

b5
b7E

b5
b7E

(U/FOUO)

b7E

(U//FOUO)

b5
b7E

(U//FOUO) *If the Assessment is opened by an SA:* The SA may open a Type 5 Assessment with his/her SSA approval. If the recruitment is successful, the Type 5 Assessment must be closed when the CHS is opened in If the recruitment is unsuccessful, the Type 5 Assessment must be closed. b7E

(U//FOUO) *If the Assessment is opened by an IA:* The IA must obtain the approval of his/her SIA and the supervisor of the relevant investigative or HUMINT squad to open a Type 5 Assessment. (Note: An IA may not open an individual as a CHS in) If the Assessment determines the person has placement and access to information or intelligence that would be of value, the Type 5 Assessment must be transferred to the appropriate investigative squad or the HUMINT squad to further evaluate and recruit the potential CHS. b7E

5.6.3.5 (U) Type 6 Assessments

(U) Type 6 Assessment defined: Seek information, proactively or in response to investigative leads, relating to matters of foreign intelligence interest responsive to foreign intelligence requirements.

(U//FOUO) A Type 6 Assessment is designed to allow the FBI to determine whether the circumstances within a field office's territory would enable the office to conduct a Full Investigation to collect information responsive to a Positive Foreign Intelligence (PFI) requirement. PFI requirements are described in DIOG Section 9.1. A Type 6 Assessment

focuses on a field office's capability to collect on those PFI requirements. While no particular factual predication is required, the basis of the Assessment cannot be arbitrary or groundless speculation, nor can the Assessment be based solely on the exercise of First Amendment protected activities or on race, ethnicity, national origin or religion, or a combination of only those factors.

(U//FOUO) Foreign Intelligence is "information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, or foreign persons." The FBI defines a PFI requirement as a collection requirement issued by the USIC and is accepted by the FBI DI that seeks to collect information outside the FBI's core national security mission.

(U//FOUO) FBI employees must prioritize collection in response to FBI national collection requirements before attempting to collect against a positive foreign intelligence collection requirement. The IPG furnishes guidance on the prioritization of collection.

(U//FOUO) See Section 5.11 below for intelligence collection, (i.e., incidental collection) and documentation requirements. [redacted] b7E

5.6.3.5.1 (U) DURATION

(U//FOUO) There are no time limitations on the duration of a Type 6 Assessment. The effective date of the Assessment is the date on which the DI – Domain Collection and HUMINT Management Section (DCHMS), Domain Collection Program Management Unit (DCPMU), UC approves the EC. See DIOG section 5.6.2 above. A Type 6 Assessment may continue for as long as necessary to achieve its authorized purpose and clearly defined objective(s). Although a Type 6 Assessment is not limited in duration, when the authorized purpose and clearly defined objective(s) have been met, the Assessment must be closed or converted to a Full Investigation with an EC approved by the field office SSA or SIA and the DCPMU UC. When closing a Type 6 Assessment that is designated as a SIM, the SAC and the DCHMS SC must approve the closing EC.

5.6.3.5.2 (U) DOCUMENTATION

(U//FOUO) A Type 6 Assessment must be opened by EC, using the appropriate [redacted] The title/caption of the opening EC must contain the word "Assessment," and the synopsis must identify the authorized purpose and the clearly defined objective(s) of the Assessment. The authorized purpose and clearly defined objective(s) should be described in more detail in the Details section of the EC. If additional objectives arise during the course of the Assessment, they must also be documented in an EC and approved by the field office SSA or SIA [redacted] b7E

(U//FOUO) [redacted] b7E

5.6.3.5.3 (U) APPROVAL

(U//FOUO) All Type 6 Assessments must be opened by EC and approved in advance by an SSA or SIA and the appropriate DI UC. A Type 6 Assessment must be approved in accordance with the standards provided in DIOG Section 5.5. Notwithstanding any other provision in the DIOG, a Type 6 Assessment cannot be opened on oral approval.

5.6.3.5.4 (U) SENSITIVE INVESTIGATIVE MATTERS (SIM)

(U//FOUO) If a Type 6 Assessment involves a sensitive investigative matter, the CDC/OGC must review and the SAC and the appropriate DI SC must approve the Assessment prior to opening. If a sensitive investigative matter arises after the opening of a Type 6 Assessment, Assessment activity may continue, but the matter must be reviewed by the CDC and approved by the SAC and the DCHMS SC, as soon as practicable, but not more than five (5) business days after the sensitive investigative matter arises. The term "sensitive investigative matter" is defined in DIOG Section 5.7 and Section 10.

5.6.3.5.5 (U) NOTICE

(U//FOUO) FBIHQ authority, as specified above, is required to open a Type 6 Assessment; the opening EC will serve as notice to the DI. There is no requirement to provide notice to DOJ of opening or closing a Type 6 Assessment.

5.6.3.5.6 (U) FILE REVIEW

(U//FOUO) A Type 6 Assessment requires file reviews in accordance with DIOG Section 3.4.4.

5.6.3.5.7 (U) RESPONSIBLE ENTITY

(U//FOUO) A Type 6 Assessment may only be opened and conducted by the FIG and the DI (Refer to IPG for further details). Under the management of the FIG, field office investigative squads or FBIHQ divisions may support the collection of information in a Type 6 Assessment.

5.6.3.5.8 (U) EXAMPLES/SCENARIOS OF TYPE 6 ASSESSMENTS

5.6.3.5.8.1 (U) EXAMPLE 1

(U/FOUO) *Example 1:*

b7E

(U//FOUO)

b5
b7E

5.6.3.5.8.2 (U) EXAMPLE 2

(U//FOUO) *Example 2:*

b7E

(U//FOUO)

b5
b7E

5.7 (U) SENSITIVE INVESTIGATIVE MATTERS (SIM) IN ASSESSMENTS

(U//FOUO)

b7E

DIOG Section 10 contains the required approval authority and factors for consideration when determining whether to open or approve an Assessment involving a SIM.

5.7.1 (U) SIM CATEGORIES IN ASSESSMENTS

(U//FOUO) A SIM is an investigative matter involving the activities of a domestic public official or domestic political candidate (involving corruption or a threat to the national security), religious or domestic political organization or individual prominent in such an organization, or news media, an academic nexus, or any other matter which, in the judgment of the official authorizing an Assessment, should be brought to the attention of FBIHQ and other DOJ officials. (AGG-Dom, Part VII.N.) As a matter of FBI policy, "judgment" means that the decision of the authorizing official is discretionary

b7E

(U//FOUO) [redacted] b7E

5.7.2 (U) ACADEMIC NEXUS IN ASSESSMENTS

(U//FOUO) [redacted] b7E

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

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

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

(U//FOUO) [redacted] see the classified provisions in DIOG Appendix G. b7E

5.8 (U) STANDARDS FOR OPENING OR APPROVING THE USE OF AN AUTHORIZED INVESTIGATIVE METHOD

(U//FOUO) Prior to opening or approving the use of an authorized investigative method, an FBI employee or approving official must determine whether:

A) (U//FOUO) The use of the particular investigative method is likely to further the authorized purpose and clearly defined objective(s) of the Assessment;

B) (U//FOUO) The investigative method selected is the least intrusive method reasonable based upon the circumstances of the investigation;

C) (U//FOUO) The anticipated value of the Assessment justifies the use of the selected investigative method or methods;

D) (U//FOUO) If the purpose of the Assessment is to collect positive foreign intelligence, the investigative method complies with the AGG-Dom requirement that the FBI operate openly and consensually with an USPER, to the extent practicable; and

E) (U//FOUO) The investigative method is an appropriate use of personnel and financial resources.

5.9 (U) AUTHORIZED INVESTIGATIVE METHODS IN ASSESSMENTS

5.9.1 (U) TYPE 1 THROUGH 4 AND TYPE 6 ASSESSMENTS

(U//FOUO) A complete discussion of these investigative methods, including approval requirements, is contained in DIOG Section 18. The use or dissemination of information obtained by the use of the below-methods must comply with the AGG-Dom and DIOG Section 14. Only the following investigative methods are authorized in Type 1 through 4 and Type 6 Assessments:

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

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

C) (U) Records or information - Other federal, state, local, tribal, or foreign government agency. (Section 18.5.3)

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

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

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

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

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

I) (U) Grand jury subpoenas – for telephone or electronic mail subscriber information only (**only available in a Type 1 & 2 Assessment**). (Section 18.5.9)

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

5.9.2 (U) TYPE 5 ASSESSMENTS

(U//FOUO) In addition to those investigative methods listed above in 5.9.1(A) – (H), Type 5 Assessments only may also use the following investigative methods: b7E

A) (U) Use of AFID – with certain approvals required. (See [redacted] b7E

B) (U) Polygraph Examinations (See [redacted]

C) (U) Trash Covers (Searches that do not require a warrant or court order). (See Section 18.6.12)

5.10 (U) OTHER INVESTIGATIVE METHODS NOT AUTHORIZED DURING ASSESSMENTS

(U//FOUO) Additional investigative methods, which are authorized for Predicated Investigations, may not be used in Assessments.

5.11 (U) INTELLIGENCE COLLECTION (I.E., INCIDENTAL COLLECTION)

(U//FOUO) [redacted] b7E

(See DIOG Section 15.6.1.2 - Written Intelligence Products) b7E

(U//FOUO)

5.12 (U) RETENTION AND DISSEMINATION OF PRIVACY ACT RECORDS

(U//FOUO) The Privacy Act restricts the maintenance of records relating to the exercise of First Amendment rights by individuals who are USPERs. Such records may be maintained if the information is pertinent to and within the scope of authorized law enforcement activities or for which there is otherwise statutory authority for the purposes of the Privacy Act (5 U.S.C. § 522a[e][7]). Activities authorized by the AGG-Dom are authorized law enforcement activities. Thus, information concerning the exercise of First Amendment rights by USPERs may be retained if it is pertinent to or relevant to the FBI's law enforcement or national security activity. Relevancy must be determined by the circumstances. If the information is not relevant to the law enforcement activity being conducted, then it may not be retained. For more information see DIOG Section 4.1. (AGG-Dom, Part I.C.5)

(U) The Privacy Act, however, may not exempt from disclosure information gathered by the FBI during Positive Foreign Intelligence Assessments (Type 6 Assessments) and investigations of qualified U.S. citizens or lawfully admitted permanent residents if personally identifying information about such persons resides in those files. FBI employees should therefore be particularly vigilant about properly classifying any such information and should avoid unnecessary references to, and the documentation of, identifying information about U.S. citizens and lawfully admitted permanent residents in Positive Foreign Intelligence files. See DIOG Section 4.1.3.

(U//FOUO) Even if information obtained during an Assessment does not warrant opening a Predicated Investigation, the FBI may retain personally identifying information for criminal and national security purposes. In this context, the information may eventually serve a variety of valid analytic purposes as pieces of the overall criminal or intelligence picture are developed to detect and disrupt criminal and terrorist activities. In addition, such information may assist FBI personnel in responding to questions that may subsequently arise as to the nature and extent of the Assessment and its results, whether positive or negative. Furthermore, retention of such information about an individual collected in the course of an Assessment will alert other divisions or field offices considering conducting an Assessment on the same individual that the particular individual is not a criminal or national security threat. As such, retaining personally identifying information collected in the course of an Assessment will also serve to conserve resources and prevent the initiation of unnecessary Assessments and other investigative activities.

5.12.1 (U) *MARKING CLOSED ASSESSMENTS THAT CONTAIN PERSONAL INFORMATION*

(U) Information obtained during an Assessment that has insufficient value to justify further investigative activity may contain personal information. As a result: (i) when records retained in an Assessment specifically identify an individual or group whose possible involvement in criminal or national security-threatening activity was checked out through the Assessment; and (ii) the Assessment turns up no sufficient basis to justify further investigation of the individual or group, then the records must be clearly annotated as follows:

> (U) **"It is noted that the individual or group identified during the Assessment does not warrant further FBI investigation at this time. Any dissemination of information from this Assessment regarding the individual or group identified must include an appropriate caveat with the shared information. It is recommended that this Assessment be closed."**

(U) Extreme care should be taken when disseminating personally identifiable information collected during an Assessment that does not lead to sufficient facts to open a Predicated Investigation. If personal information from the Assessment is disseminated outside the FBI according to authorized dissemination guidelines and procedures, it must be accompanied by the required annotation that the Assessment involving this individual or group did not warrant further investigation by the FBI at the time the Assessment was closed.

5.12.1.1 (U) TYPE 1& 2 ASSESSMENTS

(U//FOUO) [redacted] FD-71 or Guardian [redacted] b7E

5.12.1.2 (U) TYPE 3, 4, AND 6 ASSESSMENTS

(U//FOUO) [redacted] b7E
Moreover, any FBI employee who shares information from such a closed Assessment file must ensure the following caveat is included in the dissemination:

> (U) **"This person [or group] was identified during an Assessment but no information was developed at that time that warranted further investigation of the person [or group]."**

5.12.1.3 (U) TYPE 5 ASSESSMENTS

(U//FOUO) [redacted] b7E
Moreover, any FBI employee who shares information from such a closed Assessment file must ensure the following caveat is included in the dissemination:

> (U) **"This person [or group] was identified during an Assessment to identify potential human sources but the person [or group] did not warrant further development as a source at that time."**

5.13 (U) ASSESSMENT FILE RECORDS MANAGEMENT AND RETENTION

(U//FOUO) [redacted] b7E

[redacted] FD-71 or Guardian [redacted] [redacted] Records must be retained according to National Archives and Records Administration (NARA) approved disposition authorities.

(U//FOUO) Guardian [redacted] b7E

[redacted] Guardian [redacted] records in Guardian, or any successor information technology system, must be retained according to NARA-approved disposition authorities. Consult the RMD Help Desk for assistance.

(U//FOUO) Type 3, 4, 5, and 6 Assessments must have [redacted] b7E

[redacted] must be approved by the SSA or SIA [redacted] If additional objectives arise during the Assessment, they must be [redacted] approved by the SSA or SIA, and [redacted] Assessment classification files must be retained according to NARA-approved disposition authorities.

5.14 (U) OTHER PROGRAM SPECIFIC INVESTIGATION REQUIREMENTS

(U//FOUO) To facilitate compliance within an existing investigative program, the FBI employee should consult the relevant division's PG. FBIHQ division PGs, however, may not contradict, alter or otherwise modify the standards established in the DIOG.

This Page is Intentionally Blank.

6 (U) PRELIMINARY INVESTIGATIONS

6.1 (U) OVERVIEW

(U) The AGG-Dom authorizes a second level of investigative activity—Predicated Investigations. Predicated Investigations that concern federal crimes or threats to the national security are subdivided into Preliminary Investigations (PI) and Full Investigations (Full). A Preliminary Investigation may be opened on the basis of any "allegation or information" indicative of possible criminal activity or threats to the national security.

6.2 (U) PURPOSE AND SCOPE

(U//FOUO) A Preliminary Investigation may be opened to detect, obtain information about, or prevent or protect against federal crimes or threats to the national security. However, a Preliminary Investigation cannot be opened or used solely for the purpose of collecting against Positive Foreign Intelligence (PFI) requirements, or for conducting an Enterprise Investigation (EI).

(U) The purposes for conducting Preliminary Investigation include such matters as: determining whether a federal crime has occurred or is occurring, or if planning or preparation for such a crime is taking place; identifying, locating, and apprehending the perpetrators; obtaining evidence needed for prosecution; or identifying threats to the national security.

(U) The investigation of threats to the national security may constitute an exercise of the FBI's criminal investigation authority as well as its authority to investigate threats to the national security. As with criminal investigations, detecting and solving crimes and arresting and prosecuting the perpetrators are likely objectives of investigations relating to threats to the national security. These investigations, however, serve important purposes outside the ambit of normal criminal investigations, by providing the basis for decisions concerning other measures needed to protect the national security.

6.3 (U) CIVIL LIBERTIES AND PRIVACY

(U) The pursuit of legitimate investigative goals without infringing upon the exercise of constitutional freedoms is a challenge that the FBI meets through the application of sound judgment and discretion. In order to protect civil liberties in the conduct of criminal and national security investigations, every Preliminary Investigation under this subsection must have adequate predication that is documented in the opening communication.

(U) No investigative activity, including Preliminary Investigations, may be taken solely on the basis of activities that are protected by the First Amendment or on the race, ethnicity, national origin or religion of the subject, or a combination of only those factors. Preliminary Investigations of individuals, groups or organizations must focus on activities related to the threats and or crimes being investigated, not solely on First Amendment activities or on the race, ethnicity, national origin or religion of the subject. In this context, it is particularly important

clearly to identify and document the law enforcement or national security basis of the Preliminary Investigation.

(U) *Example*: Individuals or groups who communicate with each other or with members of the public in any form in pursuit of social or political causes—such as opposing war or foreign policy, protesting government actions, promoting certain religious beliefs, championing particular local, national, or international causes, or a change in government through non-criminal means, and actively recruit others to join their causes—have a fundamental constitutional right to do so. A Preliminary Investigation may not be opened based solely on the exercise of these First Amendment rights.

(U) The AGG-Dom present investigators with a number of authorized investigative methods in the conduct of a Preliminary Investigation. Considering the effect on the privacy and civil liberties of individuals and the potential to damage the reputation of individuals, some of these investigative methods are more intrusive than others. The least intrusive method if reasonable based upon the circumstances of the investigation is to be used, but the FBI must not hesitate to use any lawful method consistent with the AGG-Dom. A more intrusive method may be warranted in light of the seriousness of a criminal or national security threat.

(U) By emphasizing the use of the least intrusive means to obtain intelligence, information, and/or evidence, FBI employees can effectively execute their duties while mitigating the potential negative impact on the privacy and civil liberties of all people encompassed within the investigation, including targets, witnesses, and victims. This principle is not intended to discourage FBI employees from seeking relevant and necessary intelligence, information, or evidence, but rather is intended to encourage FBI employees to choose the least intrusive—but still reasonable based upon the circumstances of the investigation — means from the available options to obtain the intelligence, information or evidence. (See DIOG Section 4.4).

6.4 (U) LEGAL AUTHORITY

6.4.1 (U) CRIMINAL INVESTIGATIONS

(U) The FBI has statutory authority to investigate all federal crime not assigned exclusively to another federal agency. (See 28 U.S.C. § 533; 18 U.S.C. § 3052; 28 C.F.R. § 0.85 [a])

(U) The FBI also has special investigative jurisdiction to investigate violations of state law in limited circumstances. Specifically, the FBI has jurisdiction to investigate felony killings of state law enforcement officers (28 U.S.C. § 540), violent crimes against interstate travelers (28 U.S.C. § 540A), and serial killers (28 U.S.C. § 540B). Authority to investigate these matters is contingent on receiving a request by an appropriate state official.

6.4.2 (U) THREATS TO THE NATIONAL SECURITY

(U) The FBI has authority to investigate threats to the national security pursuant to executive orders, Attorney General authorities, and various statutory sources. (See Appendix B: Executive Order (EO) 12333; 50 U.S.C. §§ 401 et seq.; 50 U.S.C. §§ 1801 et seq.)

(U) "Threats to the national security" are specifically defined to mean: international terrorism; espionage and other intelligence activities, sabotage, and assassination, conducted by, for, or on behalf of foreign powers, organizations, or persons; foreign computer intrusion; and other matters determined by the Attorney General, consistent with EO 12333 or any successor order. (AGG-Dom, Part VII.S)

6.5 (U) PREDICATION

(U) A Preliminary Investigation may be opened on the basis of "information or an allegation" indicating the existence of a circumstance described as follows:

A) (U) An activity constituting a federal crime or a threat to the national security has or may have occurred, is or may be occurring, or will or may occur and the investigation may obtain information or intelligence relating to the activity or the involvement or role of an individual, group, or organization in such activity. (AGG-Dom, Part II.B.3)

B) (U) An individual, group, organization, entity, information, property, or activity is or may be a target of attack, victimization, acquisition, infiltration, or recruitment in connection with criminal activity in violation of federal law or a threat to the national security and the investigation may obtain information or intelligence that would help to protect against such activity or threat. (AGG-Dom, Part II.B.3)

(U//FOUO) *Examples*: The following examples have sufficient predication to open a Preliminary Investigation:

A) (U//FOUO) A CHS, with no established history, alleges that an individual is a member of a terrorist group; this "allegation" is sufficient predication to open a Preliminary Investigation; and

B) (U//FOUO) If an analyst, while conducting an assessment, discovers on a blog a threat to a specific person, this "information" is enough to open a Preliminary Investigation.

6.6 (U) STANDARDS FOR OPENING OR APPROVING A PRELIMINARY INVESTIGATION

(U) Before opening or approving the conduct of a Preliminary Investigation, an FBI employee or approving official must determine whether:

A) (U//FOUO) Adequate predication exist for opening a Preliminary Investigation;

B) (U//FOUO) The Preliminary Investigation is not based solely on the exercise of First Amendment activities or on the race, ethnicity, national origin or religion of the subject or a combination of only such factors; and

C) (U//FOUO) The Preliminary Investigation is an appropriate use of personnel and financial resources.

(U//FOUO) Additional policies regarding Preliminary Investigations involving any foreign ambassador, foreign official, foreign student or exchange visitor, protected persons or premises as subjects may be found in to DIOG Appendix G – Classified Provisions [No Foreign Policy Objection].

(U//FOUO) A Preliminary Investigation cannot be opened based solely on an FBI collection requirement.

6.7 (U) Opening Documentation, Approval, Effective Date, Notice, Extension, Pending Inactive Status, Conversion, and File Review

6.7.1 (U) Opening Documentation

(U//FOUO) The predication to open a Preliminary Investigation must be documented in the opening Electronic Communication (EC). The appropriate approving authority may grant oral authority to open a Preliminary Investigation if the standards for opening or approving a Preliminary Investigation are met. Should oral authorization to conduct a Preliminary Investigation be granted, an EC setting forth the predicating facts, as well as the identity of the authorizing supervisor and date of oral authorization, must be documented to the supervisor who granted the oral authorization, as soon as practicable, but not more than five (5) business days after granting oral authorization.

(U//FOUO) [redacted] b7E

(U//FOUO) The DIOG prohibits the use of control files or administrative files to document investigative activity. (See DIOG Appendix J)

6.7.1.1 (U) Approval / Effective Date / Notice

(U//FOUO) The effective date of the Preliminary Investigation is the date the final approval authority (e.g., Supervisory Special Agent (SSA) or Special Agent-in-Charge (SAC)) approves the EC [redacted] b7E If the Preliminary Investigation is opened on oral authority, the date on which the oral authority was granted is the effective date. See DIOG Section 3.4.2.2. Adding another subject after opening the Preliminary Investigation does not change the original effective date or the extension date.

A) (U//FOUO) ***Opened By a Field Office:*** The opening of a Preliminary Investigation by the field office requires prior approval of the SSA. [redacted] b7E

B) (U//FOUO) ***Opened By FBIHQ:*** The opening of a Preliminary Investigation by FBIHQ requires prior approval of the Unit Chief (UC) [redacted]

C) (U//FOUO) ***Sensitive Investigative Matters (SIM):*** The opening of a Preliminary Investigation involving a SIM:

1) (U//FOUO) ***SIM Opened by a Field Office:*** requires prior Chief Division Counsel (CDC) review and SAC approval, and written notification (EC and a disseminable Letterhead Memorandum (LHM)), to the appropriate FBIHQ operational UC and Section Chief (SC)

within 15 calendar days following the opening. Additionally, the field office must notify the United States Attorney's Office (USAO), in writing, unless such notification is inappropriate under the circumstances (e.g., a public corruption investigation of a person who is personally close to the United States Attorney (USA)) or the matter is a counterintelligence or espionage investigation. (See CD PG for details concerning notice in counterintelligence and espionage investigations.) If notice is not provided to the USAO under the exceptions described above, the field office must explain those circumstances in the written notice to FBIHQ. The responsible FBIHQ section must notify, in writing, the appropriate DOJ Criminal Division or NSD official as soon as practicable, but no later than 30 calendar days after the investigation is opened. The notice must identify all known SIMs involved in the investigation (see DIOG Appendix G - Classified Provisions for additional notice requirements). If a SIM arises after the opening of a Preliminary Investigation, investigative activity may continue, but the matter must be reviewed by the CDC and approved by the SAC as soon as practicable, but not more than five (5) business days thereafter to continue the investigation. Notice must be provided as specified above.

2) (U//FOUO) ***SIM Opened by FBIHQ:*** requires prior OGC review and SC approval, and written notification (an EC and disseminable LHM) to any appropriate field office within 15 calendar days following the opening; the USAO, unless such notification is inappropriate under the circumstances, (e.g., a public corruption investigation of a person who is personally close to the USA) or the matter is a counterintelligence or espionage investigation; and the appropriate DOJ Criminal Division or NSD official, as soon as practicable, but no later than 30 calendar days after the investigation is opened. (See CD PG for details concerning notice in counterintelligence and espionage investigations.) If notice is not provided to the USAO under the circumstances described above, FBIHQ must explain those circumstances in the written notice to the field office(s) and DOJ. The notice must identify all known SIMs involved in the investigation (see DIOG Appendix G - Classified Provisions for additional notice requirements). If a SIM arises after the opening of a Preliminary Investigation, investigative activity may continue, but the matter must be reviewed by OGC and approved by the appropriate FBIHQ operational SC as soon as practicable, but not more than five (5) business days thereafter to continue the investigation. Notice must be provided as specified above.

D) (U//FOUO) ***FBIHQ Disapproves Opening:*** The Executive Assistant Director (EAD) for the National Security Branch must notify the Deputy Attorney General if FBIHQ disapproves a field office's opening of a Preliminary Investigation relating to a threat to the national security on the ground that the predication for the investigation is insufficient, and the EAD for the National Security Branch is responsible for establishing a system that will allow for the prompt retrieval of such denials. (AGG-Dom, Part II.B.5.d)

6.7.2 (U) EXTENSION

(U//FOUO) A Preliminary Investigation must be concluded within six months of its opening but may be extended for up to six months by the SAC (delegable to the ASAC)[6]. FBIHQ division PGs may require written notification of this six month extension to the appropriate FBIHQ operational unit and section. Extensions of Preliminary Investigations beyond a year are discouraged and may only be approved by the appropriate FBIHQ operational section for "good cause." (AGG-Dom, Part II.B.4.a.ii)

[6] (U//FOUO) SAC approval required to extend Preliminary Investigations was non-delegable in the previous version of the DIOG. That restriction has been removed in this version.

6.7.2.1 (U) GOOD CAUSE

(U//FOUO) The following factors must be used to determine whether "good cause" exists to extend the Preliminary Investigation beyond one year:

A) (U//FOUO) Whether logical investigative steps have yielded information that tends to inculpate or exculpate the subject;

B) (U//FOUO) The progress that has been made toward determining whether a Full Investigation should be opened or the Preliminary Investigation should be closed;

C) (U//FOUO) Whether, based on the planned course of investigation for the following six months, it is reasonably likely that information will be obtained that will lead to predication for a Full Investigation, thereby warranting an extension for another six months, or will lead to exculpatory information, thereby warranting closing the Preliminary Investigation; and

D) (U//FOUO) Whether adequate predication has been developed to justify opening a Full Investigation or whether sufficient information has been developed that justifies closing the Preliminary Investigation.

6.7.3 (U) PENDING INACTIVE STATUS

(U//FOUO) [redacted] b7E

6.7.4 (U) CONVERSION TO FULL INVESTIGATION

(U//FOUO) When converting a Preliminary Investigation to a Full Investigation, see DIOG Section 7 for approval and notification requirements.

6.7.5 (U) FILE REVIEW

(U//FOUO) Supervisory file reviews must be conducted at least once every 90 days in accordance with DIOG Section 3.4.4. File reviews for probationary FBI employees must be conducted at least every 60 days.

6.8 (U) STANDARDS FOR OPENING OR APPROVING THE USE OF AN AUTHORIZED INVESTIGATIVE METHOD IN PRELIMINARY INVESTIGATIONS

(U//FOUO) Prior to opening or approving the use of an investigative method, an FBI employee or approving official must determine whether:

A) (U//FOUO) The use of the particular investigative method is likely to further the authorized purpose of the Preliminary Investigation;

B) (U//FOUO) The investigative method selected is the least intrusive method, if reasonable based upon the circumstances of the investigation; and

C) (U//FOUO) The method to be used is an appropriate use of personnel and financial resources.

6.9 (U) AUTHORIZED INVESTIGATIVE METHODS IN PRELIMINARY INVESTIGATIONS

(U) All lawful methods may be used in a Preliminary Investigation, except for mail opening, physical search requiring a Federal Rules of Criminal Procedure (FCRP) Rule 41 search warrant or a Foreign Intelligence Surveillance Act (FISA) order, electronic surveillance requiring a judicial order or warrant (Title III or FISA), or Title VII FISA requests. Authorized methods include, but are not limited to, those listed below. Some of the methods listed are subject to special restrictions or review or approval requirements. (AGG-Dom, Part V.4.A)

(U//FOUO) A complete discussion of these investigative methods, including approval requirements, is contained in Section 18. The use or dissemination of information obtained by the use of the below methods must comply with the AGG-Dom and DIOG Section 14. The following investigative methods are authorized to be used in Preliminary Investigations:

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)

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

(U//FOUO) *Note:* For those state, local and tribal governments that do not sanction or provide a law enforcement exception available to the FBI for one-party consent recording of communications with persons within their jurisdiction, the SAC must approve the consensual monitoring of communications as an Otherwise Illegal Activity (OIA). Prior to the SAC authorizing the OIA, one-party consent must be acquired. The SAC may delegate the OIA approval authority to an Assistant Special Agent-in-Charge (ASAC) or Supervisory Special Agent (SSA).

(U//FOUO) See the classified provisions in Appendix G for additional information.

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

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

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

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

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

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

P) (U) Stored wire and electronic communications and transactional records. (See Section 18.6.8)[7]

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

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

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

T) (U) Trash Covers (Searches that do not require a warrant or court order). (See Section 18.6.12)

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

(U) See the classified provisions in DIOG Appendix G for additional information.

6.10 (U) SENSITIVE INVESTIGATIVE MATTERS (SIM) IN PRELIMINARY INVESTIGATIONS

(U//FOUO) [redacted] b7E
[redacted] DIOG Section 10 contains the required approval authority and factors for consideration when determining whether to conduct or approve a Preliminary Investigation involving a SIM.

6.10.1 (U) SIM CATEGORIES IN PRELIMINARY INVESTIGATIONS

(U//FOUO) A SIM is an investigative matter involving the activities of a domestic public official or domestic political candidate (involving corruption or a threat to the national security), religious or domestic political organization or individual prominent in such an organization, or news media, an academic nexus, or any other matter which, in the judgment of the official authorizing an investigation, should be brought to the attention of FBIHQ and other DOJ officials. (AGG-Dom, Part VII.N.) As a matter of FBI policy, "judgment" means that the decision of the authorizing official is discretionary. [redacted] b7E

6.10.2 (U) ACADEMIC NEXUS IN PRELIMINARY INVESTIGATIONS

(U//FOUO) [redacted] b7E

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

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

[7] (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)

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

(U//FOUO) b7E

6.11 (U) INTELLIGENCE COLLECTION (I.E., INCIDENTAL COLLECTION)

(U//FOUO) b7E

(See DIOG Section 15.6.1.2 - Written Intelligence Products)

(U//FOUO) b7E

6.12 (U) STANDARDS FOR APPROVING THE CLOSING OF A PRELIMINARY INVESTIGATION

6.12.1 (U) STANDARDS

(U//FOUO) At the conclusion of a Preliminary Investigation, each of the following items must be documented in the closing communication (EC and/or LHM):

A) (U//FOUO) A summary of the results of the investigation;

B) (U//FOUO) Whether all logical and reasonable investigation was completed;

C) (U//FOUO) Whether all investigative methods/techniques initiated have been completed and/or discontinued;

D) (U//FOUO) Whether all leads set have been completed and/or discontinued;

E) (U//FOUO) Whether all evidence has been returned, destroyed or retained in accordance with evidence policy; and

F) (U//FOUO) A summary statement of the basis on which the Preliminary Investigation will be closed, and a selection of the appropriate closing status:

1) (U//FOUO) C-4: Administrative Closing, which includes:

a) (U//FOUO) No further investigation is warranted because logical investigation and/or leads have been exhausted, and the investigation to date did not identify a criminal violation or a priority threat to the national security

b) (U//FOUO) Investigation assigned a new file number

c) (U//FOUO) Investigation consolidated into a new file number or an existing file number, or

d) (U//FOUO) Unaddressed Work investigation file closed because no investigation or no further investigation will be conducted

2) (U//FOUO) C-5: USA Declination Closing, which includes:

a) (U//FOUO) The USAO declined prosecution – individual matter declination

b) (U//FOUO) The USAO declined prosecution – blanket declination

3) (U//FOUO) C-6: Other Closing, which includes:

a) (U//FOUO) National security investigation has been completed

b) (U//FOUO) Prosecution became non-viable for national security reasons

c) (U//FOUO) Any other reason to close

6.12.2 *(U) Approval Requirements to Close*

(U//FOUO) The appropriate closing supervisor described below must review and approve the closing communication (as described in Section 6.12.1) to ensure it contains the above required information and sufficient details of the investigation on which to base the decision to close the Preliminary Investigation. The closing supervisor must note on the closing document "C," the closing number 4, 5 or 6 (e.g., C-4, C-5 or C-6) and the closing date. The appropriate closing supervisors are:

A) (U//FOUO) **Opened by a Field Office:** Closing a Preliminary Investigation opened by a field office requires approval from the SSA. Notification to the FBIHQ operational unit may be required by division PGs.

B) (U//FOUO) **Opened by FBIHQ:** Closing a Preliminary Investigation opened by FBIHQ requires approval from the UC and notification to any appropriate field office.

C) (U//FOUO) **SIM Opened by a Field Office:** Closing a Preliminary Investigation opened by a field office involving a SIM requires approval from the SAC, written notification to the FBIHQ operational unit and section and the USAO, if the USAO was notified of the opening.

D) (U//FOUO) **SIM Opened by FBIHQ:** Closing a Preliminary Investigation opened by FBIHQ involving a SIM requires approval from the SC and written notification to any appropriate field office.

6.13 (U) Other Program Specific Investigative Requirements

(U//FOUO) To facilitate compliance with investigative program specific requirements, the FBI employee should consult the relevant division's PG. FBIHQ division PGs, however, may not contradict, alter or otherwise modify the standards established in the DIOG.

7 (U) FULL INVESTIGATIONS

7.1 (U) OVERVIEW

(U//FOUO) The AGG-Dom authorizes a second level of investigative activity—Predicated Investigations. Predicated Investigations that concern federal crimes or threats to the national security are subdivided into Preliminary Investigations (PI) and Full Investigations (Full). A Full Investigation may be opened if there is an "articulable factual basis" of possible criminal or national threat activity, as discussed in greater detail in Section 7.5, below. There are three types of Full Investigations: (i) single and multi-subject; (ii) Enterprise; and (iii) positive foreign intelligence collection.

7.2 (U) PURPOSE AND SCOPE

(U) A Full Investigation may be opened to detect, obtain information about, or prevent or protect against federal crimes or threats to the national security or to collect foreign intelligence.

(U) The purposes for conducting Full Investigations include such matters as:

A) (U) determining whether a federal crime is being planned, prepared for, occurring or has occurred;

B) (U) identifying, locating, and apprehending the perpetrators;

C) (U) obtaining evidence for prosecution;

D) (U) identifying threats to the national security;

E) (U) investigating an enterprise (as defined in DIOG Section 8); or

F) (U) collecting positive foreign intelligence (PFI) (as defined in DIOG Section 9).

(U) The investigation of threats to the national security can be investigated under the FBI's criminal investigation authority or its authority to investigate threats to the national security. As with criminal investigations, detecting and solving crimes, gathering evidence and arresting and prosecuting the perpetrators are frequently the objectives of investigations relating to threats to the national security. These investigations also serve important purposes outside the ambit of normal criminal investigations, however, by providing the basis for decisions concerning other measures needed to protect the national security.

(U//FOUO) A Full Investigation solely for the collection of positive foreign intelligence extends the sphere of the FBI's information gathering activities beyond federal crimes and threats to the national security and permits the FBI to seek information regarding a broader range of matters relating to foreign powers, organizations, or persons that may be of interest to the conduct of the United States' foreign affairs. (See DIOG Section 9)

7.3 (U) CIVIL LIBERTIES AND PRIVACY

(U) The pursuit of legitimate investigative goals without infringing upon the exercise of constitutional freedoms is a challenge that the FBI meets through the application of sound

judgment and discretion. In order to protect civil liberties e the conduct of criminal and national security investigations, every Full Investigation under this subsection must have adequate predication that is documented in the opening communication.

(U) No investigative activity, including Full Investigations, may be taken solely on the basis of activities that are protected by the First Amendment or on the race, ethnicity, national origin or religion of the subject, or a combination of only those factors. Full Investigations of individuals, groups or organizations must focus on activities related to the threats or crimes being investigated, not solely on First Amendment activities or on the race, ethnicity, national origin or religion of the subject. In this context, it is particularly important clearly to identify and document the law enforcement or national security basis of the Full Investigation.

(U) *Example:* Individuals or groups who communicate with each other or with members of the public in any form in pursuit of social or political causes—such as opposing war or foreign policy, protesting government actions, promoting certain religious beliefs, championing particular local, national, or international causes, or a change in government through non-criminal means, and actively recruit others to join their causes—have a fundamental constitutional right to do so. A Full Investigation may not be opened based solely on the exercise of these First Amendment rights.

(U) The AGG-Dom authorize all lawful investigative methods in the conduct of a Full Investigation. Considering the effect on the privacy and civil liberties of individuals and the potential to damage the reputation of individuals, some of these investigative methods are more intrusive than others. The least intrusive method if reasonable based upon the circumstances of the investigation is to be used, but the FBI must not hesitate to use any lawful method consistent with the AGG-Dom. A more intrusive method may be warranted in light of the seriousness of a criminal or national security threat or the importance of a foreign intelligence requirement.

(U) By emphasizing the use of the least intrusive means to obtain intelligence or evidence, FBI employees can effectively execute their duties while mitigating the potential negative impact on the privacy and civil liberties of all people encompassed within the investigation, including targets, witnesses, and victims. This principle is not intended to discourage FBI employees from seeking relevant and necessary intelligence, information, or evidence, but rather is intended to encourage FBI employees to choose the least intrusive—but still reasonable based upon the circumstances of the investigation—from the available options to obtain the intelligence, information or evidence. (See DIOG Section 4)

7.4 (U) LEGAL AUTHORITY

7.4.1 (U) CRIMINAL INVESTIGATIONS

(U) The FBI has statutory authority to investigate all federal crime not assigned exclusively to another federal agency. (See 28 U.S.C. § 533; 18 U.S.C. § 3052; 28 C.F.R. § 0.85 [a].)

(U) The FBI also has special investigative jurisdiction to investigate violations of state law in limited circumstances. Specifically, the FBI has jurisdiction to investigate felony killings of state law enforcement officers (28 U.S.C. § 540), violent crimes against interstate travelers (28 U.S.C.

§ 540A), and serial killers (28 U.S.C. § 540B). Authority to investigate these matters is contingent on receiving a request by an appropriate state official.

7.4.2 (U) THREATS TO THE NATIONAL SECURITY

(U) The FBI has authority to investigate threats to the national security pursuant to executive orders, Attorney General authorities, and various statutory sources. (See E.O. 12333; 50 U.S.C. §§ 401 et seq.; 50 U.S.C. §§ 1801 et seq.)

(U) "Threats to the national security" are specifically defined to mean: international terrorism; espionage and other intelligence activities, sabotage, and assassination, conducted by, for, or on behalf of foreign powers, organizations, or persons; foreign computer intrusion; and other matters determined by the Attorney General, consistent with Executive Order 12333 or any successor order. (AGG-Dom, Part VII.S)

7.4.3 (U) FOREIGN INTELLIGENCE COLLECTION

(U) The FBI authority to collect foreign intelligence derives from a mixture of administrative and statutory sources. (See E.O. 12333; 50 U.S.C. §§ 401 et seq.; 50 U.S.C. §§ 1801 et seq.; 28 U.S.C. § 532 note (incorporates the Intelligence Reform and Terrorism Protection Act, P.L. 108-458 §§ 2001-2003).

(U) "Foreign Intelligence" is defined as information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations or foreign persons, or international terrorists. (AGG-Dom, Part VII.E)

7.5 (U) PREDICATION

(U) A Full Investigation may be opened if there is an "articulable factual basis" that reasonably indicates one of the following circumstances exists:

A) (U) An activity constituting a federal crime or a threat to the national security has or may have occurred, is or may be occurring, or will or may occur and the investigation may obtain information relating to the activity or the involvement or role of an individual, group, or organization in such activity;

B) (U) An individual, group, organization, entity, information, property, or activity is or may be a target of attack, victimization, acquisition, infiltration, or recruitment in connection with criminal activity in violation of federal law or a threat to the national security and the investigation may obtain information that would help to protect against such activity or threat; or

C) (U) The investigation may obtain foreign intelligence that is responsive to a PFI requirement, as defined in DIOG Section 7.4.3, above.

(U//FOUO) *Examples*: The following examples have sufficient predication to open a Full Investigation:

A) (U//FOUO) corroborated information from an intelligence agency states that an individual is a member of a terrorist group;

B) (U//FOUO) an analyst discovers on a blog a threat to a specific home builder and additional information connecting the blogger to a known terrorist group; and

C) (U//FOUO) FBI DI has posted an authorized PFI requirement for collection.

7.6 (U) STANDARDS FOR OPENING OR APPROVING A FULL INVESTIGATION

(U//FOUO) Before opening or approving the conduct of a Full Investigation, an FBI employee or approving official must determine whether:

A) (U//FOUO) Adequate predication exist for opening a Full Investigation;

B) (U//FOUO) The Full Investigation is not based solely on the exercise of First Amendment activities or on the race, ethnicity, national origin or religion of the subject or a combination of only such factors; and

C) (U//FOUO) The Full Investigation is an appropriate use of personnel and financial resources.

(U//FOUO) Additional policies regarding Full Investigations involving any foreign ambassador, foreign official, foreign student or exchange visitor, protected persons or premises as subjects may be found in DIOG Appendix G – Classified Provisions [No Foreign Policy Objection (NFPO)].

(U//FOUO) A Full Investigation cannot be opened solely based on an FBI collection requirement.

7.7 (U) OPENING DOCUMENTATION, APPROVAL, EFFECTIVE DATE, NOTICE, PENDING INACTIVE STATUS, FILE REVIEW, AND LETTER HEAD MEMORANDUM

7.7.1 (U) OPENING DOCUMENTATION

(U/FOUO) The predication to open a Full Investigation must be documented in the opening EC. The appropriate approving authority may grant oral authority to open a Full Investigation if the standards for opening or approving a Full Investigation are met. Should oral authorization to conduct a Full Investigation be granted, an EC setting forth the predicating facts, as well as the identity of the authorizing supervisor and date of oral authorization, must be documented to the supervisor who granted the oral authorization, as soon as practicable, but not more than five (5) business days after granting the authorization.

b7E

(U//FOUO) [redacted]

(U//FOUO) The DIOG prohibits the use of control files or administrative files to document investigative activity. See DIOG Appendix J.

7.7.1.1 (U) APPROVAL / EFFECTIVE DATE / NOTICE

(U/FOUO) The effective date of the Full Investigation is the date the final approval authority (e.g., SSA or SAC) approves the EC [redacted] If the Full Investigation is opened on oral

b7E

authority, the date on which the oral authority was granted is the date the investigation was opened. See Section 3.4.2.2.

A) (U//FOUO) ***Opened By a Field Office:*** The opening of a Full Investigation for circumstances described in Sections 7.5.A and 7.5.B (i.e., for any reason other than to collect intelligence that is responsive to a PFI requirement) by a field office requires prior approval of the SSA with written notification within 15 calendar days of the opening to the responsible FBIHQ operational unit. The opening of a Full Investigation of a United States person (USPER) relating to a threat to the national security for circumstances described in Sections 7.5.A and 7.5.B (i.e., for any reason other than to collect intelligence that is responsive to a PFI requirement) requires the responsible FBIHQ-NSB unit to notify DOJ NSD as soon as practicable, but in all events within 30 calendar days after the investigation is opened or the subject is determined to be an USPER. If the subject of the investigation is a non-USPER and later becomes or is determined to be an USPER, the notice provisions in this subsection to DOJ NSD also apply.

B) (U//FOUO) ***Opened By FBIHQ:*** The opening of a Full Investigation by FBIHQ for circumstances described in Sections 7.5.A and 7.5.B (i.e., for any reason other than to collect intelligence that is responsive to a PFI requirement) requires prior approval of the UC with written notification within 15 calendar days of the opening to any appropriate field office. The opening of a Full Investigation by FBIHQ of an USPER relating to a threat to the national security for circumstances described in Sections 7.5.A and 7.5.B (i.e., for any reason other than to collect intelligence that is responsive to a PFI requirement) also requires notice to DOJ NSD as soon as practicable, but in all events within 30 days after the investigation is opened or the subject is determined to be an USPER. If the subject of the investigation is a non-USPER and later becomes or is determined to be an USPER, the notice provisions in this subsection to the field office and DOJ also apply.

C) (U//FOUO) ***Sensitive Investigative Matters (SIM):*** The opening of a Full Investigation involving a sensitive investigative matter:

1) (U//FOUO) ***SIM Opened By a Field Office:*** requires prior CDC review and SAC approval, and written notification (EC and disseminable LHM) to the appropriate FBIHQ operational UC and SC within 15 calendar days following the opening. Additionally, the field office must notify the USAO, in writing, unless such notification is inappropriate under the circumstances (e.g., a public corruption investigation of a person who is personally close to the United States Attorney (USA)), or the matter is a counterintelligence or espionage investigation. (See CD PG for details concerning notice in counterintelligence and espionage investigations.) If notice is not provided to the USAO under the circumstances described above, the field office must explain those circumstances in the written notice to FBIHQ. The responsible FBIHQ section must notify, in writing, the appropriate DOJ Criminal Division official or NSD official as soon as practicable, but no later than 30 calendar days after the investigation is opened. [redacted] b7E Notice must be furnished as specified above.

2) (U//FOUO) ***SIM Opened By FBIHQ:*** requires prior OGC review and SC approval, and written notification (EC and disseminable LHM) to any appropriate field office within 15 calendar days following the opening. Additionally, FBIHQ operational unit must notify the

appropriate USAO(s) in writing, unless such notification is inappropriate under the circumstances (e.g., a public corruption investigation of a person who is personally close to the USA) or the matter is a counterintelligence or espionage investigation; and the appropriate DOJ Criminal Division official or NSD official, as soon as practicable, but no later than 30 calendar days after such an investigation is opened. (See CD PG for details concerning notice in counterintelligence and espionage investigations.) If notice is not provided to the USAO under the "circumstances" exception described above, FBIHQ must explain the circumstances in the written notice to the field office(s) and DOJ. [redacted] b7E

[redacted] Notice must be furnished as specified above. (AGG-Dom, Part II.B.5.a)

D) (U//FOUO) ***Positive Foreign Intelligence Full Investigation:*** The opening of a Full Investigation in order to collect positive foreign intelligence for circumstances described in Section 7.5.C above must be approved as provided in DIOG Section 9. Additionally, written notification to FBIHQ Domain, Collection, HUMINT Management Section (DCHMS) SC and DOJ NSD is required as soon as practicable but no later than 30 calendar days after opening the investigation.

E) (U//FOUO) ***FBIHQ Disapproves Opening:*** The EAD for the National Security Branch (NSB) must notify the Deputy Attorney General if FBIHQ disapproves a field office's opening of a Full Investigation relating to a threat to the national security on the ground that the predication for the investigation is insufficient, and the EAD for the NSB is responsible for establishing a system that will allow for the prompt retrieval of such denials. (AGG-Dom, Part II.B.5.d)

7.7.2 (U) PENDING INACTIVE STATUS

(U/FOUO) A Full Investigation may be placed in "pending inactive" status once all logical investigation has been completed and only prosecutive action or other disposition remains to be reported. Examples of Full Investigations that may be placed in "pending inactive" status would include, but not be limited to: criminal investigations pending an appeal; fugitive investigations, when all logical investigation has been conducted and the subject is still in fugitive status; parental kidnapping investigations, when the parent who kidnapped the child is residing in a foreign country and the local authorities will not or cannot extradite the subject back to the United States.

7.7.3 (U) FILE REVIEW

(U/FOUO) Supervisory file reviews must be conducted at least once every 90 days in accordance with DIOG Section 3.4.4. File reviews for probationary FBI employees must be conducted at least every 60 days.

7.7.4 (U) ANNUAL LETTERHEAD MEMORANDUM

(U/FOUO) Annual letterhead memoranda regarding the status of Full Investigations are not required by the AGG-Dom; however, the FBIHQ operational divisions may require such reports

in their PGs. See foreign intelligence collection in Section 9 for annual reporting requirements to FBIHQ DCHMS and DOJ.

7.8 (U) STANDARDS FOR OPENING OR APPROVING THE USE OF AN AUTHORIZED INVESTIGATIVE METHOD IN FULL INVESTIGATIONS

(U//FOUO) Prior to opening or approving the use of an investigative method, an FBI employee or approving official must determine whether:

A) (U//FOUO) The use of the particular investigative method is likely to further the authorized purpose of the Full Investigation;

B) (U//FOUO) The investigative method selected is the least intrusive method, if reasonable based upon the circumstances of the investigation;

C) (U//FOUO) If the Full Investigation is for collecting positive foreign intelligence, the FBI is operating openly and consensually with a USPER, to the extent practicable; and

D) (U//FOUO) The method to be used is an appropriate use of personnel and financial resources.

7.9 (U) AUTHORIZED INVESTIGATIVE METHODS IN FULL INVESTIGATIONS

(U) All lawful methods may be used in a Full Investigation, unless the investigation is to collect foreign intelligence. A complete discussion of these investigative methods, including approval requirements, is contained in Section 18. The use or dissemination of information obtained by the use of these methods must comply with the AGG-Dom and DIOG Section 14. The following investigative methods are authorized to be used in all Full Investigations, other than investigations to collect foreign intelligence:

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

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

C) (U) Records or information - Other federal, state, local, tribal, or foreign government agency. (Section 18.5.3)

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

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

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

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

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

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

(U//FOUO) *Note*: [redacted] b7E

(U//FOUO) See the classified provisions in Appendix G for additional information.

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

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

L) (U) Administrative subpoenas. (Section 18.6.4)

M)(U) Grand jury subpoenas. (Section 18.6.5)

N) (U) National Security Letters. (Section 18.6.6)

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

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

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

R) (U) Mail covers. (Section 18.6.10)

S) (U) Polygraph examinations. (Section 18.6.11)

T) (U) Trash Covers (Searches that do not require a warrant or court order). (Section 18.6.12)

U) (U) Undercover Operations (Section 18.6.13)

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

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

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

(U) See the classified provisions in DIOG Appendix G for additional information.

7.10 (U) SENSITIVE INVESTIGATIVE MATTERS (SIM) IN FULL INVESTIGATIONS

(U//FOUO) [redacted] b7E

[redacted]DIOG Section 10 contains the required approval authority and factors to be considered when determining whether to conduct or approve a Full Investigation involving a SIM.

7.10.1 (U) SIM CATEGORIES IN FULL INVESTIGATIONS

(U/FOUO) A SIM is an investigative matter involving the activities of a domestic public official or domestic political candidate (involving corruption or a threat to the national security), religious or domestic political organization or individual prominent in such an organization, or news media, an academic nexus, or any other matter which, in the judgment of the official authorizing an investigation, should be brought to the attention of FBIHQ and other DOJ officials. (AGG-Dom, Part VII.N). As a matter of FBI policy, "judgment" means that the decision of the authorizing official is discretionary. DIOG Section 10 and/or the DIOG Appendix G – Classified Provisions define [redacted]

b7E

7.10.2 *(U) Academic Nexus in Full Investigations*

(U/FOUO)

A) (U//FOUO) b7E

B) (U//FOUO)

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

(U//FOUO) b7E

7.11 (U) Intelligence Collection (i.e., Incidental Collection)

(U//FOUO) b7E

(See DIOG Section 15.6.1.2 - Written Intelligence Products)

(U//FOUO) b7E

(U) Because the authority to collect positive foreign intelligence enables the FBI to obtain information pertinent to the United States' conduct of its foreign affairs, even if that information is not related to criminal activity or threats to the national security, the information gathered may concern lawful activities. Accordingly, the FBI must operate openly and consensually with an USPER to the extent practicable when collecting positive foreign intelligence that does not concern criminal activities or threats to the national security.

7.12 (U) STANDARDS FOR APPROVING THE CLOSING OF A FULL INVESTIGATION

7.12.1 (U) STANDARDS

(U//FOUO) At the conclusion of a Full Investigation, each of the following items must be documented in the closing communication (EC and/or LHM):

A) (U//FOUO) A summary of the results of the investigation;

B) (U//FOUO) Whether sufficient personnel and financial resources were expended on the investigation, or an explanation/justification for not expending sufficient resources;

C) (U//FOUO) Whether logical and reasonable investigation was completed;

D) (U//FOUO) Whether all investigative methods/techniques initiated have been completed and/or discontinued;

E) (U//FOUO) Whether all leads set have been completed and/or discontinued;

F) (U//FOUO) Whether all evidence has been returned, destroyed or retained in accordance with evidence policy; and

G) (U//FOUO) A summary statement of the reason the Full Investigation will be closed, and selection of the appropriate closing status:

1) (U//FOUO) C-4: Administrative Closing, which includes:

a) (U//FOUO) No further investigation is warranted because logical investigation and/or leads have been exhausted, and the investigation to date did not identify a criminal violation or a priority threat to the national security

b) (U//FOUO) Investigation assigned a new file number

c) (U//FOUO) Investigation consolidated into a new file number or an existing file number

d) (U//FOUO) Unaddressed Work investigation file closed because no investigation or no further investigation will be conducted

2) (U//FOUO) C-5: USA Declination Closing, which includes:

a) (U//FOUO) The USAO declined prosecution – individual matter declination

b) (U//FOUO) The USAO declined prosecution – blanket declination

3) (U//FOUO) C-6: Other Closing, which includes:

a) (U//FOUO) Final prosecution or final prosecutive action has been completed

b) (U//FOUO) National security investigation has been completed

c) (U//FOUO) Prosecution became non-viable for national security reasons

d) (U//FOUO) A federal grand jury returned a "No True Bill"

e) (U//FOUO) A nolle prosequi has been entered with the court

f) (U//FOUO) any other reason for closing

7.12.2 (U) APPROVAL REQUIREMENTS TO CLOSE

(U//FOUO) The appropriate closing supervisor described below must review and approve the closing communication (as described in Section 7.12.1) to ensure it contains the above-required information and sufficient details of the investigation on which to base the decision to close the Full Investigation. The closing supervisor must note on the closing document "C," the closing number 4, 5 or 6 (e.g., C-4, C-5 or C-6) and the closing date. Although there is no duration limit for a Full Investigation, the investigation must be closed upon all investigative activity being exhausted. The appropriate closing supervisors are:

A) (U//FOUO) ***Opened by a Field Office:*** Closing a Full Investigation opened by a field office requires approval from the SSA. Notification to the FBIHQ operational unit may be required by division PGs.

B) (U//FOUO) ***Opened by FBIHQ:*** Closing a Full Investigation opened by FBIHQ requires approval from the UC and notification to the appropriate field office.

C) (U//FOUO) ***SIM Opened by a Field Office:*** Closing a Full Investigation opened by a field office involving a sensitive investigative matter requires approval from the SAC and written notification to the FBIHQ operational unit and section and the USAO, if the USAO was notified of the opening.

D) (U//FOUO) ***SIM Opened by FBIHQ:*** Closing a Full Investigation opened by FBIHQ involving a sensitive investigative matter requires approval from the SC and written notification to the appropriate field office.

E) (U//FOUO) ***Positive Foreign Intelligence:*** (See DIOG Section 9)

7.13 (U) OTHER PROGRAM SPECIFIC INVESTIGATIVE REQUIREMENTS

(U//FOUO) To facilitate compliance with investigative program-specific requirements, the FBI employee should consult the relevant division's PG to ascertain any program-specific requirements. FBIHQ division PGs, however, may not contradict, alter or otherwise modify the standards established in the DIOG.

This Page is Intentionally Blank.

8 (U) ENTERPRISE INVESTIGATIONS (EI)

8.1 (U) OVERVIEW

(U) An Enterprise Investigation (EI) may only be opened and operated as a Full Investigation and is subject to the same requirements that apply to a Full Investigation as described in DIOG Section 7, although there are additional approval requirements that affect Enterprise Investigations. An Enterprise Investigation focuses on a group or organization that may be involved in the most serious criminal or national security threats to the public, as described in Section 8.5 below. An Enterprise Investigation cannot be conducted as Preliminary Investigation or an Assessment, nor may they be conducted for the sole purpose of collecting positive foreign intelligence (PFI). See Section 8.2, below, regarding Preliminary Investigations and Assessments.

8.2 (U) PURPOSE, SCOPE AND DEFINITIONS

(U) **Enterprise defined:** An enterprise is a group of persons associated together for a common purpose of engaging in a course of conduct. The term "enterprise" includes any partnership, corporation, association, or other legal entity, and any union or group of individuals associated in fact, although not a legal entity.

(U) **Associated in fact defined:** The term "associated in fact" means the persons have an ongoing organization, formal or informal, and that the persons function together as a continuing unit.

(U) **Purpose/Scope:** The purpose of an Enterprise Investigation is to examine the structure, scope, and nature of the group or organization including: its relationship, if any, to a foreign power; the identity and relationship of its members, employees, or other persons who may be acting in furtherance of its objectives; its finances and resources; its geographical dimensions; its past and future activities and goals; and its capacity for harm. (Attorney General's Guidelines for Domestic FBI Operations (AGG-Dom), Part II.C.2)

(U) *Note:* Enterprise Investigations were designed, among other things, to combine and replace the traditional "Racketeering Enterprise Investigations" (92 classification) and "Terrorism Enterprise Investigations" (100 classification). An Enterprise Investigation is only authorized to be opened on the most serious criminal or national security threats. The term Enterprise Investigation as used in the DIOG should not be confused with other usages of the word "enterprise," such as criminal enterprise investigations (e.g., 281 classification, 245 classification, etc.), which are not Enterprise Investigations as defined in DIOG Section 8. See DIOG Sections 8.4 and 8.5.

(U//FOUO) Although an Enterprise Investigation may not be conducted as a Preliminary Investigation, a Preliminary Investigation may be used to determine whether a group or organization is a criminal or terrorist enterprise if the FBI has "information or an allegation" that an activity constituting a federal crime or a threat to the national security has or may have occurred, is or may be occurring, or will or may occur, and the investigation may obtain

information relating to the activity of the group or organization in such activity. An Assessment may also be opened to determine whether a group or organization is involved in activities constituting violations of federal criminal law or threats to the national security.

8.3 (U) CIVIL LIBERTIES AND PRIVACY

(U) The pursuit of legitimate investigative goals without infringing upon the exercise of constitutional freedoms is a challenge that the FBI meets through the application of sound judgment and discretion. In order to protect civil liberties in the conduct of criminal and national security investigations, every Full Investigation, including an Enterprise Investigation under this subsection, must have adequate predication documented in the opening communication.

(U) No investigative activity, including an Enterprise Investigation, may be taken solely on the basis of activities that are protected by the First Amendment or on the race, ethnicity, national origin or religion of the subject or a combination of only those factors. An Enterprise Investigation of groups and organizations must focus on activities related to the threats or crimes being investigated, not solely on First Amendment activities or on the race, ethnicity, national origin or religion of the members of the group or organization. In this context, it is particularly important clearly to identify and document the law enforcement or national security basis of the Enterprise Investigation.

(U//FOUO) *Example:* Groups who communicate with each other or with members of the public in any form in pursuit of social or political causes—such as opposing war or foreign policy, protesting government actions, promoting certain religious beliefs, championing particular local, national, or international causes, or a change in government through non-criminal means, and actively recruit others to join their causes—have a fundamental constitutional right to do so. An Enterprise Investigation may not be opened based solely on the exercise of these First Amendment rights.

(U) The AGG-Dom authorizes all lawful investigative methods in the conduct of an Enterprise Investigation. Considering the effect on the privacy and civil liberties of individuals and the potential to damage the reputation of individuals, some of these investigative methods are more intrusive than others. The least intrusive method if reasonable based upon the circumstances of the investigation is to be used, but the FBI must not hesitate to use any lawful method consistent with the AGG-Dom. A more intrusive method may be warranted in light of the seriousness of a criminal or national security threat.

(U) By emphasizing the use of the least intrusive means to obtain information, intelligence and/or evidence, FBI employees can effectively execute their duties while mitigating the potential negative impact on the privacy and civil liberties of all people encompassed within the investigation, including targets, witnesses, and victims. This principle is not intended to discourage FBI employees from seeking relevant and necessary intelligence, information, or evidence, but rather is intended to encourage FBI employees to choose the least intrusive—but still effective means—from the available options to obtain the information , intelligence or evidence. See DIOG Section 4.4.

8.4 (U) PREDICATION

(U) A Full Investigation of a group or organization may be opened as an Enterprise Investigation if there is an articulable factual basis for the investigation that reasonably indicates the group or organization may have engaged, or may be engaged in, or may have or may be engaged in planning or preparation or provision of support for: (AGG-Dom, Part II.C.1)

A) (U) **Racketeering Activity**:

(U) A pattern of racketeering activity as defined in 18 U.S.C. § 1961(5) - (92 and 305A matters may be opened as Enterprise Investigations-Racketeering Activity (EI/RA));

B) (U) **International Terrorism**:

(U) International terrorism, as defined in 18 U.S.C. § 2331 and AGG-Dom, Part VII.J or other national security threat – (415 matters may be opened as Enterprise Investigations);

C) (U) **Domestic Terrorism**:

1) (U) Domestic terrorism as defined in 18 U.S.C. § 2331(5) involving a violation of federal criminal law - (100 matters may be opened as Enterprise Investigations);

2) (U) Furthering political or social goals wholly or in part through activities that involve force or violence and a violation of federal criminal law – (100 matters may be opened as Enterprise Investigations); or

3) (U) An offense described in 18 U.S.C. § 2332b(g)(5)(B) or 18 U.S.C. § 43 – (100 matters may be opened as Enterprise Investigations).

(U) The "articulable factual basis" for opening an Enterprise Investigation is met with the identification of a group whose statements made in furtherance of its objectives or its conduct demonstrate a purpose of committing crimes or securing the commission of crimes by others. The group's activities and statements of its members may be considered in combination to comprise the "articulable factual basis," even if the statements alone or activities alone would not warrant such a determination.

(U//FOUO)

A) (U//FOUO)

B) (U//FOUO)

b7E

C) (U//FOUO)

8.5 (U) STANDARDS FOR OPENING OR APPROVING AN ENTERPRISE INVESTIGATION

(U//FOUO) Before opening or approving the conduct of an Enterprise Investigation, an FBI employee or approving official must determine whether:

A) (U//FOUO) Adequate predication exists for opening an Enterprise Investigation;

B) (U//FOUO) The Enterprise Investigation is not based solely on the exercise of First Amendment activities or on the race, ethnicity, national origin or religion of the subject or a combination of only such factors; and

C) (U//FOUO) The Enterprise Investigation is an appropriate use of personnel and financial resources.

(U//FOUO) Additional policies regarding Enterprise Investigation involving any foreign ambassador, foreign official, foreign student or exchange visitor, protected persons or premises as subjects may be found in DIOG Appendix G – Classified Provisions [No Foreign Policy Objection (NFPO)].

(U//FOUO) A Predicated Investigation, including an Enterprise Investigation, cannot be opened solely based on an FBI collection requirement.

8.6 (U) OPENING DOCUMENTATION, EFFECTIVE DATE, APPROVAL, NOTICE, AND FILE REVIEW

8.6.1 (U) OPENING DOCUMENTATION

(U//FOUO) The predication to open an Enterprise Investigation must be documented in the opening electronic communication (EC).

(U//FOUO) [redacted] b7E

(U//FOUO) The appropriate approving authority (Section Chief) may grant oral authority to open an Enterprise Investigation if the standards for opening or approving an Enterprise Investigation are met. Should oral authorization to conduct an Enterprise Investigation be granted, an EC setting forth the predicating facts, as well as the identity of the approving official(s) (i.e., SC), and the date of oral authorization must be documented to the approving official(s) who granted the oral authorization as soon as practicable, but not more than five (5) business days after granting oral authorization.

(U//FOUO) The DIOG prohibits the use of control files or administrative files to document investigative activity. (See DIOG Appendix J)

8.6.2 (U) EFFECTIVE DATE

(U//FOUO) The effective date of the Enterprise Investigation is the date the final approval authority (i.e., SC) approves the [redacted] If the Enterprise Investigation is opened on oral b7E

authority, the date on which the oral approval authority was granted is the effective date. See DIOG Section 3.4.2.2.

8.6.3 (U) APPROVAL REQUIREMENTS FOR OPENING AN ENTERPRISE INVESTIGATION

8.6.3.1 (U) EI OPENED BY A FIELD OFFICE WITH SECTION CHIEF APPROVAL

(U//FOUO) The opening of an Enterprise Investigation by an FBI field office requires the prior approval of the appropriate FBIHQ SC, as well as written notification to the United States Attorney's Office (USAO) and the Department of Justice (DOJ) as specified below.

8.6.3.2 (U) EI OPENED BY FBIHQ WITH SECTION CHIEF APPROVAL

(U//FOUO) The opening of an Enterprise Investigation by an FBIHQ division requires the prior approval of the appropriate FBIHQ SC, as well as written notification to the appropriate field office(s), USAO and DOJ as specified below

8.6.3.3 (U) SIM EI OPENED BY A FIELD OFFICE WITH SPECIAL AGENT IN CHARGE AND SECTION CHIEF APPROVAL

(U//FOUO) A SIM Enterprise Investigation opened by a field office requires prior CDC review, SAC and appropriate FBIHQ SC approval, and written notification to DOJ in the form of an LHM or similar documentation. The LHM or similar documentation for dissemination to DOJ must be submitted to the appropriate FBIHQ operational section within 15 calendar days following the opening. Additionally, the field office must notify the USAO, in writing, unless such notification is inappropriate under the circumstances (e.g., a public corruption Enterprise Investigation of a group that is personally close to the United States Attorney (USA)), or the matter is a counterintelligence or espionage investigation. (See CD PG for details concerning notice in counterintelligence and espionage investigations.) If notice is not provided to the USAO under the circumstances described above, the field office must explain those circumstances in the written notice to FBIHQ. The responsible FBIHQ operational section must notify, in writing, the appropriate DOJ Criminal Division or National Security Division (NSD) official as soon as practicable, but no later than 30 calendar days after the investigation is opened.

b7E

(U//FOUO)

Notice must be furnished as specified above.

8.6.3.4 (U) SIM EI OPENED BY FBIHQ WITH SECTION CHIEF APPROVAL

(U//FOUO) A SIM Enterprise Investigation opened by FBIHQ requires prior OGC review and SC approval, and written notification to DOJ and appropriate field office(s) in the form of an LHM or similar documentation. The LHM or similar documentation for dissemination to the field office(s) must be submitted within 15 calendar days following the opening.

Additionally, the FBIHQ operational unit must notify the appropriate USAO(s) in writing, unless such notification is inappropriate under the circumstances (e.g., a public corruption Enterprise Investigation of a group that is personally close to the USA), or the matter is a counterintelligence or espionage investigation. (See CD PG for details concerning notice in counterintelligence and espionage investigations.) If notice is not provided to the USAO under the circumstances described above, the FBIHQ operational unit must explain those circumstances in the written notice to the field office(s) and DOJ. The responsible FBIHQ operational section must notify, in writing, the appropriate DOJ Criminal Division or National Security Division (NSD) official as soon as practicable, but no later than 30 calendar days after the investigation is opened.

b7E

(U//FOUO) Notice must be furnished as specified above.

8.6.4 (U) NOTICE REQUIREMENTS

(U//FOUO) FBIHQ division PGs may require specific facts to be included in a field office request to open an Enterprise Investigation. At a minimum, the request must include whether the Enterprise Investigation is a SIM.

(U//FOUO) The responsible FBIHQ section must notify the DOJ NSD or the Organized Crime and Racketeering Section (OCRS) of the opening of an Enterprise Investigation by a field office or by FBIHQ, as soon as practicable but no later than 30 calendar days after the opening of the investigation.

(U//FOUO) For Enterprise Investigations that involve groups of persons who pose a national security threat, the responsible DOJ component for the purpose of notification and reports is the NSD. For Enterprise Investigations relating to a pattern of racketeering activity that does not involve a national security threat, the responsible DOJ component is the OCRS of the Criminal Division. (AGG-Dom, Part II.C.3)

(U) The Assistant Attorney General for National Security or the Chief of the OCRS, as appropriate, may at any time request the FBI to provide a report on the status of an Enterprise Investigation, and the FBI will provide such reports as requested. (AGG-Dom, Part II C.3.d)

8.6.5 (U) FILE REVIEW

(U//FOUO) Supervisory file reviews must be conducted at least once every 90 days in accordance with DIOG Section 3.4.4. File reviews for probationary agents must be conducted at least once every 60 days.

8.7 (U) AUTHORIZED INVESTIGATIVE METHODS IN AN ENTERPRISE INVESTIGATION

(U//FOUO) An Enterprise Investigation may only be opened and operated as a Full Investigation and is subject to the same requirements that apply to a Full Investigation. Therefore, the standards for opening or approving the use of investigative methods and the availability of investigative methods that may be used in an Enterprise Investigation are the same as set forth in Sections 7.8 and 7.9.

8.8 (U) SENSITIVE INVESTIGATIVE MATTERS (SIM) IN ENTERPRISE INVESTIGATIONS

(U//FOUO) [redacted] b7E

DIOG Section 10 contains the required approval authority and factors to be considered when determining whether to conduct or approve a Full Enterprise Investigation involving a SIM.

8.8.1 (U) SIM CATEGORIES IN ENTERPRISE INVESTIGATIONS

(U//FOUO) A SIM is an investigative matter involving the activities of a domestic public official or domestic political candidate (involving corruption or a threat to the national security), religious or domestic political organization or individual prominent in such an organization, or news media, an academic nexus, or any other matter which, in the judgment of the official authorizing an investigation, should be brought to the attention of FBIHQ and other DOJ officials. (AGG-Dom, Part VII.N). As a matter of FBI policy, "judgment" means that the decision of the authorizing official is discretionary. DIOG Section 10 and/or the DIOG Appendix G – Classified Provisions define [redacted] b7E

8.8.2 (U) ACADEMIC NEXUS IN ENTERPRISE INVESTIGATIONS

(U//FOUO) [redacted]

A) (U//FOUO) [redacted]

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

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

(U//FOUO) b7E

8.9 (U) INTELLIGENCE COLLECTION (I.E., INCIDENTAL COLLECTION)

(U//FOUO) Intelligence that is responsive to PFI requirements, FBI national collection requirements and FBI field office collection requirements may be collected incidental to an Enterprise Investigation. b7E

(See DIOG Section 15.6.1.2 - Written Intelligence Products)

(U//FOUO)

8.10 (U) STANDARDS FOR APPROVING THE CLOSING OF AN ENTERPRISE INVESTIGATION

8.10.1 (U) STANDARDS

(U//FOUO) At the conclusion of an Enterprise Investigation, each of the following items must be documented in the closing communication (EC and/or LHM):

A) (U//FOUO) A summary of the results of the investigation;

B) (U//FOUO) Whether logical and reasonable investigation was completed;

C) (U//FOUO) Whether all investigative methods initiated have been completed and/or discontinued;

D) (U//FOUO) Whether all leads set have been completed and/or discontinued;

E) (U//FOUO) Whether all evidence has been returned, destroyed or retained in accordance with evidence policy; and

F) (U//FOUO) A summary statement of the basis on which the Enterprise Investigation will be closed, and selection of the appropriate closing status:

1) (U//FOUO) C-4: Administrative Closing, which includes:

a) (U//FOUO) No further investigation is warranted because logical investigation and/or leads have been exhausted, and the investigation to date did not identify a criminal violation or a priority threat to the national security

b) (U//FOUO) Investigation assigned a new file number, or

c) (U//FOUO) Investigation consolidated into a new file number or an existing file number.

2) (U//FOUO) C-6: Other Closing, which includes:

a) (U//FOUO) Enterprise Investigation has been completed; or

b) (U//FOUO) Any other type of closing

8.10.2 (U) APPROVAL REQUIREMENTS TO CLOSE

(U//FOUO) The appropriate closing supervisor described below must review and approve the closing communication (as described in Section 8.10.1) to ensure it contains the above-required information and sufficient details of the investigation on which to base the decision to close the Enterprise Investigation. The closing supervisor must note on the closing document "C," the closing status using 4 or 6 (e.g., C-4 or C-6) and the closing date. Although there is no limit on the duration of an Enterprise Investigation, the investigation must be closed upon all investigative activity being exhausted. The appropriate closing supervisors are:

A) (U//FOUO) ***Opened by a Field Office with FBIHQ SC Approval:*** Closing an Enterprise Investigation opened by a field office requires the prior approval of the appropriate FBIHQ SC.

B) (U//FOUO) ***Opened by FBIHQ:*** Closing an Enterprise Investigation opened by FBIHQ requires approval from the appropriate SC and notification to the appropriate field office.

C) (U//FOUO) ***SIM Opened by a Field Office with FBIHQ SC Approval:*** Closing an Enterprise Investigation opened by a field office involving a sensitive investigative matter requires approval from the appropriate FBIHQ SC.

(U//FOUO) ***SIM Opened by FBIHQ:*** Closing an Enterprise Investigation opened by FBIHQ involving a sensitive investigative matter requires approval from the SC, and written notification to the appropriate field office.

8.11 (U) OTHER PROGRAM SPECIFIC INVESTIGATIVE REQUIREMENTS

(U//FOUO) To facilitate compliance with investigative program-specific requirements, the FBI employee should consult the relevant division's PG to ascertain any program-specific requirements. FBIHQ division PGs, however, may not contradict, alter or otherwise modify the standards established in the DIOG.

This Page is Intentionally Blank.

9 (U) FOREIGN INTELLIGENCE

9.1 (U) OVERVIEW

(U) **Foreign Intelligence defined:** Foreign intelligence is "information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorists." A "Foreign Intelligence Requirement" is a collection requirement issued under the authority of the Director of National Intelligence (DNI) and accepted by the FBI Directorate of Intelligence (DI). Additionally, the President, a United States Intelligence Community (USIC) office designated by the President, the Attorney General, Deputy Attorney General, or other designated Department of Justice (DOJ) official may levy a foreign intelligence requirement on the FBI. Foreign intelligence collection by the FBI is based upon requirements.

(U//FOUO) Foreign intelligence requirements issued by one of the parties listed above and accepted by the FBI DI will fall into one of two categories: (i) those that address national security issues that are within the FBI's core national security mission (FBI collection requirements); and (ii) information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, foreign persons, or international terrorists which are not within the FBI's core national security mission (PFI Collection Requirements).

(U//FOUO) Requirements which fall into the first category may correspond to FBI national collection requirements as defined in DIOG Section 5.12. FBI national collection requirements are addressed in properly authorized Assessments (See DIOG Section 5.6.3.5) or Predicated Investigations. (See the Intelligence Policy Implementation Guide (IPG) for specific requirements.)

(U//FOUO) Requirements which fall into the second category are known as Positive Foreign Intelligence (PFI) Collection Requirements and may only be addressed under the authorities described in this section. Type 6 Assessments opened for the purpose of determining whether a field office has the ability to collect on a PFI Collection Requirement (See DIOG Section 5.6.3.5), and Full Investigations opened for the specific purpose of collecting on PFI Collection Requirements must be predicated on an established PFI Collection Requirement that has been accepted and approved by the FBIHQ Directorate of Intelligence (DI) – Domain Collection and HUMINT Management Section (DCHMS), Domain Collection Program Management Unit (DCPMU) UC. Preliminary Investigations for the sole purpose of collecting on PFI requirements are not authorized by the AGG-Dom. [redacted] A Full PFI Investigation opened for the intended purpose of collecting on PFI requirements must be approved by the DCPMU Unit Chief (UC). A Full PFI Investigation cannot be opened on oral authority. b7E

(U//FOUO) "The general guidance of the FBI's foreign intelligence collection activities by DNI-authorized requirements does not limit the FBI's authority to conduct investigations supportable on the basis of its other authorities—to investigate federal crimes and threats to the national security—in areas in which the information sought also falls under the definition of foreign

intelligence." (Attorney General's Guidelines for Domestic FBI Operations (AGG-Dom), Introduction A.3) Accordingly, the AGG-Dom authorizes the collection of foreign intelligence incidental to predicated criminal, counterintelligence, counterterrorism, cyber, and weapons of mass destruction investigations. b7E

See DIOG Sections 5.2 and 7.5.A and B.

(U//FOUO) A Full PFI Investigation can be opened based solely on a PFI Collection Requirement. The authorized purpose (the PFI Collection requirement) must exist and have been accepted by the FBI.

(U) *Examples:*

A) (U//FOUO)

B) (U//FOUO) b7E

(U//FOUO) FBIHQ DI provides specific guidance in its IPG regarding FBI national collection requirements, FBI field office collection requirements, and PFI requirements.

9.2 (U) Purpose and Scope

(U//FOUO) As stated above, foreign intelligence is "information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorists." The collection of positive foreign intelligence extends the sphere of the FBI's information-gathering activities beyond federal crimes and threats to the national security and permits the FBI to seek information regarding a broader range of matters relating to foreign powers, organizations, or persons that may be of interest to the conduct of the United States' foreign affairs. (AGG-Dom, Introduction A.3)

(U//FOUO) While employees may collect positive foreign intelligence in already opened Assessments and Predicated Investigations (incidental collection), this section is focused on the policies and procedures that govern opening and managing Full Investigations for the specific purpose of collecting on PFI Collection Requirements published by the DI. DIOG Section 5.6.3.4 governs opening and managing Type 6 Assessments.

9.3 (U) CIVIL LIBERTIES AND PRIVACY

(U) Because the authority to collect positive foreign intelligence pursuant to PFI Collection Requirements enables the FBI to obtain information pertinent to the United States' conduct of its foreign affairs, even if that information is not related to criminal activity or threats to the national security, the information collected may concern lawful activities. Accordingly, **the FBI must operate openly and consensually with an US Person (USPER),** to the extent practicable, when collecting positive foreign intelligence. (AGG-Dom, Introduction A.3)

(U) The pursuit of legitimate investigative goals without infringing upon the exercise of constitutional freedoms is a challenge that the FBI meets through the application of sound judgment and discretion.

(U) No investigative activity, including the collection of positive foreign intelligence pursuant to PFI Collection Requirements, may be taken solely on the basis of activities that are protected by the First Amendment or on the race, ethnicity, national origin or religion of the subject or a combination of only those factors. In order to take action intentionally to collect positive foreign intelligence, an FBI employee must open a Full Investigation that is predicated on a PFI requirement.

(U) The AGG-Dom present investigators with a number of authorized investigative methods in the conduct of a Full Investigation to collect positive foreign intelligence. Considering the effect on the privacy and civil liberties of individuals and the potential to damage the reputation of individuals, some of these investigative methods are more intrusive than others. The least intrusive method if reasonable based upon the circumstances of the investigation is to be used, but the FBI must not hesitate to use any lawful method consistent with the AGG-Dom. For further explanation of the least intrusive method refer to DIOG Section 4.

(U) Moreover, when collecting positive foreign intelligence, as part of a Full Investigation predicated on a PFI requirement, the FBI must operate openly and consensually with an USPER, to the extent practicable.

(U) By emphasizing the use of the least intrusive means to collect positive foreign intelligence and by emphasizing the need to operate openly and consensually with an USPER, to the extent practicable, FBI employees can effectively execute their duties while mitigating the potential negative impact on the privacy and civil liberties of all people encountered as part of the collection. This principle is not intended to discourage FBI employees from seeking relevant and necessary positive foreign intelligence, but rather is intended to make sure FBI employees choose the least intrusive—but still reasonable based upon the circumstances of the investigation – from the available options to obtain the information.

(U) The Privacy Act may not exempt from disclosure information the FBI collects during Positive Foreign Intelligence Assessments and investigations to qualified U.S. citizens or lawfully admitted permanent residents when personally identifying information about such persons resides in those files. FBI employees should therefore be particularly vigilant about properly classifying any such information and avoiding unnecessary references to, and the documentation of, identifying information about U.S. citizens and lawfully admitted permanent residents in Positive Foreign Intelligence files.

9.4 (U) LEGAL AUTHORITY

(U) The FBI's legal authority to collect positive foreign intelligence derives from a mixture of administrative and statutory sources. (See E.O. 12333; 50 U.S.C. §§ 401 et seq.; 50 U.S.C. §§ 1801 et seq.; 28 U.S.C. § 532 note [incorporates the Intelligence Reform and Terrorism Protection Act, P.L. 108-458 §§ 2001-2003]). In collecting positive foreign intelligence, the FBI will be guided by collection requirements issued under the authority of the DNI, including the National Intelligence Priorities Framework and the National Human Intelligence (HUMINT) Collection Directives, or any successor directives issued under the authority of the DNI and accepted by FBIHQ DI (PFI Collection Requirements).

9.4.1 (U) FULL INVESTIGATION ACTIVITIES

(U//FOUO) As discussed in Section 7 of the DIOG, the AGG-Dom cites three predication circumstances warranting a Full Investigation, one of which specifically applies to the collection of positive foreign intelligence: "The Full Investigation may obtain foreign intelligence that is responsive to a [positive] foreign intelligence requirement."

(U//FOUO) A PFI investigation may only be commenced if the Office of the DNI has levied a foreign intelligence collection requirement on the FBI and the DI has accepted the requirement as one to which the FBI will endeavor to respond to as part of its PFI Program (i.e., PFI Collection Requirements). The FBI is authorized to open 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.

9.5 (U) GENERAL REQUIREMENTS AND FBIHQ STANDARDS FOR APPROVING THE OPENING OF POSITIVE FOREIGN INTELLIGENCE INVESTIGATIONS

9.5.1 (U) GENERAL REQUIREMENTS AND PROGRAM RESPONSIBILITIES

(U//FOUO) The DCHMS is responsible for promulgating FBI policy and oversight of the Foreign Intelligence Collection Program (FICP). DCHMS, DCPMU will provide notice to the DOJ NSD upon the opening of a positive foreign intelligence Full Investigation. To ensure that all positive foreign intelligence collection is focused on authorized PFI Collection Requirements, only DCPMU may approve the opening of a Full Investigation [redacted] b7E
[redacted] Field offices must request, by EC to the DCPMU Unit Chief (UC) approval to open Full Investigations to collect on PFI Collection Requirements.

(U//FOUO) [redacted]

(U//FOUO) The DIOG prohibits the use of control files or administrative files to document investigative activity. (See DIOG Appendix J)

9.5.2 *(U) Standards For Opening a Full Investigation to Collect Positive Foreign Intelligence*

(U//FOUO) Before opening or approving a Full Investigation for the purpose of collecting PFI, the approving official must determine whether:

A) (U//FOUO) The FBI DI has established an PFI Collection Requirement for opening a Full Investigation;

B) (U//FOUO) The Full Investigation is not based solely on the exercise of First Amendment activities or on the race, ethnicity, national origin or religion of the subject or a combination of only such factors; and

C) (U//FOUO) The Full Investigation is an appropriate use of personnel and financial resources.

(U//FOUO) Additional policies regarding Predicated Investigation involving any foreign ambassador, foreign official, foreign student or exchange visitor, protected persons or premises as a subject may be found in DIOG Appendix G [No Foreign Policy Objection (NFPO)].

9.6 (U) Opening Documentation, Approval, Effective Date, and File Review

9.6.1 *(U) Opening by a Field Office With FBIHQ DCPMU UC Approval or Opening by FBIHQ*

(U//FOUO) The predication for a Full PFI Investigation must be documented in the opening electronic communication (EC). A Full PFI Investigation may not be opened on oral authority.

9.6.1.1 (U) Approval to Open a Full PFI Investigation

(U//FOUO) **Opened by a Field Office or Opened by FBIHQ:** DCPMU UC will approve the opening of a Full Investigation based on PFI Collection Requirements.

9.6.1.1.1 (U) Effective Date

(U//FOUO) **Opened by a Field Office or Opened by FBIHQ:** The effective date of the Full Investigation is the date the DCPMU UC approves the EC [redacted] b7E

[redacted]

9.6.1.2 (U) Approval to Open a Full PFI Investigation Involving a Sensitive Investigative Matter (SIM)

(U//FOUO) The opening of a Full PFI Investigation involving a SIM:

9.6.1.2.1 (U) SIM Full PFI Investigation Opened by a Field Office

(U//FOUO) The opening in a field office of a Full Investigation to collect PFI involving a SIM must have prior Chief Division Counsel (CDC) review, and approval by the Special Agent in Charge (SAC) and the DCHMS Section Chief (SC) [redacted] b7E

[redacted]

[redacted] b7E

(U//FOUO) [redacted] Notice must be provided to DOJ as indicated above.

9.6.1.2.2 (U) SIM FULL PFI INVESTIGATION OPENED BY FBIHQ

(U//FOUO) The opening by FBIHQ of a Full Investigation to collect PFI involving a SIM must have prior OGC review, and approval by the DCHMS SC. [redacted] b7E

(U//FOUO) [redacted]

9.6.1.2.3 (U) EFFECTIVE DATE

(U//FOUO) **Opened by a Field Office or Opened by FBIHQ:** The effective date of the Full Investigation involving a SIM is the date the DCHMS SC approves the EC [redacted] b7E

9.6.2 (U) NOTICE TO DOJ

9.6.2.1 (U) FOR A FULL PFI INVESTIGATION

(U//FOUO) Notice to DOJ is required when a Full Investigation to collect information responsive to a foreign intelligence requirement is opened. Notice must be forwarded from DCHMS, DCPMU to the DOJ NSD as soon as practicable but no later than 30 calendar days after the opening of the investigation. (AGG-Dom, Part II.B.5) For Full PFI Investigations that are a SIM, see DIOG Section 9.6.1.2 above.

9.6.3 (U) DURATION

(U//FOUO) A Full PFI Investigation may continue for as long as necessary until the requirement is met, or the investigation concludes they cannot satisfy the requirement.

9.6.4 (U) FILE REVIEW

9.6.4.1 (U) FULL INVESTIGATIONS

(U//FOUO) Supervisory file reviews of a Full PFI Investigation must be conducted at least every 90 days in accordance with DIOG Section 3.4.4. File reviews for probationary agents must be conducted at least every 60-days.

9.6.5 (U) ANNUAL LETTERHEAD MEMORANDUM

9.6.5.1 (U) FIELD OFFICE RESPONSIBILITY

(U//FOUO) All FIGs must submit an annual report on each Full PFI Investigation that was open for any period of time during the previous calendar year. This report is due to FBIHQ DCHMS no later than January 30th of the calendar year following each year during which a Full Investigation is open and must include the following:

A) (U//FOUO) The PFI requirement to which the investigation was responding;

B) (U//FOUO) All methods of collection used;

C) (U//FOUO) All Sensitive Investigative Matters encountered;

D) (U//FOUO) A list of all IIRs by number issued based on information collected during the investigation;

E) (U//FOUO) A summary of the PFI collected; and

F) (U//FOUO) The date the Full Investigation was opened and, if applicable, the date it was closed.

(U//FOUO) These reports should be submitted by EC. The EC must be uploaded into ACS as designated in the IPG.

9.6.5.2 (U) FBIHQ RESPONSIBILITY

(U//FOUO) DCHMS must compile data from each field office regarding the scope and nature of the prior year's PFI collection program. No later than April 1st of each year, the DCHMS must submit a comprehensive report of all activity described above to DOJ NSD. The report must include the following information:

A) (U//FOUO) The PFI requirement to which the investigations were responding;

B) (U//FOUO) All Sensitive Investigative Matters encountered; and

C) (U//FOUO) The date all Full Investigation were opened and closed (if applicable).

9.7 (U) Standards for Opening or Approving the Use of an Authorized Investigative Method in a Full Positive Foreign Intelligence Investigation

(U//FOUO) Prior to opening or approving the use of an investigative method in a Full Investigation for the purpose of collecting positive foreign intelligence pursuant to a PFI Collection Requirement, an FBI employee or approving official must determine whether:

A) (U//FOUO) The use of the particular investigative method is likely to further the authorized purpose of the Full Investigation;

B) (U//FOUO) The investigative method selected is the least intrusive method, if reasonable based upon the circumstances of the investigation and, if taken relative to an US person (USPER), the method involves open and consensual activities, to the extent practicable;

C) (U//FOUO) Open and consensual activity would likely be successful (if it would, covert non-consensual contact with an USPER may not be approved); and

D) (U//FOUO) The investigative method is an appropriate use of personnel and financial resources.

9.8 (U) Authorized Investigative Methods in a Full Positive Foreign Intelligence Investigation

(U//FOUO) Prior to opening or approving the use of an investigative method, an FBI employee and approving official must apply the standards as provided in DIOG Section 9.7. With the exceptions noted below, all lawful methods may be used during a Full Investigation to collect positive foreign intelligence pursuant to PFI Collection Requirements. If actions are to be taken with respect to an USPER, the method used must be open and consensual, to the extent practicable.

(U) See DIOG Section 18 for a complete description of the following methods that may be used in Full PFI Investigations. The methods are:

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)

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) Trash Covers (Searches that do not require a warrant or court order). (Section 18.6.12)

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

(U//FOUO) [redacted] b7E

(U//FOUO) See the classified provisions in Appendix G for additional information.

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

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

M)(U) Polygraph examinations. (Section 18.6.11)

N) (U) Undercover Operations (Section 18.6.13)

O) (U//FOUO) Pen registers and trap/trace devices for non-USPERs using FISA. (See Section 18.6.9)

P) (U) Electronic surveillance using FISA or E.O. 12333. (See Section 18.7.3)

Q) (U//FOUO) Searches – with a warrant or court order using FISA or E.O. 12333 § 2.5. The DIOG classified Appendix G provides additional information regarding certain searches. (AGG-Dom, Part V.A.12) (See Section 18.7.1)

R) (U) FISA Title VII - Acquisition of positive foreign intelligence information. (See Section 18.7.3)

S) (U//FOUO) FISA Order for business records (for records relating to a non-USPER only). (See Section 18.6.7)

9.9 (U) Investigative Methods Not Authorized During A Full Positive Foreign Intelligence Investigation

(U//FOUO) The following investigative methods are not permitted to be used for the purpose of collecting positive foreign intelligence pursuant to PFI Collection Requirements:

A) (U//FOUO) National Security Letters (15 U.S.C. §§ 1681u, 1681v; 18 U.S.C. § 2709; 12 U.S.C. § 341[a][5][A]; 50 U.S.C. § 436). (Section 18.6.6)

B) (U//FOUO) FISA Order for business records (for records relating to an USPER). (Section 18.6.7)

C) (U//FOUO) Pen registers and trap/trace devices in conformity with FISA (on an USPER). (Section 18.6.9)

D) (U//FOUO) Pen registers and trap/trace devices in conformity with chapter 206 of 18 U.S.C. §§ 3121-3127. (Section 18.6.9)

E) (U//FOUO) Mail covers. (Section 18.6.10)

F) (U//FOUO) Grand jury subpoenas. (Section 18.6.5)

G) (U//FOUO) Administrative subpoenas. (Section 18.6.4)

H) (U//FOUO) Stored wire and electronic communications and transactional records. (Section 18.6.8)

9.10 (U) SENSITIVE INVESTIGATIVE MATTERS (SIM) IN A FULL POSITIVE FOREIGN INTELLIGENCE INVESTIGATION

(U//FOUO) The title/caption of the opening or subsequent EC for a Full Investigation for the collection of PFI involving a SIM must contain the words "Sensitive Investigative Matter." DIOG Section 10 contains the required approval authorities and factors to be considered relative to a Predicated Investigation involving a SIM.

9.10.1 (U) SENSITIVE INVESTIGATIVE MATTERS (SIM)

(U//FOUO) A SIM is an investigative matter involving the activities of a domestic public official or domestic political candidate (involving corruption or a threat to the national security), religious or domestic political organization or individual prominent in such an organization, or news media, an academic nexus, or any other matter which, in the judgment of the official authorizing an investigation, should be brought to the attention of FBIHQ and other DOJ officials. (AGG-Dom, Part VII.N.) As a matter of FBI policy, "judgment" means that the decision of the authorizing official is discretionary. DIOG Section 10 and/or the classified provisions in DIOG Appendix G define domestic public official, political candidate, religious or political organization or individual prominent in such an organization, and news media.

(U//FOUO) All Full PFI Investigations involving a SIM must be reviewed by the CDC/OGC, approved by the SAC and the DCHMS SC.

9.10.2 (U) ACADEMIC NEXUS

(U//FOUO)

A)

B)

b7E

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

(U//FOUO) in DIOG Appendix G.

9.11 (U) RETENTION OF INFORMATION

(U//FOUO) DCHMS must maintain a database or records systems that permits the prompt retrieval of the status of each positive foreign intelligence collection Full Investigation (open or closed), the dates of opening and closing, and the basis for the Full Investigation.

9.12 (U//FOUO) STANDARDS FOR APPROVING THE CLOSING OF A FULL POSITIVE FOREIGN INTELLIGENCE INVESTIGATION

9.12.1 (U) STANDARDS

(U//FOUO) At the conclusion of a Full positive foreign intelligence Investigation, each of the following items must be documented in the closing communication (EC and/or LHM):

A) (U//FOUO) A summary of the results of the investigation;

B) (U//FOUO) Whether logical and reasonable investigation was completed (i.e. the matter acquired the positive foreign intelligence information sought);

C) (U//FOUO) Whether all investigative methods initiated have been completed and/or discontinued;

D) (U//FOUO) Whether all leads set have been completed and/or discontinued;

E) (U//FOUO) Whether all evidence has been returned, destroyed or retained in accordance with evidence policy; and

F) (U//FOUO) A summary statement of the basis on which the foreign intelligence investigation will be closed, and the selection of C-4 for Administrative Closing, which includes:

1) (U//FOUO) No further investigation is warranted and/or leads have been exhausted;

2) (U//FOUO) Investigation assigned a new file number; or

3) (U//FOUO) Investigation consolidated into a new file number or an existing file number.

9.12.2 (U) APPROVAL REQUIREMENTS

(U//FOUO) The appropriate closing supervisor described below must review and approve the closing communication (as described in Section 9.12.1) to ensure it contains the above-required information and sufficient details of the investigation on which to base a decision to close the foreign intelligence investigation. The closing supervisor must note on the closing document "C" (for close), the closing status 4 (e.g., C-4), and the closing date. The appropriate closing supervisors are:

9.12.2.1 (U) OPENED BY A FIELD OFFICE WITH FBIHQ APPROVAL

(U//FOUO) Closing a Full PFI Investigation opened by a field office requires a written request from the FIG SSA and the approval of the DCPMU UC.

9.12.2.2 (U) OPENED BY FBIHQ

(U//FOUO) Closing a Full PFI Investigation opened by FBIHQ requires approval from the DCPMU UC and notification to the appropriate field office.

9.12.2.3 (U) SIM OPENED BY A FIELD OFFICE WITH FBIHQ APPROVAL

(U//FOUO) Closing a PFI Full Investigation opened by a field office involving a SIM requires approval from the SAC and the DCHMS SC.

9.12.2.4 (U) SIM OPENED BY FBIHQ

(U//FOUO) Closing a PFI Full Investigation opened by FBIHQ involving a SIM requires approval from the DCHMS SC, and written notification to the appropriate field office.

9.13 (U) OTHER PROGRAM SPECIFIC INVESTIGATION REQUIREMENTS

(U//FOUO) To facilitate compliance with investigative program-specific requirements, the FBI employee should consult the relevant division's PG to ascertain any program-specific requirements. However, FBIHQ division PGs may not contradict, alter or otherwise modify the standards established in the DIOG.

10 (U//FOUO) SENSITIVE INVESTIGATIVE MATTER (SIM) AND SENSITIVE OPERATIONS REVIEW COMMITTEE (SORC)

10.1 (U) SENSITIVE INVESTIGATIVE MATTERS (SIM)

10.1.1 (U) OVERVIEW

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

10.1.2 (U) PURPOSE, SCOPE, AND DEFINITIONS

10.1.2.1 (U) DEFINITION OF SENSITIVE INVESTIGATIVE MATTERS (SIM)

(U/FOUO) A sensitive investigative matter (SIM) is defined as an investigative matter involving the activities of a domestic public official or domestic political candidate (involving corruption or a threat to the national security), a religious or domestic political organization or individual prominent in such an organization, or the news media; an investigative matter having an academic nexus; or any other matter which, in the judgment of the official authorizing the investigation, should be brought to the attention of FBI Headquarters (FBIHQ) and other DOJ officials. (Attorney General's Guidelines for Domestic FBI Operations (AGG-Dom), Part VII.N.) As a matter of FBI policy, "judgment" means that the decision of the authorizing official is discretionary.

(U//FOUO) The phrase ***"investigative matter involving the activities of"*** is intended to focus on the behaviors and/or activities of the subject, target, or subject matter of the Assessment or Predicated Investigation. The phrase is generally not intended to include a witness or victim in the Assessment or Predicated Investigation. This definition does not, however, prohibit a determination that the status, involvement, or impact on a particular witness or victim would make the Assessment or Predicated Investigation a SIM under subsection 10.1.2.2.7 below.

10.1.2.2 (U) DEFINITIONS/DESCRIPTIONS OF SIM OFFICIALS AND ENTITIES

(U) Descriptions for each of the officials and entities contained in the SIM definition are as follows:

10.1.2.2.1 (U) DOMESTIC PUBLIC OFFICIAL

(U/FOUO) A domestic public official is an elected official or an appointed official serving in a judicial, legislative, management, or executive-level position in a Federal, state, local, or tribal government entity or political subdivision thereof. A matter involving a domestic public official is a SIM if the Assessment or Predicated Investigation involves corruption or a threat to the national security.

(U//FOUO) This definition is intended to exclude lower level positions and most line positions, such as a patrol officer or office secretary from the SIM category, but it does include supervisory personnel (e.g., police Sergeant or Lieutenant). The SIM definition also eliminates the "position of trust" language.

10.1.2.2.2 (U) Domestic Political Candidate

(U/FOUO) A domestic political candidate is an individual who is seeking election to, or nomination for election to, or who has authorized others to explore on his or her behalf the possibility of election to an office in a federal, state, local or tribal governmental entity or political subdivision thereof. As with domestic public officials, a matter involving a political candidate is a SIM if the Assessment or Predicated Investigation involves corruption or a threat to the national security.

10.1.2.2.3 (U) Domestic Political Organization or Individual Prominent in such an Organization

(U/FOUO

b7E

10.1.2.2.4 (U) Religious Organization or Individual Prominent in such an Organization

(U//FOUO

b7E

10.1.2.2.5 (U) Member of the News Media or a News Organization

(U/FOUO)

b7E

(U//FOUO)

(U//FOUO) Examples of news media entities include television or radio stations broadcasting to the public at large and publishers of newspapers or periodicals that make their products available to the public at large in print form or through an Internet distribution. A freelance journalist may be considered to be a member of the media if the journalist has a contract with the news entity or has a history of publishing content. Publishing a newsletter or operating a website does not by itself qualify an individual as a member of the media. Businesses, law firms, and trade associations offer newsletters or have websites; these are not considered news media. As the term is used in the DIOG, "news media" is not intended to include persons and entities that simply make information available. Instead, it is intended to apply to a person or entity that gathers information of potential interest to a segment of the general public, uses editorial skills to turn raw materials into a distinct work, and distributes that work to an audience, as a journalism professional.

(U//FOUO) If there is doubt about whether a particular person or entity should be considered part of the "news media," the doubt should be resolved in favor of considering the person or entity to be the "news media."

(U//FOUO) See the classified provisions in DIOG Appendix G for additional guidance on SIMs.

10.1.2.2.6 (U) ACADEMIC NEXUS

b7E

(U//FOUO)

A) (U//FOUO)

B) (U//FOUO)

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

b7E

(U//FOUO)

10.1.2.2.7 (U) OTHER MATTERS

(U//FOUO) Any matter that in the judgment of the official authorizing an investigation should be brought to the attention of FBIHQ and other DOJ officials is also a SIM. As a matter of FBI policy, "judgment" means that the decision of the authorizing official is discretionary.

10.1.3 (U) FACTORS TO CONSIDER WHEN OPENING OR APPROVING AN INVESTIGATIVE ACTIVITY INVOLVING A SIM

(U//FOUO) In addition to the standards for approving investigative activity in Sections 5, 6, 7, 8 and 9, the following factors should be considered by (i) the FBI employee who seeks to open an Assessment or Predicated Investigation involving a SIM, as well as by the (ii) Chief Division Counsel (CDC) or Office of the General Counsel (OGC) when reviewing such matters, and (iii) the approving official when determining whether the Assessment or Predicated Investigation involving a SIM should be authorized:

A) (U//FOUO) Seriousness/severity of the violation/threat;

B) (U//FOUO) Significance of the information sought to the violation/threat;

C) (U//FOUO) Probability that the proposed course of action will be successful;

D) (U//FOUO) Risk of public exposure, and if there is such a risk, the adverse impact or the perception of the adverse impact on civil liberties and public confidence; and

E) (U//FOUO) Risk to the national security or the public welfare if the proposed course of action is not approved (i.e., risk of doing nothing).

(U//FOUO) In the context of a SIM, particular care should be taken when considering whether the planned course of action is the least intrusive method if reasonable based upon the circumstances of the investigation.

10.1.4 (U) OPENING DOCUMENTATION, APPROVAL, NOTICE, AND CHANGE IN SIM STATUS

(U//FOUO) b7E

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

10.1.4.1 (U) REVIEW AND APPROVAL OF SIM ASSESSMENTS BY A FIELD OFFICE

10.1.4.1.1 (U) TYPE 1 & 2 ASSESSMENTS

(U//FOUO) An FBI employee may open a Type 1 & 2 Assessment, as described in Section 5.6.3.1, without prior supervisory approval. A Type 1 & 2 Assessment involving a SIM must be reviewed by the CDC and approved by the Special Agent-in-Charge (SAC) as soon as practicable, but no later than five (5) business days after the opening to authorize the Assessment to continue.

10.1.4.1.2 (U) TYPE 3 AND 4 ASSESSMENTS

(U//FOUO) An FBI employee must obtain the following review and approval to open a Type 3 and 4 Assessment as a SIM: CDC review and SAC approval. If a SIM arises after the opening of a Type 3 or 4 Assessment, the Assessment may continue, but the matter must be reviewed by the CDC and approved by the SAC as soon as practicable, but no later than five (5) business days after the SIM arises to authorize the Assessment to continue. (See DIOG Sections 5.6.3.2.4 and 5.6.3.3.4.)

10.1.4.1.3 (U) TYPE 5 ASSESSMENTS

(U//FOUO) An FBI employee must obtain the SAC's prior approval to open a Type 5 Assessment on a sensitive potential confidential human source (CHS). If it is determined after the opening of a Type 5 Assessment that the individual is a sensitive potential CHS, the Assessment may continue, but the matter must be approved by the SAC as soon as practicable, but no later than five (5) business days after this determination is made to authorize the Assessment to continue. (See DIOG Section 5.6.3.4.4.1)

10.1.4.1.4 (U) TYPE 6 ASSESSMENTS

(U//FOUO) An FBI employee must obtain the following review and approval to open a Type 6 Assessment as a SIM: CDC review, SAC approval, and Domain Collection and HUMINT Management Section (DCHMS) Section Chief (SC) approval. If the SIM arises after the opening of a Type 6 Assessment, the Assessment may continue, but the matter must be reviewed by the CDC and approved by the SAC and DCHMS SC as soon as practicable, but no later than five (5) business days after the SIM arises to authorize the Assessment to continue. (See DIOG Section 5.6.3.5.4)

(U//FOUO) FBIHQ must receive notice and approve all Type 6 Assessments whether or not they involve a SIM.

10.1.4.2 (U) NOTICE FOR SIM ASSESSMENTS BY A FIELD OFFICE

(U//FOUO) Notice for SIM Assessments—There is no requirement to notify FBIHQ, DOJ, or the United States Attorney (USA) of the opening of an Assessment involving a SIM. (AGG-Dom, Part II.B.5.a)

10.1.4.3 (U) REVIEW AND APPROVAL OF SIM PREDICATED INVESTIGATIONS BY A FIELD OFFICE

10.1.4.3.1 (U) PREDICATED INVESTIGATIONS INVOLVING A SIM

(U//FOUO) CDC review and SAC approval. (See Sections 6.10 and 7.10)

10.1.4.3.2 (U) ENTERPRISE INVESTIGATIONS INVOLVING A SIM

(U//FOUO) CDC review, SAC approval, and SC approval. (See Section 8.6)

10.1.4.3.3 (U) POSITIVE FOREIGN INTELLIGENCE FULL INVESTIGATIONS INVOLVING A SIM

(U//FOUO) CDC review, SAC approval, and DCHMS SC approval. (See DIOG Sections 9.6 and 9.10)

10.1.4.4 (U) NOTICE FOR SIM PREDICATED INVESTIGATIONS BY A FIELD OFFICE

10.1.4.4.1 (U) NOTICE FOR SIM PREDICATED INVESTIGATIONS

(U//FOUO) The field office must provide written notification (EC and a disseminable LHM) to the responsible FBIHQ unit and section within 15 calendar days after the opening of a SIM Predicated Investigation. The field office also must notify the appropriate United States Attorney's Office (USAO), in writing, unless such notification is inappropriate under the circumstances (e.g., a public corruption investigation of a person who is personally close to the Unites States Attorney (USA), or the matter is a counterintelligence or espionage investigation. (See the CD PG for details concerning notice in counterintelligence and espionage investigations.) If notice is not provided to the USAO under the circumstances described above, the field office must explain those circumstances in the written notice to FBIHQ. The responsible FBIHQ section must notify, in writing, the appropriate DOJ Criminal Division official or NSD official. The notification must be made as soon as practicable but no later than 30 calendar days after the opening of the investigation. [redacted] b7E See the classified provisions in DIOG Appendix G for [redacted]

(U//FOUO) [redacted] b7E

10.1.4.4.2 (U) NOTICE FOR SIM ENTERPRISE INVESTIGATIONS

(U//FOUO) See DIOG Section 8.6 for notice requirements.

10.1.4.4.3 (U) NOTICE FOR SIM POSITIVE FOREIGN INTELLIGENCE FULL INVESTIGATIONS

(U//FOUO) See DIOG Section 9.9 for notice requirements.

10.1.4.5 (U) REVIEW AND APPROVAL OF SIM ASSESSMENTS OPENED BY FBIHQ

10.1.4.5.1 (U) TYPE 1 & 2 ASSESSMENTS

(U//FOUO) An FBI employee may open a Type 1 & 2 Assessment, as described in Section 5.6.3.1, without prior supervisory approval. An Assessment involving a SIM must be reviewed by the OGC and approved by the SC as soon as practicable, but no later than five (5) business days after the opening to continue the Assessment. [redacted] b7E

b7E

[redacted]

10.1.4.5.2 (U) TYPE 3 AND 4 ASSESSMENTS

(U//FOUO) An FBI employee must obtain the following reviews and prior approvals to open a Type 3 or 4 SIM Assessment: OGC review and SC approval [redacted]

b7E

[redacted]

10.1.4.5.3 (U) TYPE 5 ASSESSMENTS

(U//FOUO) An FBI employee must obtain his/her SC's approval to open a Type 5 Assessment on a sensitive potential CHS [redacted]

b7E

[redacted]

10.1.4.5.4 (U) TYPE 6 ASSESSMENTS

(U//FOUO)An FBI employee must obtain the following reviews and approvals to open a Type 6 Assessment as a SIM: OGC review and SC approval. [redacted]

b7E

[redacted]

10.1.4.6 (U) NOTICE REQUIREMENTS FOR SIM ASSESSMENTS BY FBIHQ

(U//FOUO) There is no requirement to notify DOJ or the United States Attorney of the opening of an Assessment involving a SIM (including opening a sensitive potential CHS). (AGG-Dom, Part II.B.5.a)

10.1.4.6.1 (U) REVIEW AND APPROVAL OF SIM PREDICATED INVESTIGATIONS BY FBIHQ

10.1.4.6.2 (U) PREDICATED INVESTIGATIONS INVOLVING A SIM

(U//FOUO) OGC review and SC approval. (See DIOG Sections 6.7 , 6.10; 7.7 and 7.10)

10.1.4.6.3 (U) ENTERPRISE INVESTIGATIONS INVOLVING A SIM

(U//FOUO) OGC review and SC approval. (See DIOG Sections 8.6)

10.1.4.6.4 (U) POSITIVE FOREIGN INTELLIGENCE FULL INVESTIGATIONS INVOLVING A SIM

(U//FOUO) OGC review and SC approval. (See DIOG Section 9.9)

10.1.4.7 (U) NOTICE FOR SIM PREDICATED INVESTIGATIONS BY FBIHQ

10.1.4.7.1 (U) NOTICE FOR SIM PREDICATED INVESTIGATIONS

(U//FOUO) The responsible FBIHQ section must provide written notification (EC and a disseminable LHM) to any appropriate field office within 15 calendar days after the opening of a SIM Predicated Investigation; the USAO, unless such notification is inappropriate under the circumstances, or the matter is a counterintelligence or espionage investigation (See the CD PG for details concerning notice in counterintelligence and espionage investigations.); and the appropriate DOJ Criminal Division official or NSD official, as soon as practicable, but no later than 30 calendar days after the opening of the investigation. If notice is not provided to the USAO under the circumstances described above, FBIHQ must explain those circumstances in the written notice to the field office(s) and DOJ. [redacted] known SIMs involved in the investigation. See the classified provisions in DIOG Appendix G for [redacted] b7E

(U//FOUO) [redacted] b7E

10.1.4.7.2 (U) NOTICE FOR SIM ENTERPRISE INVESTIGATIONS

(U//FOUO) See DIOG Section 8.6 for notice requirements.

10.1.4.7.3 (U) NOTICE FOR SIM FULL POSITIVE FOREIGN INTELLIGENCE INVESTIGATIONS

(U//FOUO) See DIOG Section 9.9 for notice requirements.

10.1.4.8 (U) CHANGE IN SIM STATUS

(U//FOUO) [redacted] b7E

10.1.4.8.1 (U) DOCUMENTATION

(U//FOUO) The FBI employee must:

A) (U//FOUO) ***In Type 1 & 2 Assessments:*** Submit an updated FD-71 or Guardian [redacted] The FD-71 or Guardian must be approved by the supervisor responsible for the Assessment, reviewed by the CDC, and approved by the SAC. No notice to FBIHQ is required. b7E

B) (U//FOUO) ***In Type 3 through 6 Assessments:***

1) (U//FOUO) Opened by a Field Office - Submit an EC (for Type 5 Assessments, an EC or a successor form in [redacted] that must be approved by the supervisor responsible for the Assessment, reviewed by the CDC, and approved by the SAC. No notice to FBIHQ is required. b7E

2) (U//FOUO) Opened by FBIHQ - Submit an EC that must be approved by the appropriate UC responsible for the investigation, reviewed by OGC, and approved by the SC.

C) (U//FOUO) ***Predicated Investigations:***

1) (U//FOUO) Opened by a Field Office - Submit an EC that must be approved by the supervisor responsible for the investigation, reviewed by the CDC, and approved by the SAC. For Predicated Investigations, notification must be provided to the same FBIHQ entities (appropriate Unit and Section) that received notice of the SIM.

2) (U//FOUO) Opened by FBIHQ - Submit an EC that must be approved by the appropriate UC responsible for the investigation, reviewed by OGC, and approved by the SC.

D) (U//FOUO) ***Enterprise Investigations:***

1) (U//FOUO) Opened by a Field Office - Submit an EC that must be approved by the supervisor responsible for the investigation, reviewed by the CDC, and approved by the SAC and the appropriate SC.

2) (U//FOUO) Opened by FBIHQ - Submit an EC that must be approved by the appropriate UC responsible for the investigation, reviewed by OGC, and approved by the SC.

E) (U//FOUO) ***Positive Foreign Intelligence Full Investigations:***

1) (U//FOUO) Opened by a Field Office - Submit an EC that must be approved by the appropriate supervisor, reviewed by the CDC, approved by the SAC and the appropriate DI UC.

2) (U//FOUO) Opened by FBIHQ - Submit an EC that must be approved by the appropriate UC responsible for the investigation, reviewed by OGC, and approved by the DI SC.

10.1.4.9 (U) CLOSING SIM INVESTIGATIONS

10.1.4.9.1 (U) SIM ASSESSMENTS CLOSED BY A FIELD OFFICE

A) (U//FOUO) ***Type 1 & 2 Assessments*** - These SIM Assessments must be closed on the FD-71 or FD-71a (Guardian) with approval of the supervisor responsible for the investigation and the SAC. (See DIOG Section 5.6.3.1)

B) (U//FOUO) ***Type 3, 4, and 5 Assessments*** - The closing EC (or successor form in [redacted] for Type 5 Assessments) must be approved by the supervisor responsible for the investigation and the SAC. (See DIOG Section 5.6.3.2, 3, and 4) b7E

C) (U//FOUO) ***Type 6 Assessments*** - The closing EC must be approved by the supervisor responsible for the investigation, SAC and the DI SC. (See DIOG Section 5.6.3.5)

10.1.4.9.2 (U) SIM PREDICATED INVESTIGATIONS CLOSED BY A FIELD OFFICE

(U//FOUO) The closing standards, approvals and notice requirements for SIM Predicated Investigations, including Enterprise Investigations and foreign intelligence Full Investigations, are specified in DIOG Sections 6.12; 7.12; 8.9; and 9.12 above.

10.1.4.9.3 (U) SIM ASSESSMENTS CLOSED BY FBIHQ

A) (U//FOUO) ***Type 1 & 2 Assessments*** - May be closed on the FD-71 or FD-71a (Guardian) with the approval of the UC responsible for the investigation and his/her SC.

B) (U//FOUO) ***Type 3, 4, and 5 Assessments*** - The closing EC (or successor form in [redacted] for Type 5 Assessments) must be approved by the UC responsible for the investigation and his/her SC. b7E

C) (U//FOUO) ***Type 6 Assessments*** - The closing EC must be approved by the DI UC responsible for the investigation and his/her DI SC.

10.1.4.9.4 (U) SIM PREDICATED INVESTIGATIONS CLOSED BY FBIHQ

(U//FOUO) The closing standards, approvals and notice requirements for SIM Predicated Investigations, including Enterprise Investigations and Full foreign intelligence investigations, are specified in DIOG Sections 6.12; 7.12; 8.9; and 9.12 above.

10.1.5 (U) DISTINCTION BETWEEN SIM AND SENSITIVE CIRCUMSTANCE IN UNDERCOVER OPERATIONS

(U//FOUO) The term "sensitive investigative matter," as used in the DIOG, should not be confused with the term "sensitive circumstance," as that term is used in undercover operations. "Sensitive circumstance" relates to an undercover operation requiring FBIHQ approval. A comprehensive list of sensitive circumstances for criminal activities is contained in the Attorney General's Guidelines on FBI Undercover Operations and in Section 18 of the DIOG. The Criminal Undercover Operations Review Committee (CUORC) and the [redacted] must review and approve undercover operations that involve sensitive circumstances. The policy for undercover operations is described in DIOG Section 18.6.13, the Field Guide for Undercover and Sensitive Operations (FGUSO), National Security Undercover Operations Policy Implementation Guide (NSUCOPG), and the FBIHQ operational division program implementation guides. b7E

10.1.6 (U) DISTINCTION BETWEEN SIM AND SENSITIVE UNDISCLOSED PARTICIPATION

(U//FOUO) The term "sensitive investigative matter," as used in the DIOG, should not be confused with "sensitive UDP (undisclosed participation)." The rules regarding "sensitive investigative matter" and "sensitive UDP" (see DIOG Section 16.2.3.5), while similar, must be applied independently. The SIM designation applies to the overall investigation of which FBI and DOJ officials should be aware due to potential public notoriety and sensitivity. Sensitive UDP, on the other hand, applies to participation by employees or CHSs in lawful organizations that are designated as sensitive. Sensitive UDP can occur in either SIM or non-SIM designated investigations because sensitive UDP focuses on the activity (UDP) - not on the type of investigation in which it is taking place. Certain investigative or intelligence activity, particularly in situations involving academic institutions or student groups, may be covered by one or both these rules. The following scenarios demonstrate how these policies are to be applied:

10.1.6.1 (U) SCENARIOS

(U/FOUO) [redacted] b7E

(U//FOUO) [redacted] b7E

(U/FOUO) [redacted] b7E

(U//FOUO [redacted] b7E

(U/FOUO) [redacted] b7E

(U/FOUO) [redacted] b7E

10.2 (U//FOUO) SENSITIVE OPERATIONS REVIEW COMMITTEE

(U//FOUO) At the request of the Director, a new joint DOJ/ FBI oversight committee, the Sensitive Operations Review Committee (SORC), has been established to review and monitor certain aspects of FBI investigative activities that are not within the purview of other oversight committees, particularly with regard to Assessments. The SORC is described as follows:

10.2.1 (U) MEMBERSHIP AND STAFFING

A) (U//FOUO) **Chair:** [redacted] b7E

B) (U) **Members:**

1) (U//FOUO) **FBI:** Assistant Directors or designated Deputy Assistant Directors for the [redacted] b7E and any other appropriate representative, given the issue presented to the SORC.

2) (U//FOUO) **DOJ:** Assistant Attorneys General of the [redacted] and any other appropriate representative, given the issue being considered by the SORC.

C) (U//FOUO) **Advisors:** The Unit Chief or a designee of the FBI's Corporate Policy Office (CPO) will serve as a policy advisor to the SORC. In addition, DOJ's Chief Privacy and Civil Liberties Officer or a designee will also serve as an advisor to the SORC.

D) (U//FOUO) **Staff:** The staff of the SORC shall be from the executive staffs of the Executive Assistant Directors of the NSB and the CCSB. Proposals from the NSB shall be handled by its executive staff; proposals from CCSB shall be handled by its executive staff. The staffs will be collectively referred to here as "SORC Staff." The SORC Staff is responsible for ensuring that FBI and DOJ members of the SORC have the information required to perform their SORC duties and are kept fully informed of process developments in matters reviewed by the SORC.

10.2.2 (U) FUNCTION

(U//FOUO) The SORC will review and provide recommendations to the Director on matters submitted, as described below.

10.2.3 (U) REVIEW AND RECOMMENDATION

(U//FOUO) The SORC shall review sensitive activities in the categories described below and provide recommendations to the Director, who shall be the approval authority:

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

(U//FOUO) [redacted]

B) (U//FOUO) [redacted]

C) (U//FOUO) [redacted]

D) (U//FOUO) b7E

E) (U//FOUO)

10.2.3.1 (U) Factors to Consider for Review and Recommendation

(U//FOUO) In addition to factors unique to the proposal being considered, the SORC will consider the following in determining whether to recommend that a proposed activity be approved:

A) (U//FOUO) b7E
B) (U//FOUO)
C) (U//FOUO)
D) (U//FOUO)
E) (U//FOUO)
F) (U//FOUO)
G) (U//FOUO)
H) (U//FOUO)
I) (U//FOUO)

10.2.3.2 (U) Process for Review and Recommendation b7E

(U//FOUO)

(U//FOUO)

b7E

A) (U//FOUO) The applicable FBIHQ operational

B) (U//FOUO) Upon receipt of the EC and the proposal, the

C) (U//FOUO prior to a scheduled SORC meeting, the SORC Staff must

D) (U//FOUO) SORC meetings are to be conducted with the expectation that

E) (U//FOUO) If there is no consensus among the SORC members

F) (U//FOUO) Once the SORC has made its recommendation, the SORC Staff

G) (U//FOUO) For each proposal, at the next SORC meeting the SORC Staff

10.2.4 (U) EMERGENCY AUTHORIZATION

(U//FOUO) When necessary to [redacted] SORC [redacted]

10.2.4.1 (U) NOTICE/OVERSIGHT FUNCTION OF SORC

(U//FOUO) To facilitate its ability to [redacted]

A) (U//FOUO) In a [redacted] any approval to task a [redacted]

B) (U//FOUO) In a [redacted] any [redacted]

C) (U//FOUO) In a [redacted]

D) (U//FOUO) In an [redacted] any [redacted]

E) (U//FOUO) In an [redacted] to obtain [redacted]

(U//FOUO) *Note*: [redacted] falling into any of the above-listed categories must be [redacted]

F) (U//FOUO) The SORC may [redacted] to provide it:

1) (U//FOUO) [redacted]

2) (U//FOUO) [redacted]

3) (U//FOUO) [redacted]

G) (U//FOUO) The SORC must [redacted] b7E

[redacted]

H) (U//FOUO [redacted] to the SORC as [redacted]

10.2.5 (U) LOGISTICS

(U//FOUO) The Executive Assistant Director for the NSB is responsible for all logistical support required for the proper functioning of the SORC (i.e., schedule meetings, provide place for meetings, draft agendas, record keeping and retention functions, all necessary communications, etc.). The CPO and the OGC will assist in establishing the logistical support required for the SORC.

11 (U) LIAISON ACTIVITIES AND TRIPWIRES

11.1 (U) OVERVIEW

(U//FOUO) FBI employees are encouraged to engage in liaison with the general public, private entities, and with local, state, federal, tribal, and foreign government agencies for the purpose of building partnerships. As part of our liaison, community outreach, or investigative/intelligence mission, FBI employees may also establish tripwires with public entities, private entities, and other governmental agencies. Liaison and tripwire initiatives are mutually beneficial for the FBI and the public not only because they help build cooperative relationships and educate about suspicious activities or potential threats, but also because they encourage the public to contact the FBI should they become aware of such suspicious activities or threats.

11.2 (U) PURPOSE AND SCOPE

(U//FOUO) The FBI is authorized to engage in liaison activities and tripwire. The procedures for liaison and setting tripwires, together with documentation and requirements for an Assessment or Predicated Investigation are set forth below.

11.3 (U) APPROVAL REQUIREMENTS FOR LIAISON AND TRIPWIRES

(U//FOUO) Conducting liaison activities or tripwire initiatives do not require approval or the opening of an Assessment or Predicated Investigation unless they use an investigative method set forth in DIOG Sections 18.5 – 18.7. Liaison and Tripwire initiatives may be conducted as part of an already-opened Assessment or Predicated Investigation.

11.3.1 (U) SCENARIO 1

(U//FOUO) An FBI employee makes contact with a chemical supply company to introduce himself/herself and educate the owner about the Bureau's investigative focus on the illegal use of precursor chemicals to make improvised explosive devices. The employee advises the owner to contact the FBI if he/she observes any unusual or suspicious purchases of certain precursor chemicals.

(U//FOUO) ***Response:*** Such a contact would not require approval or the opening of an Assessment or Predicated Investigation because no investigative methods are used to conduct this activity.

11.3.2 (U) SCENARIO 2

b7E

(U//FOUO)

(U//FOUO)

b7E

11.4 (U) DOCUMENTATION & RECORDS RETENTION REQUIREMENTS

(U//FOUO) The terms "liaison" and "tripwire" have been defined in various ways and may differ by FBIHQ division, program, or field office. Not every contact with a member of the public will be considered liaison activity or a tripwire initiative that needs to be documented. As stated above, employees are encouraged to engage and converse with the public as part of their routine FBI investigative and intelligence mission.

(U//FOUO) Often, however, these terms are used and/or defined in a formal policy or EC to accomplish a particular investigative or intelligence objective. When an employee is directed by a supervisor, FBI policy, or a FBIHQ division to establish a liaison relationship or set a tripwire, that directive, as well as the actions taken by the employee, must be documented with an FD-999. If an employee on his or her own initiative contacts a member of the public and subsequently determines the contact was a liaison or tripwire activity, the contact must be documented using the FD-999. Any questions regarding whether the employee's contact with the public should be documented as liaison or tripwire activities should be directed to the employee's supervisor. The intent of this section is to ensure that contacts with the public which are considered to be liaison activities or a tripwire initiatives be documented with the FD-999 into a single database system for tracking and reporting purposes.

(U//FOUO) When the FD-999 is used to document liaison activities or tripwire initiatives, it must be uploaded to file number 319X-HQ-A1487718. Copies of the FD-999 must also be filed as follows:

A) (U//FOUO) **No Investigative Methods Used:** If no investigative methods (DIOG Sections 18.5 - 18.7) are used in the liaison activity or tripwire, the FD-999 may be uploaded into an investigative file or control file.

B) (U//FOUO) **Investigative Methods Used:** If investigative methods (DIOG Sections 18.5-18.7) are used in the liaison activity or tripwire, the FD-999 must also be uploaded in one of the following:

1) (U//FOUO) an Assessment file;

2) (U//FOUO) a Predicated Investigation file;

3) (U//FOUO) a domestic police cooperation file (343 classification);

4) (U//FOUO) a foreign police cooperation file (163 classification); or

5) (U//FOUO) a technical assistance control file (if only technical assistance is provided).

12 (U) ASSISTANCE TO OTHER AGENCIES

12.1 (U) OVERVIEW

(U//FOUO) Part II of the Attorney General's Guidelines for Domestic FBI Operations (AGG-Dom) authorizes the FBI to conduct investigations in order to detect or obtain information about, and prevent and protect against, federal crimes and threats to the national security and to collect foreign intelligence. (See DIOG Section 2.) Section 12 does not apply to assistance the FBI may provide to other agencies while conducting joint investigations. In such instances, other sections of the DIOG dealing with Assessments and Predicated Investigations would apply.

(U//FOUO) Section 12 specifically addresses those situations in which the FBI has been requested or is seeking to provide assistance to other agencies and does not have an open Assessment or Predicated Investigation. Part III of the AGG-Dom, Assistance to Other Agencies, authorizes the FBI to provide investigative assistance to other federal, state, local or tribal, or foreign agencies when the investigation has the same objectives as Part II of the AGG-Dom or when the investigative assistance is otherwise legally authorized. Accordingly, FBI employees may provide assistance even if it is not for one of the purposes identified as grounds for an FBI investigation or Assessment if providing the assistance is otherwise authorized by law. For example, investigative assistance is legally authorized in certain contexts to state or local agencies in the investigation of crimes under state or local law, as provided in 28 U.S.C. § 540—felonious killing of state and local law enforcement officer; 28 U.S.C. § 540A—violent crime against travelers; 28 U.S.C. § 540B—serial killings, and to foreign agencies in the investigation of foreign law violations pursuant to international agreements. The FBI may use appropriate lawful methods in any authorized investigative assistance activity.

12.2 (U) PURPOSE AND SCOPE

(U) The FBI may provide investigative and technical assistance to other agencies as set forth below.

12.2.1 (U) INVESTIGATIVE ASSISTANCE

(U) The AGG-Dom permits FBI personnel to provide investigative assistance to:

A) (U) Authorized intelligence activities of other United States Intelligence Community (USIC) agencies;

B) (U) Any federal agency in the investigation of federal crimes, threats to the national security, foreign intelligence collection, or any other purpose that may be lawfully authorized;

C) (U) Assist the President in determining whether to use the armed forces pursuant to 10 U.S.C. §§ 331-33, when authorized by Department of Justice (DOJ), as described in Section 12.3.2.2.1.1, below;

D) (U) Collect information necessary to facilitate public demonstrations and to protect the exercise of First Amendment rights and ensure public health and safety, when authorized by DOJ and done in accordance with the restrictions described in Section 12.3.2.2.1.2, below;

E) (U) State or local agencies in the investigation of crimes under state or local law when authorized by federal law (e.g., 28 U.S.C. §§ 540—felonious killing of state and local law enforcement officer; 540A—violent crime against travelers; 540B—serial killings);

F) (U) State, local, or tribal agencies in the investigation of matters that may involve federal crimes or threats to national security, or for such other purposes as may be legally authorized;

G) (U) Foreign agencies in the investigations of foreign law violations pursuant to international agreements, and as otherwise set forth below, consistent with the interests of the United States (including national security interests) and with due consideration of the effect on any US Person (USPER); and

H) (U) The Attorney General has also authorized the FBI to provide law enforcement assistance to state or local law enforcement agencies when such assistance is requested by the governor of the state pursuant to 42 U.S.C. § 10501 (for example, federal law enforcement assistance following Hurricane Katrina). The Attorney General must approve any request for assistance under 42 U.S.C. § 10501.

(U) The procedures for providing investigative assistance, together with the standards, approval, notification, documentation, and dissemination requirements are set forth in Sections 12.3, 12.5, and 12.6 below.

12.2.2 (U) TECHNICAL ASSISTANCE

(U) The FBI is authorized to provide technical assistance to all duly constituted law enforcement agencies, other organizational units of the DOJ, and other federal agencies and to foreign governments (to the extent not prohibited by law or regulation). The procedures for providing technical, together with the approval, notification, documentation, and dissemination requirements are set forth in Sections 12.4, 12.5 and 12.6 below.

12.3 (U) INVESTIGATIVE ASSISTANCE TO OTHER AGENCIES - STANDARDS, APPROVALS AND NOTICE REQUIREMENTS

(U) The FBI may provide investigative assistance to other agencies by participating in joint operations and investigative activities with such agencies. (AGG-Dom, Part III.E.1)

(U//FOUO) Dissemination of information to other agencies must be consistent with Director of National Intelligence (DNI) directives, the AGG-Dom, DIOG Section 14, FBI Foreign Dissemination Manual, the Privacy Act of 1974, and any applicable memoranda of understanding/agreement (MOU/MOA), laws, treaties or other policies. (See Sections 12.5 and 12.6 below for documentation and dissemination of information requirements.)

12.3.1 (U) STANDARDS FOR PROVIDING INVESTIGATIVE ASSISTANCE TO OTHER AGENCIES

(U//FOUO) The determination whether to provide FBI assistance to other agencies is discretionary but may only occur if:

A) (U//FOUO) The assistance is within the scope authorized by the AGG-Dom, federal laws, regulations, or other legal authorities;

B) (U//FOUO) The investigation being assisted is not based solely on the exercise of First Amendment activities or on the race, ethnicity, national origin or religion of the subject or a combination of only these factors; and

C) (U//FOUO) The assistance is an appropriate use of FBI personnel and financial resources.

12.3.2 (U) AUTHORITY, APPROVAL AND NOTICE REQUIREMENTS FOR PROVIDING INVESTIGATIVE ASSISTANCE TO OTHER AGENCIES

(U//FOUO) Investigative assistance that may be furnished to other agencies is described below by agency type.

12.3.2.1 (U) INVESTIGATIVE ASSISTANCE TO UNITED STATES INTELLIGENCE COMMUNITY (USIC) AGENCIES

12.3.2.1.1 (U) AUTHORITY

A) (U//FOUO) The FBI may provide investigative assistance (including operational support) for authorized intelligence activities of other USIC agencies. (AGG-Dom, Part III.A)

B) (U//FOUO) Investigative assistance must be in compliance with interagency MOU/MOA, if applicable. For example, specific approval and notification requirements exist for assisting the Central Intelligence Agency (CIA) and the Department of Defense (DOD) domestic activities.

12.3.2.1.2 (U) APPROVAL REQUIREMENTS

b7E

A) (U//FOUO [redacted]

B) (U//FOUO) ***Sensitive Investigative Matters (SIM):*** Any investigative assistance to other USIC agencies involving a SIM requires Chief Division Counsel (CDC)/Office of the General Counsel (OGC) review, SAC/Section Chief (SC) approval, and notification, as specified in 12.3.2.1.3.B, below.

12.3.2.1.3 (U) NOTICE REQUIREMENTS

A) (U//FOUO) ***General:*** Notice must be provided for the investigative activity or investigative method as specified in the DIOG or applicable MOU/MOAs.

B) (U//FOUO) ***Sensitive Investigative Matters (SIM):*** In addition to the above-required approvals, any investigative assistance to USIC agencies involving a SIM requires notification to the appropriate FBI Headquarters (FBIHQ) operational Unit Chief (UC) and SC by Electronic Communication (EC) as soon as practicable, but no later than 15 calendar days after the initiation of the investigative assistance. The appropriate FBIHQ operational unit must provide notice to the DOJ Criminal Division or National Security Division (NSD) as soon as practicable, but not later than 30 calendar days after the initiation of any investigative assistance involving a SIM.

C) (U//FOUO) ***Classified Appendix:*** See the classified provisions in DIOG Appendix G for additional notice requirements.

12.3.2.1.4 (U) DOCUMENTATION REQUIREMENTS

(U//FOUO) Investigative assistance (including expert) to USIC agencies using an investigative method, other than those authorized in assessments, must be documented with the FD-999, filed and uploaded to an appropriate file as specified in Sections 12.5 and 12.6 below. Division PGs may require specific additional reporting requirements for their programs.

12.3.2.2 (U) INVESTIGATIVE ASSISTANCE TO OTHER UNITED STATES FEDERAL AGENCIES

12.3.2.2.1 (U) AUTHORITY

A) (U//FOUO) The FBI may provide investigative assistance to any other federal agency in the investigation of federal crimes or threats to the national security or in the collection of positive foreign intelligence. (Pursuant to DIOG Section 9, collection of positive foreign intelligence requires prior approval from the Collection Management Section (CMS), FBIHQ.) The FBI may provide investigative assistance to any federal agency for any other purpose that may be legally authorized, including investigative assistance to the United States Secret Service (USSS) in support of its protective responsibilities. (AGG-Dom, Part III.B.1) See DIOG Section 12.4 below for guidance in providing technical assistance to federal agencies.

B) (U//FOUO) Investigative assistance must be in compliance with interagency MOU/MOA, if applicable.

12.3.2.2.1.1 (U) ACTUAL OR THREATENED DOMESTIC CIVIL DISORDERS

A) (U) At the direction of the Attorney General, the Deputy Attorney General, or the Assistant Attorney General for the Criminal Division, the FBI shall collect information relating to actual or threatened civil disorders to assist the President in determining (pursuant to the authority of the President under 10 U.S.C. §§ 331-33) whether use of the armed forces or militia is required and how a decision to commit troops should be implemented. The information sought shall concern such matters as (AGG-Dom, Part III.B.2):

1) (U) The size of the actual or threatened disorder, both in number of people involved or affected and in geographic area;

2) (U) The potential for violence;

3) (U) The potential for expansion of the disorder in light of community conditions and underlying causes of the disorder;

4) (U) The relationship of the actual or threatened disorder to the enforcement of federal law or court orders and the likelihood that state or local authorities will assist in enforcing those laws or orders; and

5) (U) The extent of state or local resources available to handle the disorder.

B) (U) Civil disorder investigations will be authorized only for a period of 30 days, but the authorization may be renewed for subsequent 30 day periods.

C) (U) The only investigative methods that may be used during a civil disorder investigation are:

1) (U) Public information (See DIOG Section 18.5.1);

2) (U) Records or information - FBI or DOJ (See DIOG Section 18.5.2);

3) (U) Records or information - Other Federal, state, local, or tribal, or foreign governmental agency (See DIOG Section 18.5.3);

4) (U) Online services and resources (See DIOG Section 18.5.4);

5) (U) Interview or request information from the public or private entities (See DIOG Section 18.5.6);

(U//FOUO) *Note:* Such interviews may only be conducted if the FBI employee identifies himself or herself as an FBI employee and accurately discloses the purpose of the interview.

6) (U) Information voluntarily provided by governmental or private entities (See DIOG Section 18.5.7); and

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

12.3.2.2.1.2 (U) PUBLIC HEALTH AND SAFETY AUTHORITIES IN RELATION TO DEMONSTRATIONS

A) (U) At the direction of the Attorney General, the Deputy Attorney General, or the Assistant Attorney General for the Criminal Division, the FBI shall collect information relating to demonstration activities that are likely to require the federal government to take action to facilitate the activities and provide public health and safety measures with respect to those activities. The information sought in such an investigation shall be that needed to facilitate an adequate federal response to ensure public health and safety and to protect the exercise of First Amendment rights, such as:

1) (U) The time, place, and type of activities planned;

2) (U) The number of persons expected to participate;

3) (U) The expected means and routes of travel for participants and expected time of arrival; and

4) (U) Any plans for lodging or housing of participants in connection with the demonstration.

B) (U) The only investigative methods that may be used in an investigation under this paragraph are:

1) (U) Public Information (See DIOG Section 18.5.1);

2) (U) Records or information – FBI and DOJ (See DIOG Section 18.5.2);

3) (U) Records or information – other Federal, state, local, tribal, or foreign government agencies (See DIOG Section 18.5.3);

4) (U) Use online services and resources (See DIOG Section 18.5.4);

5) (U) Interview or request information from the public or private entities (See DIOG Section 18.5.6);

(U//FOUO) *Note:* Such interviews may only be conducted if the FBI employee identifies himself or herself as an FBI employee and accurately discloses the purpose of the interview;

6) (U) Accept information voluntarily provided by governmental or private entities (See DIOG Section 18.5.7); and

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

12.3.2.2.2 (U) APPROVAL REQUIREMENTS

b7E

A) (U//FOUO) [redacted]

B) (U//FOUO) ***Sensitive Investigative Matters (SIM):*** Any investigative assistance to other federal agencies involving a SIM requires prior CDC/OGC review and SAC/SC approval, and notification, as specified in 12.3.2.2.3.B below.

12.3.2.2.3 (U) NOTICE REQUIREMENTS

A) (U//FOUO) ***General:*** Notice must be provided for the investigative activity or investigative method as specified in the DIOG and applicable MOU/MOAs.

B) (U//FOUO) ***Sensitive Investigative Matters (SIM):*** In addition to the above-required approvals, any investigative assistance to another federal agency involving a SIM requires notification to the appropriate FBIHQ operational UC and SC by EC as soon as practicable, but no later than 15 calendar days after the initiation of the assistance. The appropriate FBIHQ operational unit must provide notice to the DOJ Criminal Division or NSD as soon as practicable, but not later than 30 calendar days after the initiation of any assistance involving a SIM.

C) (U//FOUO) ***Classified Appendix:*** See the classified provisions in DIOG Appendix G for additional notice requirements.

12.3.2.2.4 (U)DOCUMENTATION REQUIREMENTS

(U//FOUO) Investigative assistance (including expert) to other Federal agencies using an investigative method, other than those authorized in assessments, must be documented with the FD-999, filed and uploaded to an appropriate file as specified in Sections 12.5 and 12.6 below. Division PGs may require specific additional reporting requirements for their programs.

12.3.2.3 (U) INVESTIGATIVE ASSISTANCE TO STATE, LOCAL AND TRIBAL AGENCIES

(U) The FBI may provide investigative assistance to state, local and tribal agencies:

A) (U) in the investigation of crimes under state or local law when authorized by federal law (e.g., 28 U.S.C. §§ 540—felonious killing of state and local law enforcement officer; 540A—violent crime against travelers; 540B—serial killings);

B) (U) in the investigation of matters that may involve federal crimes or threats to national security, or for such other purposes as may be legally authorized;

C) (U) when such assistance is requested by the governor of the state pursuant to 42 U.S.C. § 10501 [redacted] The Attorney General must approve any request for assistance under 42 U.S.C. § 10501; and

D) (U) under limited circumstances, the FBI is authorized to provide "expert" personnel to assist law enforcement agencies in their investigations [redacted] b7E

(U) The authority to provide "expert assistance" to state investigations has been the subject of several opinions from the Office of Legal Counsel (OLC), DOJ. OLC has opined that the limited authority the FBI has in this area generally derives from its authority to "assist in conducting, at the request of a State [or] unit of local government… local and regional training programs for the training of State and local criminal justice personnel engaged in the investigation of crime and the apprehension of criminals," 42 U.S.C. §3771, and its authority to provide Laboratory assistance even if there is no federal crime, 28 C.F.R. §0.85(g). OLC has made clear that this is not a broad grant of authority [redacted] b7E

(U) It should be stressed that the limitations on this authority relate to providing expert investigative assistance – not to other types of interaction that could be helpful to our domestic law enforcement colleagues, including standard liaison and training [redacted]

(U) As used here, "expert personnel" are FBI employees who possess special skill or knowledge not normally possessed by professional law enforcement officers, that is derived from the employee's education, training, or experience; the term does not include [redacted] b7E

(U) Areas of expertise for which requests for investigative assistance are commonly made include: [redacted] If the pertinent program has a PG or Policy Directive, the policy, procedures and approval requirements contained within the PG or Policy Directive must be followed.

12.3.2.3.1 (U) APPROVAL REQUIREMENTS

A) (U) ***General:*** If the request for investigative assistance is based on Section 12.3.2.3. A or B above, the approval requirements specified in DIOG Sections 6 or 7 must be followed. If the request for investigative assistance is based on Section 12.3.2.3.C above, the Attorney General must approve the request.

B) (U) ***Expert Investigative Assistance:*** If the request for expert investigative assistance is based on Section 12.3.2.3.D above and it is not covered by an existing PG or Policy Directive, the

ADIC/SAC in the field office (or the FBIHQ SC if the request is received at FBIHQ) may approve the request with notification as soon as practicable to the General Counsel if:

1) (U) The head (or designee) of the state, local, or tribal law enforcement agency has submitted a written request (including by email) to the FBI which:

   a) (U) Identifies the need for specific expertise from the FBI;

   b) (U) Articulates the risk of an imminent threat of death or serious injury to members of the public or law enforcement personnel or a significant risk to public safety; and

   c) (U) Represents that the agency does not have available employees with the needed expertise or that the employees who do have the needed expertise are not sufficiently well trained to handle the immediate situation.

   (U) *Note:* If due to the exigency of the situation there is not time for the request to be submitted in writing, the request may be made orally, but must be followed by a written request as soon as practicable, but not more than five (5) business days.

2) (U) b7E

3) (U) The requesting agency is acting in the lawful execution of an authorized function of that organization; and

4) (U) The loan of FBI personnel is an appropriate use of personnel and financial resources and does not jeopardize any ongoing FBI investigation.

12.3.2.3.2 (U) NOTICE REQUIREMENTS

A) (U//FOUO) ***General:*** Notice must be provided for the investigative activity or investigative method as specified in the DIOG, and applicable MOU/MOAs and/or treaties.

B) (U//FOUO) ***Sensitive Investigative Matters (SIM):*** In addition to the above-required approvals, any investigative assistance provided to a state, local, or tribal law enforcement agency involving a SIM requires notification to the appropriate FBIHQ operational unit and section by EC as soon as practicable, but no later than 15 calendar days after the initiation of the assistance. The appropriate FBIHQ operational unit must provide notice to the DOJ Criminal Division or NSD as soon as practicable, but not later than 30 calendar days after the initiation of any assistance involving a sensitive investigative matter.

(U//FOUO) ***Classified Appendix:*** See the classified provisions in DIOG Appendix G for additional notice requirements.

12.3.2.3.3 (U) DOCUMENTATION REQUIREMENTS

(U//FOUO) Investigative assistance (including expert) using an investigative method, other than those authorized in assessments, must be documented with the FD-999, filed

and uploaded to an appropriate file as specified in Sections 12.5 and 12.6 below. Division PGs may require specific additional reporting requirements for their programs.

12.3.2.3.4 (U) EXAMPLES OF EXPERT INVESTIGATIVE ASSISTANCE

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

b7E

(U//FOUO) **Response 1:**

b7E

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

b7E

(U//FOUO) **Response 2:**

b7E

(U//FOUO) **Example 3:**

b7E

(U//FOUO) **Response 3:**

b7E

[redacted] b7E

12.3.2.4 (U) Investigative Assistance to Foreign Agencies

(U//FOUO) The foundation of the FBI's international program is the Legal Attaché (Legat). Each Legat is the Director's personal representative in the foreign countries in which he/she resides or has regional responsibilities. The Legat's job is to respond to the FBI's domestic and foreign investigative needs. The Legat can accomplish this because he/she develops partnerships and fosters cooperation with his or her foreign counterparts on every level and is familiar with investigative rules, protocols, and practices that differ from country to country. This is the Legat's primary responsibility. As such, foreign agency requests for assistance will likely come to the FBI through the Legat or International Operations Division (IOD) [redacted] b7E

12.3.2.4.1 (U) Authorities

A) (U//FOUO) At the request of foreign law enforcement, intelligence, or security agencies, the FBI may conduct investigations or provide assistance to investigations by such agencies, consistent with the interests of the United States (including national security interests) and with due consideration of the effect on any US person (USPER). (AGG-Dom, Part III.D.1) The FBI must follow applicable MOUs and MOAs (to include those with other US Government (USG) agencies), Mutual Legal Assistance Treaties (MLAT), Letters Rogatory, and other treaties when it provides assistance to foreign governments. b7E

1) (U//FOUO) [redacted]

2) (U//FOUO) [redacted]

B) (U//FOUO) [redacted]

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

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

12.3.2.4.2 (U) APPROVAL REQUIREMENTS

A) (U//FOUO) When a request to assist a foreign agency is received from a Legat or IOD, and such assistance will require the use of investigative methods other than those that are authorized in Assessments, prior SSA approval must be obtained and documented as specified in 12.3.2.4.4 below.

B) (U//FOUO) If a request for assistance is received directly from a foreign law enforcement or intelligence service and is not processed through a Legat or IOD, written notification documenting the foreign assistance request must be provided to the appropriate Legat and IOD by the FD-999, and IOD must grant approval prior to providing assistance, regardless of what investigative methods are used. (See also classified provisions in DIOG Appendix G)

C) (U//FOUO) The Office of International Affairs (OIA) in the DOJ's Criminal Division, has the responsibility and authority for the execution of all foreign assistance requests requiring judicial action or compulsory process. FBI IOD must coordinate all such requests with the DOJ OIA. (See DAG Memorandum, dated 5/16/2011, titled "Execution of Foreign Requests for Assistance in Criminal Cases.")

D) (U//FOUO) Higher supervisory approvals and specific notifications may be required for assistance to foreign agencies involving joint operations, SIMs, and using particular investigative methods, as noted below and in Sections 10 and 18 of the DIOG, and in division PGs.

E) (U//FOUO) Investigations and assistance conducted overseas, as well as related or official foreign travel of FBI personnel, require country clearances and notification to the Chief of Mission (COM) or designee. Such overseas investigations and assistance must adhere to the supplemental guidance in the IOD PG.

12.3.2.4.3 (U) NOTICE REQUIREMENTS

A) (U//FOUO) When a foreign assistance request is submitted directly to a Legat or IOD by a foreign agency or through an FBIHQ-authorized joint task force operation involving foreign agencies that has previously been briefed to the Legat, IOD has notice of the request and the FBI employee does not need IOD approval prior to providing the assistance. The FBI employee must provide IOD and the Legat the results of the assistance.

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

C) (U//FOUO) ***Classified Appendix:*** See the classified provisions in DIOG Appendix G for additional notice requirements.

D) (U//FOUO) ***Sensitive Investigative Matters (SIM):*** Any request for investigative assistance to a foreign agency involving a SIM requires OGC review and IOD SC approval, and notification as specified below. In addition to these approvals, any investigative assistance to a

foreign agency involving a SIM requires notification to the appropriate FBIHQ operational UC and SC by EC with an LHM suitable for dissemination to DOJ as soon as practicable, but no later than 15 calendar days after the initiation of the assistance. Additionally, the appropriate IOD unit must provide notice to the DOJ Criminal Division or NSD as soon as practicable, but not later than 30 calendar days after the initiation of any assistance involving a SIM.

12.3.2.4.4 (U) DOCUMENTATION REQUIREMENTS

(U//FOUO) All investigative assistance to foreign agencies must be documented with an FD-999 and uploaded to an appropriate file as specified in Sections 12.5 and 12.6 below.

12.3.2.4.5 (U) EXAMPLES

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

b7E

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

b7E

12.4 (U) TECHNICAL ASSISTANCE TO OTHER AGENCIES – STANDARDS, APPROVALS AND NOTICE REQUIREMENTS

(U//FOUO) FBI technical assistance may be provided to other agencies when:

A) (U//FOUO)

B) (U//FOUO)

b7E

C) (U//FOUO)

12.4.1 (U) AUTHORITY

(U//FOUO) Pursuant to 28 C.F.R. §0.85(g), FBI Laboratories, including but not limited to, the Laboratory Division, Operational Technology Division's Digital Evidence Laboratory, and Regional Computer Forensic Laboratories are authorized to provide technical or scientific assistance and expert testimony to any duly constituted law enforcement agency. Additionally, pursuant to Attorney General (AG) Order 2954-2008, the FBI is authorized to provide reasonable technical and expert assistance to Federal, state, local, and tribal law enforcement agencies to assist such agencies in the lawful execution of their authorized functions. (See also 28 U.S.C §§ 509, 510 and 530(C)). Such assistance may also be provided to certain foreign agencies (see Section 12.4.2.4 below). Under the Order, such technical and expert assistance includes, but is not limited to:

A) (U) Lending or sharing equipment or property;

B) (U) Sharing facilities or services;

C) (U) Collaborating in the development, manufacture, production, maintenance, improvement, distribution, or protection of technical investigative capabilities;

D) (U) Sharing or providing transmission, switching, processing, storage or other services;

E) (U) Disclosing technical designs, knowledge, information or expertise, or providing training in the same;

F) (U) Providing the assistance of expert personnel in accordance with written guidelines issued by the FBI General Counsel or approved by the General Counsel (See Section 12.3.2.3 above); and

G) (U) Providing forensic analysis and examination of submitted evidence.

12.4.2 (U) APPROVAL REQUIREMENTS

12.4.2.1 (U) TECHNICAL ASSISTANCE TO USIC AGENCIES

(U//FOUO) [redacted] b7E

12.4.2.2 (U) TECHNICAL ASSISTANCE TO FEDERAL, STATE, LOCAL AND TRIBAL (DOMESTIC) AGENCIES REGARDING ELECTRONIC SURVEILLANCE, EQUIPMENT, AND FACILITIES

(U) Field-based technical assistance requests under this section must be approved by the field office Assistant Director in Charge (ADIC) or SAC in compliance with the Operational Technology Division (OTD) Domestic Technical Assistance (DTA) PG. If the request for technical assistance involves equipment, facilities or property from more than one field office, each field office must approve the use of its resources.

(U) As specified below, FBIHQ senior executive officials and/or officials of the DOJ must approve a request for FBI technical assistance that involves: b7E

A) (U) [redacted]

B) (U) [redacted]

C) (U) [redacted] b7E

D) (U) Assistance to foreign law enforcement agencies (See Section 12.4.2.4 below).

(U) The OTD [redacted] provides additional details specifying the procedures and approval process that must be followed when the [redacted]

(U) For technical assistance to foreign law enforcement agencies see Section 12.4.2.4 and the [redacted]

12.4.2.3 (U) Technical Assistance to Federal, State, Local and Tribal (Domestic) Agencies Involving Equipment or Technologies Other than Electronic Surveillance Equipment

(U) There are limited other situations in which, in the absence of a federal nexus, a domestic law enforcement agency may seek technical assistance through the short term loan of equipment from the FBI. If there is an applicable PG or Policy Directive, the policy and procedures contained within the PG or Policy Directive must be followed (see, e.g., Corporate Policy Directive: Deployment of MRAP Armored Vehicles in the Absence of Federal Jurisdiction). If no PG or Policy Directive governs the particular equipment sought to be borrowed *and* if the loan of the equipment does not necessarily also entail the loan of personnel to use or operate the equipment, then the ADIC/SAC of the field office must approve the loan of the equipment in accordance with the following policy and procedures. If the loan of the equipment necessarily entails the loan of FBI employees, the policies governing expert assistance set forth below must also be followed.

(U) Any loan of equipment must be documented through a written agreement between the ADIC/SAC and the head of the borrowing law enforcement agency or his/her designee. At a minimum, the agreement must provide that the borrowing law enforcement agency will reimburse the FBI should the equipment be lost or damaged and that the borrowing law enforcement agency will promptly return the equipment when asked to do so by the FBI. If due to the exigency of the situation there is not time for the request to be submitted in writing, the request may be made orally but must be followed by a written agreement as soon as practicable, but not more than five (5) business days following the loan.

(U) In considering whether to lend the equipment to the federal, state, local and tribal law enforcement agency, the ADIC/SAC must take into account the following:

A) (U) The purpose for which the equipment is being requested and how the equipment will be used to advance that objective;

B) (U) The likelihood that the equipment will be damaged by the requested use;

C) (U) The likelihood that the field office will need the equipment during the proposed loan period; and

D) (U) Whether the borrowing law enforcement agency has previously violated the terms of any loan of equipment or damaged any equipment previously lent by the FBI.

(U) The [redacted] provides additional details specifying the procedures and approval process that must be followed when [redacted] b7E

(U) For technical assistance to foreign law enforcement agencies see Section 12.4.2.4 below and the [redacted]

12.4.2.4 (U) Technical Assistance to Foreign Agencies

12.4.2.4.1 (U) Authorities

A) (U//FOUO) The AGG-Dom, Part III.D.4 authorizes the FBI to provide other technical assistance to foreign governments to the extent not otherwise prohibited by law.

B) (U//FOUO) AG Order 2954-2008 authorizes the FBI to provide technical assistance to foreign national security and law enforcement agencies cooperating with the FBI in the execution of the FBI's counter-terrorism and counter-intelligence duties and to foreign law enforcement agencies to assist such agencies in the lawful execution of their authorized functions. Requests under this section for technical assistance with respect to electronic surveillance and other OTD technologies are to be handled pursuant to the OTD FTA PG.

12.4.2.4.2 (U) Approval Requirements

(U//FOUO) Approvals of requests for [redacted] are to be handled pursuant to the [redacted] b7E

12.4.2.4.3 (U) Notice Requirements

A) (U//FOUO) ***General:*** Notice must be provided for the investigative activity or investigative method as specified in the DIOG, and applicable MOU/MOAs and/or treaties.

B) (U//FOUO) ***Sensitive Investigative Matters (SIM):*** In addition to the above-required approvals, any investigative technical assistance to the agencies listed in this section involving a SIM requires approval by the SAC (HQ assistance requires SC approval) with notification to the appropriate FBIHQ operational unit and section and appropriate OTD section by EC as soon as practicable, but no later than 15 calendar days after the initiation of the assistance. The appropriate FBIHQ operational unit must provide notice to the DOJ Criminal Division or NSD as soon as practicable, but not later than 30 calendar days after the initiation of any assistance involving a SIM.

C) (U//FOUO) ***Classified Appendix:*** See the classified provisions in DIOG Appendix G for additional notice requirements.

12.4.2.4.4 (U) Documentation Requirements

(U//FOUO) All technical assistance rendered must be documented with the FD-999, filed and uploaded to an appropriate file as specified in Sections 12.5 and 12.6 below.

12.5 (U) Documentation Requirements for Investigative or Technical Assistance to Other Agencies

12.5.1 *(U) Documentation Requirements in General*

(U//FOUO)

b7E

(U//FOUO) When an FD-999 is used to document the "dissemination" of information to another agency, it is understood that "assistance" was provided to said agency and a separate FD-999 does not have to be completed to document the assistance to that agency (domestic or foreign).

12.5.2 *(U) Documentation Requirements for Investigative Assistance (including Expert Assistance) to Other Agencies (Domestic or Foreign)*

b7E

(U//FOUO) ***Mandatory use of the FD-999:*** The FD-999 must be used when providing

A) (U)
B) (U)
C) (U)
D) (U)

(U//FOUO)

b7E

(U//FOUO)

12.5.3 (U) Documentation Requirements for Technical Assistance to Other Agencies (Domestic or Foreign)

(U//FOUO) ***Mandatory use of the FD-999:*** The FD-999 must be used when providing any [redacted] b7E

A) (U) [redacted]
B) (U)
C) (U)
D) (U)

12.6 (U) Dissemination of Information to Other Agencies – Documentation Requirements

(U//FOUO) Dissemination of information to other agencies must be consistent with Director of National Intelligence directives, the AGG-Dom, DIOG Section 14, FBI Foreign Dissemination Manual, the Privacy Act of 1974, and any applicable MOU/MOA, law, treaty or other policy.

(U//FOUO) Classified information may only be disseminated pursuant to applicable federal law, Presidential directive, Attorney General policy and FBI policy.

(U) The Privacy Act mandates specific documentation of any dissemination of information to an agency outside the DOJ involving a U.S. Citizen or alien lawfully admitted for permanent residence, i.e., a U.S. person (USPER).

(U//FOUO) Dissemination of information to foreign agencies must be in accordance with the FBI Foreign Dissemination Manual, dated May 23, 2008, or as revised.

(U//FOUO) ***Mandatory use of the FD-999:*** The FD-999 must be used to document the dissemination of all unclassified or classified (up to Secret level) information to:

A) (U) USIC Agencies;

B) (U) United States Federal Agencies - when the disseminated information is related to their respective responsibilities;

C) (U) State, Local, or Tribal Agencies - when the disseminated information is related to their respective responsibilities; or

D) (U) Foreign Agencies.

(U//FOUO) *Note:* Dissemination of Top Secret or higher classified information must be documented in the appropriate classified file or the Sensitive Compartmented Information Operational Network (SCION).

(U//FOUO) ***Optional use of the FD-999:*** The FD-999 is permitted, but is not required to be used, for the dissemination of information if:

A) (U//FOUO) the information disseminated is being furnished to an agency within the DOJ with which the FBI is working a joint investigation; or

B) (U//FOUO) the information is disseminated with an IIR, SIR, or other FBI document that is maintained in an approved database of records.

12.7 (U) RECORDS RETENTION REQUIREMENTS

12.7.1 (U) USE OF THE FD-999

(U//FOUO) All FD-999s must be created on the FBI's SharePoint site. This requirement allows the FBI to maintain a database to comply with the AGG-Dom, Part III.E.3 because it will permit, with respect to each such activity, the prompt retrieval of the:

A) (U) status of the assistance activity (opened or closed);

B) (U) the dates of opening and closing; and

C) (U) the basis for the assistance activity.

12.7.2 (U) UPLOADING THE FD-999

(U//FOUO) The FD-999 must be uploaded to the appropriate file, which may be:

A) (U) an Assessment file;

B) (U) a zero sub-assessment file;

C) (U) a Predicated Investigation file;

D) (U) a domestic police cooperation file – 343 Classification (the new 343 file classification system replaces the former 62 classification) as described below;

E) (U) a foreign police cooperation file – 163 Classification (the revised 163 file classification system) as described below;

F) (U) a zero classification file; or

G) (U) any other investigative or technical assistance control file using a unique investigative file number created by the field office, Legat, or FBIHQ division to document the dissemination of information or assistance to another agency.

(U//FOUO) These records will assume the NARA approved retention periods approved for the file classification in which they are maintained.

12.7.3 (U) REQUEST FOR FD-999 EXEMPTION

(U//FOUO) FBI entities/programs may submit to the Corporate Policy Office (CPO), Director's Office, a written request for an exemption to the mandatory FD-999 requirements contained in DIOG Section 12 provided the entity/program maintains a similar database to permit the prompt retrieval of the information required above. The CPO, in conjunction with personnel from the Office of Integrity and Compliance (OIC) and the OGC, will evaluate the exemption request to determine database compliance with the AGG-Dom. The CPO will approve or deny the exemption request, and maintain a list of all approved exempted entities/programs.

12.7.4 (U//FOUO) 343 File Classification - Domestic Police Cooperation Files

(U//FOUO) The former 62 file classification may no longer be utilized to document domestic police cooperation. The new **343** file classification system with alpha-designators must be utilized to document domestic police cooperation matters.

12.7.5 (U//FOUO) 163 File Classification – Foreign Police Cooperation Files

(U//FOUO) The 163 file classification was revised with "new" alpha-designators. The 163 file classification system must be utilized to document foreign police cooperation matters.

This Page is Intentionally Blank.

13 (U) EXTRATERRITORIAL PROVISIONS

13.1 (U) OVERVIEW

(U//FOUO) The FBI may conduct investigations abroad, participate with foreign officials in investigations abroad, or otherwise conduct activities outside the United States. The guidelines for conducting investigative activities outside of the United States are currently contained in:

A) (U) *The Attorney General's Guidelines for Extraterritorial FBI Operations and Criminal Investigations;*

B) (U) *The Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection (NSIG, Part II.E);*

C) (U) *The Attorney General Guidelines on the Development and Operation of FBI Criminal Informants and Cooperative Witnesses in Extraterritorial Jurisdictions;*

D) (U) *The Attorney General Procedure for Reporting and Use of Information Concerning Violations of Law and Authorization for Participation in Otherwise Illegal Activity in FBI Foreign Intelligence, Counterintelligence or International Terrorism Intelligence Investigations* (August 8, 1988); and

E) (U) *Memorandum of Understanding Concerning Overseas and Domestic Activities of the Central Intelligence Agency and the Federal Bureau of Investigation (2005).*

(U//FOUO) Collectively, these guidelines and procedures are referred to in the DIOG as the Extraterritorial Guidelines.

13.2 (U) PURPOSE AND SCOPE

b7E

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

A) (U//FOUO)

B) (U//FOUO)

C) (U//FOUO)

D) (U//FOUO)

E) (U//FOUO)

F) (U//FOUO)

b7E

G) (U//FOUO)

H) (U//FOUO)

I) (U//FOUO)

J) (U//FOUO)

(U//FOUO) FBI personnel planning to engage in any of the investigative activities described in the subsection above must obtain the concurrence of the appropriate Legal Attaché (Legat) and must comply with the remaining procedural requirement of the Extraterritorial Guidelines, which may be found in the classified provisions in DIOG Appendix G.

13.3 (U) JOINT VENTURE DOCTRINE

(U//FOUO) The "joint venture" doctrine provides that in certain circumstances, Fourth or Fifth Amendment rights may attach and evidence seized overseas, including statements of a defendant, may be subject to suppression if the foreign law enforcement officers did not comply with U.S. law. A determination that a "joint venture" exists requires a finding of "active" or "substantial" involvement by U.S. agents in the foreign law enforcement activity. Because the determination will be fact specific and very few cases illuminate what constitutes "active" or "substantial" participation, FBI employees should contact their CDC or OGC for guidance. See also Chapter 35, DOJ Federal Narcotics Manual (March 2011) available on the DOJ intranet.

13.4 (U) LEGAL ATTACHÉ PROGRAM

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

14 (U) RETENTION AND SHARING OF INFORMATION

14.1 (U) PURPOSE AND SCOPE

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

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

A) (U//FOUO) Facilitates the documentation of official decisions, policies, activities, and transactions;

B) (U//FOUO) Facilitates the timely retrieval of needed information;

C) (U//FOUO) Ensures continuity of FBI business;

D) (U//FOUO) Controls the creation and growth of FBI records;

E) (U//FOUO) Reduces operating costs by managing records according to FBI business needs and by disposing of unneeded records in a timely manner;

F) (U//FOUO) Improves efficiency and productivity through effective records storage and retrieval methods;

G) (U//FOUO) Ensures compliance with applicable laws and regulations;

H) (U//FOUO) Safeguards the FBI's mission-critical information;

I) (U//FOUO) Preserves the FBI's corporate memory and history; and

J) (U//FOUO) Implements records management technologies to support all of the goals listed above.

(U) Note: The hardcopy file is the **"official file"** at the present time and a hardcopy of all electronic or on-line forms or documents must be printed and serialized into the field office or FBIHQ hardcopy file.

14.2 (U) THE FBI'S RECORDS RETENTION PLAN, AND DOCUMENTATION

(U//FOUO) The FBI must retain records relating to investigative activities according to the FBI's records retention plan that has been approved by the National Archives and Records Administration (NARA). (AGG-Dom, Part VI.A.1)

(U//FOUO) The FBI's disposition authorities provide specific instructions about the length of time that records must be maintained. In some instances, records may be destroyed after a

prescribed period of time has elapsed. Other records are never destroyed and are transferred to NARA a certain number of years after an investigation is closed.

14.2.1 (U) DATABASE OR RECORDS SYSTEM

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

(U//FOUO) The FBI's official File Classification System covers records related to all investigative and intelligence collection activities, including Assessments. Records must be maintained in the FBI's Central Records System, or other designated systems of records, which provides the required maintenance and retrieval functionality.

14.2.2 (U) RECORDS MANAGEMENT DIVISION DISPOSITION PLAN AND RETENTION SCHEDULES

(U//FOUO) (U//FOUO) All investigative records, whether from Assessments or Predicated Investigations, must be retained in accordance with the Records Management Division Disposition Plan and Retention Schedules. No records, including those generated during Assessments, may be destroyed or expunged earlier than the destruction schedule without written approval from NARA, except in "expungement" circumstances as further described in RMD policy. Records, including those generated during Assessments, may not be retained longer than the destruction schedule unless otherwise directed by RMD to include, "litigation hold" circumstances as described in RMD policy. See the RMD webpage and

b7E

In the event an office believes they need to retain records beyond their destruction schedule, they should contact RMD for further guidance.

14.3 (U) INFORMATION SHARING

(U//FOUO) The FBI 2008 National Information Sharing Strategy (NISS) provides the common vision, goals, and framework needed to guide information sharing initiatives with our federal, state, local, and tribal agency partners, foreign government counterparts, and private sector stakeholders. The FBI NISS addresses the cultural and technological changes required to move the FBI to "a responsibility to provide" culture.

14.3.1 (U) PERMISSIVE SHARING

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

A) (U//FOUO) Within the FBI and to all other components of the DOJ if the recipients need the information in the performance of their official duties.

B) (U//FOUO) To other federal agencies if disclosure is compatible with the purpose for which the information was collected and it is related to their responsibilities. In relation to other USIC agencies, the determination whether the information is related to the recipient responsibilities may be left to the recipient.

C) (U//FOUO) To state, local, or Indian tribal agencies directly engaged in the criminal justice process when access is directly related to a law enforcement function of the recipient agency.

D) (U//FOUO) To Congress or to congressional committees in coordination with the FBI Office of Congressional Affairs (OCA) and the DOJ Office of Legislative Affairs.

E) (U//FOUO) To foreign agencies if the FBI determines that the information is related to their responsibilities; the dissemination is consistent with the interests of the United States (including national security interests); consideration has been given to the effect on any identifiable USPER; and disclosure is compatible with the purpose for which the information was collected.

F) (U//FOUO) If the information is publicly available, does not identify USPERs, or is disseminated with the consent of the person whom it concerns.

G) (U//FOUO) If the dissemination is necessary to protect the safety or security of persons or property, to protect against or prevent a crime or threat to the national security, or to obtain information for the conduct of an authorized FBI investigation.

H) (U//FOUO) If dissemination of the information is otherwise permitted by the Privacy Act (5 U.S.C.§ 552a) (AGG-Dom, Part VI.B.1)

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

14.3.2 (U) Required Sharing

(U//FOUO) The FBI must share and disseminate information as required by law and applicable policy. Working through the supervisory chain and other appropriate entities, FBI employees must ensure compliance with statutes, including the Privacy Act, treaties, Executive Orders, Presidential directives, National Security Council (NSC) directives, Homeland Security Council (HSC) directives, Director of National Intelligence directives, Attorney General-approved policies, and MOUs or MOAs.

14.4 (U) Information Related to Criminal Matters

14.4.1 (U) Coordinating with Prosecutors

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

14.4.2 (U) CRIMINAL MATTERS OUTSIDE FBI JURISDICTION

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

14.4.3 (U) REPORTING CRIMINAL ACTIVITY OF AN FBI EMPLOYEE OR CHS

(U//FOUO) When it appears that an FBI employee has engaged in criminal activity in the course of an investigation, the FBI must notify the USAO or an appropriate DOJ division. When it appears that a CHS has engaged in criminal activity in the course of an investigation, the FBI must proceed as provided in the AGG-CHS. When information concerning possible criminal activity by any other person appears in the course of an investigation, the FBI may open an investigation of the criminal activity if warranted, and must proceed as provided in Section14.4.1 and 14.4.2 above. (AGG-Dom, Part VI.C.3)

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

14.5 (U) INFORMATION RELATED TO NATIONAL SECURITY AND FOREIGN INTELLIGENCE MATTERS

(U//FOUO) All information sharing with a foreign government related to classified national security and foreign intelligence must be done in accordance with the FBI Foreign Dissemination Manual and effective policies governing MOUs.

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

consultation with other DOJ components, and for sharing national security and foreign intelligence information with White House agencies, as provided below. (AGG-Dom, Part VI.D)

14.5.1 (U) DEPARTMENT OF JUSTICE

(U//FOUO) The DOJ National Security Division (NSD) must have access to all information obtained by the FBI through activities relating to threats to the national security or foreign intelligence. The Director of the FBI and the Assistant Attorney General for NSD must consult concerning these activities whenever requested by either of them, and the FBI must provide such reports and information concerning these activities as the Assistant Attorney General for NSD may request. In addition to any reports or information the Assistant Attorney General for NSD may specially request under this subparagraph, the FBI must provide annual reports to the NSD concerning its foreign intelligence collection program, including information concerning the scope and nature of foreign intelligence collection activities in each FBI field office. (AGG-Dom, Part VI.D.1)

(U//FOUO) The FBI must keep the NSD apprised of all information obtained through activities under the AGG-Dom that is necessary to the ability of the United States to investigate or protect against threats to the national security; this should be accomplished with regular consultations between the FBI and the NSD to exchange advice and information relevant to addressing such threats through criminal prosecution or other means. (AGG-Dom, Part VI.D.1)

(U//FOUO) Except for counterintelligence investigations, a relevant USAO must have access to and must receive information from the FBI relating to threats to the national security, and may engage in consultations with the FBI relating to such threats, to the same extent as the NSD. The relevant USAO must receive such access and information from the FBI field offices. (AGG-Dom, Part VI.D.1)

(U//FOUO) In a counterintelligence investigation – i.e., an investigation of espionage or other intelligence activities, sabotage, or assassination, conducted by, for, or on behalf of foreign powers, organizations, or persons [AGG-Dom, Part VII.S.2]– the FBI may only provide information to and consult with a relevant USAO if authorized to do so by the NSD. Until the policies required by AGG-Dom, Part VI.D.1.d are promulgated, the FBI may consult freely with the USAO concerning investigations within the scope of this subparagraph during an emergency, so long as the NSD is notified of such consultation as soon as practicable after the consultation. (AGG-Dom, Part VI.D.1).

(U//FOUO) Information shared with a USAO pursuant to DIOG Section 14.5 (National Security) must be disclosed only to the USA or any AUSA designated by the USA as points of contact to receive such information. The USA and designated AUSA must have an appropriate security clearance and must receive training in the handling of classified information and information derived from FISA, including training concerning the secure handling and storage of such information and training concerning requirements and limitations relating to the use, retention, and dissemination of such information. (AGG-Dom, Part VI.D.1)

(U//FOUO) The disclosure and sharing of information by the FBI under this paragraph is subject to any limitations required in orders issued by the FISC, controls imposed by the originators of sensitive material, and restrictions established by the Attorney General or the Deputy Attorney

General in particular investigations. The disclosure and sharing of information by the FBI under this paragraph that may disclose the identity of a CHS is governed by the relevant provisions of the AGG-CHS. (AGG-Dom, Part VI.D.1)

14.5.2 (U) THE WHITE HOUSE

(U//FOUO) In order to carry out their responsibilities, the President, the Vice President, the Assistant to the President for National Security Affairs, the Assistant to the President for Homeland Security Affairs, the NSC and its staff, the HSC and its staff, and other White House officials and offices require information from all federal agencies, including foreign intelligence, and information relating to international terrorism and other threats to the national security. Accordingly, the FBI may disseminate to the White House foreign intelligence and national security information obtained through activities under the AGG-Dom, subject to the following standards and procedures.

14.5.2.1 (U) REQUESTS SENT THROUGH NSC OR HSC

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

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

14.5.2.2 (U) APPROVAL BY THE ATTORNEY GENERAL

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

14.5.2.3 (U) INFORMATION SUITABLE FOR DISSEMINATION

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

A) (U//FOUO) Information concerning international terrorism;

B) (U//FOUO) Information concerning activities of foreign intelligence services in the United States;

C) (U//FOUO) Information indicative of imminent hostilities involving any foreign power;

D) (U//FOUO) Information concerning potential cyber threats to the United States or its allies;

E) (U//FOUO) Information indicative of policy positions adopted by foreign officials, governments, or powers, or their reactions to United States foreign policy initiatives;

F) (U//FOUO) Information relating to possible changes in leadership positions of foreign governments, parties, factions, or powers;

G) (U//FOUO) Information concerning foreign economic or foreign political matters that might have national security ramifications; and

H) (U//FOUO) Information set forth in regularly published national intelligence requirements.

14.5.2.4 (U) NOTIFICATION OF COMMUNICATIONS

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

14.5.2.5 (U) DISSEMINATION OF INFORMATION RELATING TO BACKGROUND INVESTIGATIONS

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

14.5.3 (U) CONGRESS

(U//FOUO) FBI employees must work through supervisors and the FBI OCA to keep the congressional intelligence committees fully and currently informed of the FBI's intelligence activities as required by the National Security Act of 1947, as amended. Advice on what activities fall within the supra of required congressional notification can be obtained from OCA [A Corporate Policy Directive is forthcoming].

14.6 (U) SPECIAL STATUTORY REQUIREMENTS

(U) Information acquired under the FISA may be subject to minimization procedures and other requirements specified in that Act. (AGG-Dom, Part VI.D.3.a)

(U) Information obtained through the use of National Security Letters (NSLs) under 15 U.S.C. § 1681v (full credit reports) may be disseminated in conformity with the general standards of AGG-Dom, Part VI, and DIOG Section 18.6.6.6.1.8. Information obtained through the use of NSLs under other statutes may be disseminated in conformity with the general standards of the AGG-Dom, Part VI, subject to any specific limitations in the governing statutory provisions (see DIOG Section 18): 12 U.S.C. § 3414(a)(5)(B); 15 U.S.C. § 1681u(f); 18 U.S.C. § 2709(d); 50 U.S.C. § 436(e). (AGG-Dom, Part VI.D.3.b)

(U) Federal Rule of Criminal Procedure 6(e) generally prohibits disclosing "matters occurring before the grand jury." This includes documents, records, testimony of witnesses, or any other evidence deemed relevant by a sitting grand jury. The Attorney General has issued revised Guidelines for the Disclosure and Use of Grand Jury Information under Rule 6(e)(3)(D). On May 15, 2008, the Deputy Attorney General issued a memorandum which provides amplifying guidance as to lawful use and disclosure of 6(e) information. See also AGG-Dom, Part V.A.8 and DIOG Section 18.6.5.3.7.4.5.

14.7 (U) THREAT TO LIFE – DISSEMINATION OF INFORMATION

14.7.1 (U) OVERVIEW

(U//FOUO) The FBI has a responsibility to notify persons of threats to their life or threats that may result in serious bodily injury and to notify other law enforcement agencies of such threats (Extracted from DOJ Office of Investigative Policies, Resolution 20, dated 12/16/96). Depending on the exigency of the situation, an employee, through their supervisor, should notify the appropriate operational division at FBIHQ of the existence of the threat and the plan for notification. That plan may be followed unless advised to the contrary by FBIHQ.

14.7.2 (U//FOUO) INFORMATION RECEIVED THROUGH FISA SURVEILLANCE

(U//FOUO) If information is received through a FISA-authorized investigative technique indicating a threat to life or serious bodily harm within the scope of Section 14.7, the field office case agent responsible for that FISA must immediately coordinate the matter with the FBIHQ SSA responsible for that investigation and an NSLB attorney from the applicable counterintelligence or counterterrorism law unit. These individuals must consult the applicable FISA minimization procedures, consider the operational posture of the investigation, and collectively determine the appropriate manner in which to proceed. FBI executive management may be consulted, as appropriate (e.g., if DIDO or declassification authority is needed). The field office case agent must document the dissemination. If the decision is made not to disseminate the threat information, that decision must be approved by an ASAC or higher and the reasons must be documented in the applicable investigative file.

14.7.3 (U) DISSEMINATION OF INFORMATION CONCERNING THREATS AGAINST INTENDED VICTIMS (PERSONS)

14.7.3.1 (U) WARNING TO THE INTENDED VICTIM (PERSON)

14.7.3.1.1 (U) EXPEDITIOUS WARNINGS TO IDENTIFIABLE INTENDED VICTIMS

(U//FOUO) Except as provided below in Sections 14.7.3.1.1.1 (Exceptions) and 14.7.3.1.2 (Custody or Protectee), when an employee has information that a person who is identified or can be identified through reasonable means (hereafter a "intended victim") is subject to a credible threat to his/her life or of serious bodily injury, the FBI employee must attempt expeditiously to warn the intended victim of the nature and extent of the threat.

14.7.3.1.1.1 (U) EXCEPTIONS TO WARNING

(U//FOUO) An employee is not required to warn an intended victim if:

b7E

A) (U//FOUO) [redacted]

B) (U//FOUO) the intended victim knows the nature and extent of the specific threat against him/her.

14.7.3.1.1.2 (U) MEANS, MANNER, AND DOCUMENTATION OF WARNING/NOTIFICATION OR DECISION NOT TO WARN

(U//FOUO) The FBI employee, in consultation with his or her supervisor, must determine the means and manner of the warning, using the method most likely to provide direct notice to the intended victim. In some cases, this may require the assistance of a third party. The employee must document on an FD-999 the content of the warning, as well as when, where and by whom it was delivered to the intended victim. The FD-999 must be placed in a zero file or if investigative methods are used, the appropriate investigative file.

(U//FOUO) The employee, in consultation with his or her supervisor, may seek the assistance of another law enforcement agency to provide the warning. If this is done, the employee must document on an FD-999 that notice was provided by that law enforcement agency, as well as when, where and by whom (i.e., the name of the other agency's representative) it was delivered. The employee must also document the other agency's agreement to provide a timely warning. The FD-999 must be filed as specified above.

(U//FOUO) Whenever time and circumstances permit, an employee's decision not to provide a warning in these circumstances must be approved by an ASAC or higher. In all cases, the reasons for not providing a warning must be documented by EC or similar successor form in a zero file or if investigative methods are used, the appropriate investigative file.

14.7.3.1.2 (U) WARNINGS WHEN INTENDED VICTIM IS IN CUSTODY OR IS A PROTECTEE

(U//FOUO) When an employee has information that a person described below is an intended victim, the employee, in consultation with his or her supervisor, must expeditiously notify the law enforcement agency that has protective or custodial jurisdiction of the threatened person.

(U//FOUO) This section applies when the intended victim is:

A) (U//FOUO) a public official who, because of his/her official position, is provided a protective detail;

b7E

B) (U//FOUO) [redacted]

C) (U//FOUO) detained or incarcerated.

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

b7E

(U//FOUO) This paragraph does not apply to employees serving on the security detail of the FBI Director or any other FBI protected persons when the threat is to the individual they protect.

14.7.3.1.2.1 (U) MEANS, MANNER, AND DOCUMENTATION OF WARNING/NOTIFICATION

(U//FOUO) The employee, in consultation with his or her supervisor, may determine the means and manner of the notification. When providing notification, the employee shall provide as much information as possible regarding the threat and the credibility of the threat. The employee must document on an FD-999 what he or she informed the other law enforcement agency, and when, where, how (e.g., telephone call, email) and to whom the notice was delivered. The FD-999 must be placed in a zero file or if investigative methods are used, the appropriate investigative file.

14.7.3.2 (U) NOTIFICATION TO LAW ENFORCEMENT AGENCIES THAT HAVE INVESTIGATIVE JURISDICTION

14.7.3.2.1 (U) EXPEDITIOUS NOTIFICATION

14.7.3.2.1.1 (U) THREATS TO INTENDED PERSONS

(U//FOUO) Except as provided in Sections 14.7.3.2.2, when an employee has information that a person (other than a person described above in Section 14.7.3.1.2) who is identified or can be identified through reasonable means is subject to a credible threat to his/her life or of serious bodily injury, the employee must attempt expeditiously to notify other law enforcement agencies that have investigative jurisdiction concerning the threat.

14.7.3.2.1.2 (U) THREATS TO OCCUPIED STRUCTURES OR CONVEYANCES

(U//FOUO) When an employee has information that a structure or conveyance which can be identified through reasonable means is the subject of a credible threat which could cause a loss of life or serious bodily injury to its occupants, the employee, in consultation with his or her supervisor, must provide expeditious notification to other law enforcement agencies that have jurisdiction concerning the threat.

14.7.3.2.2 (U) EXCEPTIONS TO NOTIFICATION

(U//FOUO) An employee need not attempt to notify another law enforcement agency that has investigative jurisdiction concerning a threat:

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

B) (U//FOUO) when the other law enforcement agency knows the nature and extent of the specific threat to the intended victim.

(U//FOUO) Whenever time and circumstances permit, an employee's decision not to provide notification to another law enforcement agency in the foregoing circumstances must be

approved by an ASAC or higher. In all cases, the reasons for an employee's decision not to provide notification must be documented in writing in a zero file or if investigative methods are used, the appropriate investigative file.

14.7.3.2.3 MEANS, MANNER, AND DOCUMENTATION OF NOTIFICATION

(U//FOUO) The employee may determine the means and manner of the notification. The employee must document in writing in the applicable investigative file the content of the notification, and when, where, and to whom it was delivered.

14.7.4 (U//FOUO) DISSEMINATION OF INFORMATION CONCERNING THREATS, POSSIBLE VIOLENCE OR DEMONSTRATIONS AGAINST FOREIGN ESTABLISHMENTS OR OFFICIALS IN THE UNITED STATES

(U//FOUO) If information is received indicating a threat to life within the scope of Section 14.7, or possible violence or demonstrations against foreign establishments or officials in the United States, the field office case agent must immediately coordinate the matter with the FBIHQ SSA responsible for the case, who must notify the Department of State (DOS), United States Secret Service (USSS), and any other Government agencies that may have an interest. See Section IV of the 1973 FBI USSS MOU, which is available at [redacted] b7E for the FBI's information sharing responsibilities with the USSS in such cases.

14.7.5 (U) DISSEMINATION OF INFORMATION CONCERNING THREATS AGAINST THE PRESIDENT AND OTHER DESIGNATED OFFICIALS

(U//FOUO) The United States Secret Service (USSS) has statutory authority to protect or to engage in certain activities to protect the President and certain other persons as specified in 18 U.S.C. § 3056. An MOU between the FBI and USSS specifies the FBI information that the USSS wants to receive in connection with its protective responsibilities.

(U//FOUO) Detailed guidelines regarding threats against the President of the United States and other USSS protectees can be found in "Presidential and Presidential Staff Assassination, Kidnapping and Assault." (See the Violent Crimes PG)

This Page is Intentionally Blank.

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 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 Policy Implementation Guide (IPG)) must be used to document this analysis. See the IPG 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.

b7E

See DIOG Section 11 for further discussion of tripwires. Further guidance regarding domain management and examples of intelligence products are contained in the FBIHQ

(U//FOUO) All information collected during a Type 4 Domain Assessment must be documented in as directed in the

b7E

or Predicated Investigation must be opened

(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 sub-file named **"INTELPRODS"** exists for all investigative classifications, and a copy of all written intelligence products described above 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) [redacted]

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

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

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

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

16.1.2 (U) MITIGATION OF RISK

(U//FOUO)

16.1.3 (U) SENSITIVE UDP DEFINED

(U//FOUO)

b7E

16.1.4 (U) NON-SENSITIVE UDP DEFINED

(U//FOUO)

16.1.5 (U) TYPE OF ACTIVITY

(U//FOUO)

16.2 (U) PURPOSE, SCOPE, AND DEFINITIONS

b7E

16.2.1 (U) ORGANIZATION

(U//FOUO)

16.2.2 (U) LEGITIMATE ORGANIZATION

(U//FOUO)

b7E

16.2.3 (U) PARTICIPATION

(U//FOUO)

b7E

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

A) (U//FOUO)

B) (U//FOUO)

b7E

C) (U//FOUO)

b7E

[9] (U//FOUO)

(U//FOUO)

D) (U//FOUO)

b7E

(U//FOUO)

(U//FOUO) Examples of

A) (U//FOUO)

b7E

(U//FOUO)

b5

B) (U//FOUO)

b7E

(U//FOUO)

b5

C) (U//FOUO)

b7E

D) (U//FOUO)

b5

16.2.3.1 (U) UNDISCLOSED PARTICIPATION

(U//FOUO)

b7E

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

(U//FOUO)

b7E

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) UNDISCLOSED PARTICIPATION

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

A) (U//FOUO)

B) (U//FOUO)

b7E

C) (U//FOUO)

(U//FOUO)

(U//FOUO)

b7E

b7E

16.2.3.6 (U) Already a Member of the Organization or a Participant in its Activities

(U//FOUO)

b7E

16.3 (U) Requirements for Approval

16.3.1 (U) General Requirements

(U//FOUO)

b7E

16.3.1.1 (U) Undercover Activity

(U//FOUO)

16.3.1.2 (U) Concurrent Approval

(U//FOUO)

b7E

16.3.1.3 (U) DELEGATION AND "ACTING" STATUS

(U//FOUO)

(U//FOUO)

b7E

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

16.3.1.4.1 (U//FOUO)

A) (U//FOUO)

B) (U//FOUO)

b7E

16.3.1.4.2 (U//FOUO)

(U//FOUO)

A) (U//FOUO)

B) (U//FOUO)

b7E

C) (U//FOUO)

D) (U//FOUO)

b7E

16.3.1.5 (U) Specific Requirements for Sensitive Undisclosed Participation (Sensitive UDP)

16.3.1.5.1 (U//FOUO)

A) (U//FOUO)

b7E

B) (U//FOUO)

b5
b7E

16.3.1.5.2 (U//FOUO)

(U//FOUO)

b5
b7E

16.3.1.5.3 (U//FOUO)

b7E

(U//FOUO)

A) (U//FOUO)

b7E

B) (U//FOUO)

b5
b7E

C) (U//FOUO)

b5
b7E

16.4 (U) SUPERVISORY APPROVAL NOT REQUIRED

(U//FOUO)

b7E

A) (U//FOUO)

B) (U//FOUO)

b7E

C) (U//FOUO)

D) (U//FOUO)

b7E

E) (U//FOUO)

b7E

16.5 (U) Standards for Review and Approval

(U//FOUO)

A) (U//FOUO) b7E

B) (U//FOUO)

C) (U//FOUO)

D) (U//FOUO) b7E

E) (U//FOUO)

(U//FOUO)

A) (U//FOUO) b7E

B) (U//FOUO)

(U//FOUO)

(U//FOUO) b7E

(U//FOUO)

16.6 (U) Requests for Approval of Undisclosed Participation

(U//FOUO) b7E

[10] (U//FOUO)

b7E

(U//FOUO)

A) (U//FOUO)

B) (U//FOUO)

b7E

C) (U//FOUO)

D) (U//FOUO)

E) (U//FOUO)

b7E

F) (U//FOUO)

(U//FOUO)

b7E

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: b7E

A) (U//FOUO)

B) (U//FOUO) b7E

(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)

b7E

16.9.2 (U//FOUO)

(U//FOUO)

b7E

16.9.3 (U//FOUO)

(U//FOUO)

A) (U//FOUO)

b7E

B) (U//FOUO)

b7E

1) (U//FOUO)

2) (U//FOUO)

b7E

3) (U//FOUO)

a) (U//FOUO)

b7E

b) (U//FOUO)

b7E

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

(U//FOUO)

b7E

(U//FOUO)

b7E

(U//FOUO)

16.10 (U) UDP EXAMPLES

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

b7E

(U/FOUO)

b5
b7E

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

b7E

(U//FOUO)

b5
b7E

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

b7E

(U//FOUO)

b5
b7E

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

b7E

(U//FOUO)

b5
b7E

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

b7E

(U//FOUO)

b5
b7E

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

b7E

(U//FOUO)

b5
b7E

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

b7E

(U/FOUO)

(U/FOUO)

b5
b7E

(U/FOUO)

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

b7E

b7E

(U//FOUO)

b5
b7E

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

b7E

(U//FOUO)

b5
b7E

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

b7E

(U//FOUO)

b5
b7E

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

b7E

(U//FOUO)

b5
b7E

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

b7E

(U//FOUO)

b5
b7E

b7E

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

b7E

(U//FOUO)

b5
b7E

This Page is Intentionally Blank.