

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

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

[Including subsequent revisions by the Attorney General Orders]

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

PREAMBLE

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

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

TABLE OF CONTENTS

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

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

INTRODUCTION

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

1. Federal Crimes

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

2. Threats to the National Security

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

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

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

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

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

3. Foreign Intelligence

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

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

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

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

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

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

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

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

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

B. THE FBI AS AN INTELLIGENCE AGENCY

The FBI is an intelligence agency as well as a law enforcement agency. Its basic functions accordingly extend beyond limited investigations of discrete matters, and include broader analytic and planning functions. The FBI's responsibilities in this area derive from various administrative and statutory sources. See, e.g., E.O. 12333; 28 U.S.C. 532 note (incorporating P.L. 108-458 §§ 2001-2003) and 534 note (incorporating P.L. 109-162 § 1107). Enhancement of the FBI's intelligence analysis capabilities and functions has consistently been recognized as a key priority in the legislative and administrative reform efforts following the September 11, 2001, terrorist attacks:

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

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

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

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

C. OVERSIGHT

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

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

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

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

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

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

I. GENERAL AUTHORITIES AND PRINCIPLES

A. SCOPE

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

B. GENERAL AUTHORITIES

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

C. USE OF AUTHORITIES AND METHODS

1. Protection of the United States and Its People

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

2. Choice of Methods

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

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

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

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

3. Respect for Legal Rights

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

4. Undisclosed Participation in Organizations

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

5. Maintenance of Records under the Privacy Act

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

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

D. NATURE AND APPLICATION OF THE GUIDELINES

1. Repealers

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

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

2. Status as Internal Guidance

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

3. Departures from the Guidelines

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

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

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

4. Other Activities Not Limited

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

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

II. INVESTIGATIONS AND INTELLIGENCE GATHERING

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

A. ASSESSMENTS

1. Purposes

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

2. Approval

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

3. Authorized Activities

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

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

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

4. Authorized Methods

Only the following methods may be used in assessments:

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

B. PREDICATED INVESTIGATIONS

1. Purpose

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

2. Approval

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

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

3. Circumstances Warranting Investigation

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

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

4. Preliminary and Full Investigations

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

a. Preliminary investigations

i. Predication Required for Preliminary Investigations

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

ii. Duration of Preliminary Investigations

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

¹ Special Agents in Charge may allow Assistant Special Agents in Charge to authorize extension of time for concluding preliminary investigations by up to six months consistent with FBI policy. See Deputy Attorney General's Memorandum for the Heads of Department Components captioned, "*Delegation of Certain Special Agent in Charge Functions under the Attorney General's Guidelines for Domestic FBI Operations*", dated November 24, 2008.

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

year must be approved by FBI Headquarters.

iii. **Methods Allowed in Preliminary Investigations**

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

b. **Full Investigations**

i. **Predication Required for Full Investigations**

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

ii. **Methods Allowed in Full Investigations**

All lawful methods may be used in a full investigation.

5. **Notice Requirements**

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

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

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

C. ENTERPRISE INVESTIGATIONS

1. Definition

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

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

2. Scope

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

3. Notice and Reporting Requirements

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

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

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

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

III. ASSISTANCE TO OTHER AGENCIES

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

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

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

A. THE INTELLIGENCE COMMUNITY

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

B. FEDERAL AGENCIES GENERALLY

1. In General

The FBI may provide assistance to any federal agency in the investigation of federal crimes or threats to the national security or in the collection of foreign intelligence, and investigative assistance to any federal agency for any other purpose that may be legally authorized, including investigative assistance to the Secret Service in support of its protective responsibilities.

2. The President in Relation to Civil Disorders

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

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

collect information relating to actual or threatened civil disorders to assist the President in determining (pursuant to the authority of the President under 10 U.S.C. 331-33) whether use of the armed forces or militia is required and how a decision to commit troops should be implemented. The information sought shall concern such matters as:

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

3. Public Health and Safety Authorities in Relation to Demonstrations

- a. At the direction of the Attorney General, the Deputy Attorney General, or the Assistant Attorney General for the Criminal Division, the FBI shall collect information relating to demonstration activities that are likely to require the federal government to take action to facilitate the activities and provide public health and safety measures with respect to those activities. The information sought in such an investigation shall be that needed to facilitate an adequate federal response to ensure public health and safety and to protect the exercise of First Amendment rights, such as:
 - i. The time, place, and type of activities planned.
 - ii. The number of persons expected to participate.

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

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

C. STATE, LOCAL, OR TRIBAL AGENCIES

The FBI may provide investigative assistance to state, local, or tribal agencies in the investigation of matters that may involve federal crimes or threats to the national security or for such other purposes as may be legally authorized.

D. FOREIGN AGENCIES

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

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

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

E. APPLICABLE STANDARDS AND PROCEDURES

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

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

IV. INTELLIGENCE ANALYSIS AND PLANNING

The FBI is authorized to engage in analysis and planning. The FBI's analytic activities enable the FBI to identify and understand trends, causes, and potential indicia of criminal activity and other threats to the United States that would not be apparent from the investigation of discrete matters alone. By means of intelligence analysis and strategic planning, the FBI can more effectively discover crimes, threats to the national security, and other matters of national intelligence interest and can provide the critical support needed for the effective discharge of its investigative responsibilities and other authorized activities. For example, analysis of threats in the context of special events management, concerning public events or activities that may be targeted for terrorist attack, is an authorized activity under this Part.

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

A. STRATEGIC INTELLIGENCE ANALYSIS

The FBI is authorized to develop overviews and analyses of threats to and vulnerabilities of the United States and its interests in areas related to the FBI's responsibilities, including domestic and international criminal threats and activities; domestic and international activities, circumstances, and developments affecting the national security; and matters relevant to the conduct of the United States' foreign affairs. The overviews and analyses prepared under this Subpart may encompass present, emergent, and potential threats and vulnerabilities, their contexts and causes, and identification and analysis of means of responding to them.

B. REPORTS AND ASSESSMENTS GENERALLY

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

C. INTELLIGENCE SYSTEMS

The FBI is authorized to operate intelligence, identification, tracking, and information systems in support of authorized investigative activities, or for such other or additional purposes as may be legally authorized, such as intelligence and tracking systems relating to terrorists, gangs, or organized crime groups.

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

V. AUTHORIZED METHODS

A. PARTICULAR METHODS

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

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

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

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

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

B. SPECIAL REQUIREMENTS

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

1. Contacts with Represented Persons

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

2. Use of Classified Investigative Technologies

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

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

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

C. OTHERWISE ILLEGAL ACTIVITY

1. Otherwise illegal activity by an FBI agent or employee in an undercover operation relating to activity in violation of federal criminal law that does not concern a threat to the national security or foreign intelligence must be approved in conformity with the Attorney General's Guidelines on Federal Bureau of Investigation Undercover Operations. Approval of otherwise illegal activity in conformity with those guidelines is sufficient and satisfies any approval requirement that would otherwise apply under these Guidelines.
2. Otherwise illegal activity by a human source must be approved in conformity with the Attorney General's Guidelines Regarding the Use of FBI Confidential Human Sources.
3. Otherwise illegal activity by an FBI agent or employee that is not within the scope of paragraph 1. must be approved by a United States Attorney's Office or a Department of Justice Division, except that (i) an FBI agent or employee may engage in the consensual monitoring of communications in accordance with FBI policy, even if a crime under state, local, territorial, or tribal law, and (ii) a Special Agent in Charge may authorize the following:
 - a. otherwise illegal activity that would not be a felony under federal, state, local, territorial, or tribal law;
 - b. the controlled² purchase, receipt, delivery, or sale of drugs, firearms, stolen property, contraband, or other items that are subject to legal or regulatory restrictions on transfer, such as prescription medication or medical devices;
 - c. the delivery or sale of stolen property whose ownership cannot be determined, provided that the property does not pose a significant risk of death or serious injury to any person;
 - d. the payment of bribes or kickbacks;
 - e. the making of false representations in concealment of personal identity or the true ownership of a proprietary, but not including sworn testimony;
 - f. conducting money laundering transactions (including acting as an

² In a controlled transaction, the item(s) will be monitored by the FBI and retained or seized at the conclusion of the transaction.

Domestic Investigations and Operations Guide

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

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

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

4. The following activities may not be authorized:

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

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

- 5. An agent or employee may engage in otherwise illegal activity that could be authorized under this Subpart without the authorization required by paragraph 3, if necessary to meet an immediate threat to the safety of persons or property or to the national security, or to prevent the compromise of an investigation or the loss of a significant investigative opportunity. In such a case, prior to engaging in the otherwise illegal activity, every effort should be made by the agent or employee to consult with the Special Agent in Charge, and by the Special Agent in Charge to consult with the United States Attorney's Office or appropriate Department of Justice Division where the authorization of that office or division would be required under paragraph 3., unless the circumstances preclude such consultation. Cases in which otherwise illegal activity occurs pursuant to this paragraph without the authorization required by paragraph 3. shall be reported as soon as possible to the Special Agent in Charge, and by the Special Agent in Charge to FBI Headquarters and to the United States Attorney's Office or appropriate Department of Justice

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

Division.

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

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

VI. RETENTION AND SHARING OF INFORMATION

A. RETENTION OF INFORMATION

1. The FBI shall retain records relating to activities under these Guidelines in accordance with a records retention plan approved by the National Archives and Records Administration.
2. The FBI shall maintain a database or records system that permits, with respect to each predicated investigation, the prompt retrieval of the status of the investigation (open or closed), the dates of opening and closing, and the basis for the investigation.

B. INFORMATION SHARING GENERALLY

1. Permissive Sharing

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

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

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

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

2. Required Sharing

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

C. INFORMATION RELATING TO CRIMINAL MATTERS

1. Coordination with Prosecutors

In an investigation relating to possible criminal activity in violation of federal law, the agent conducting the investigation shall maintain periodic written or oral contact with the appropriate federal prosecutor, as circumstances warrant and as requested by the prosecutor. When, during such an investigation, a matter appears arguably to warrant prosecution, the agent shall present the relevant facts to the appropriate federal prosecutor. Information on investigations that have been closed shall be available on request to a United States Attorney or his or her designee or an appropriate Department of Justice official.

2. Criminal Matters Outside FBI Jurisdiction

When credible information is received by an FBI field office concerning serious criminal activity not within the FBI's investigative jurisdiction, the field office shall promptly transmit the information or refer the complainant to a law enforcement agency having jurisdiction, except where disclosure would jeopardize an ongoing investigation, endanger the safety of an individual, disclose the identity of a human source, interfere with a human source's cooperation, or reveal legally privileged information. If full disclosure is not made for the reasons indicated, then, whenever feasible, the FBI field office shall make at least limited disclosure to a law enforcement agency or agencies having jurisdiction, and full disclosure shall be made as soon as the need for restricting disclosure is no longer present. Where full disclosure is not made to the appropriate law enforcement agencies within 180 days, the FBI field office shall promptly notify FBI Headquarters in writing of the facts and circumstances concerning the criminal activity. The FBI shall make periodic reports to the Deputy Attorney General on such nondisclosures and incomplete disclosures, in a form suitable to protect the identity of human sources.

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

3. Reporting of Criminal Activity

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

D. INFORMATION RELATING TO NATIONAL SECURITY AND FOREIGN INTELLIGENCE MATTERS

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

1. Department of Justice

- a. The National Security Division shall have access to all information obtained by the FBI through activities relating to threats to the national security or foreign intelligence. The Director of the FBI and the Assistant Attorney General for National Security shall consult concerning these activities whenever requested by either of them, and the FBI shall provide such reports and information concerning these activities as the Assistant Attorney General for National Security may request. In addition to any reports or information the Assistant Attorney General for National Security may

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

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

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

Domestic Investigations and Operations Guide

States Attorneys and designated Assistant United States Attorneys shall have appropriate security clearances and shall receive training in the handling of classified information and information derived from the Foreign Intelligence Surveillance Act, including training concerning the secure handling and storage of such information and training concerning requirements and limitations relating to the use, retention, and dissemination of such information.

- f. The disclosure and sharing of information by the FBI under this paragraph is subject to any limitations required in orders issued by the Foreign Intelligence Surveillance Court, controls imposed by the originators of sensitive material, and restrictions established by the Attorney General or the Deputy Attorney General in particular cases. The disclosure and sharing of information by the FBI under this paragraph that may disclose the identity of human sources is governed by the relevant provisions of the Attorney General's Guidelines Regarding the Use of FBI Confidential Human Sources.

2. White House

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

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

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

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

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

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

3. Special Statutory Requirements

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

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

VII. DEFINITIONS

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

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

directed and controlled by such a foreign government or governments;

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

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

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

J. INTERNATIONAL TERRORISM:

Activities that:

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

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

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

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

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

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

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

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

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

U. UNITED STATES PERSON:

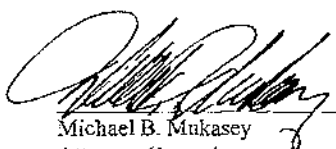
Any of the following, but not including any association or corporation that is a foreign power as defined in Subpart G.1.-3.:

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

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

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

Date: 09/29/08


Michael B. Mukasey
Attorney General

This Page is Intentionally Blank.

B APPENDIX B: (U) EXECUTIVE ORDER 12333

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

EXECUTIVE ORDER
13526

A M O N T M O N

UNITED STATES INTELLIGENCE ACTIVITIES
JANUARY 4, 1981
(AS AMENDED BY EXECUTIVE ORDERS 13124 (1993), 13506 (2004),
AND 13570 (2005))

PURPOSE

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

PART I Title, Direction, Purpose, and Responsibilities with Respect to United States Intelligence Efforts

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

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

UNCLASSIFIED - ~~FOR OFFICIAL USE ONLY~~

Domestic Investigations and Operations Guide

Abstract

the "The Shared Interest Movement" has a seven-year-old, and shall continue in the conduct of intelligence activities under this name, so persons enjoy the legal rights on all United States persons, including freedoms, civil liberties, and privacy rights guaranteed by federal law.

of Intelligence collection under this order should be guided by the need for information to support US intelligence priorities set by the President.

id: Special concerns should be given to detecting and
 completing

III. Espionage and other threats and activities
disclosed by foreign powers or their intelligence
services against the United States and its interests

(2) Threats to the United States and its interests from worldwide and

131 Threats to the United States and the interests
from the development, possession, proliferation, and
use of weapons of mass destruction.

for. Opinions expressed shall be placed to the protection of timely, accurate, and meaningful reports, responsive to stakeholders in the services to state. The flow in all appropriate manner of information, identifying your source information, must appear in analysis should be, including diverse analysis viewpoints, and accurately represent appropriate mitigative views.

11. State, local, and tribal governments are critical partners in ensuring and defending the United States from terrorism and other threats to the United States and its interests. Our national intelligence effort should take full account of the responsibilities and requirements of State, local, and tribal governments and, as appropriate, private entities

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

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

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

1.3 The National Security Council.

(a) Purpose. The National Security Council (NSC) shall act as the highest ranking and policy instrument that provides support to the President for review of, guidance for, and decisions on the conduct of all foreign intelligence, counterintelligence, and covert action, and associated policies and programs.

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

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

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

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

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

(i) Is hereby assigned the function under section 1.5(a) of the Act, to determine how intelligence, regardless of the source from which derived and including information gathered within or outside the United States, pertains to the work of the United States Department of Justice; and

(ii) Shall develop guidelines for how information or intelligence is provided to or accessed by the Intelligence Community in accordance with section 1.5(a) of this order, and for how the information or intelligence may be used and shared by the Intelligence Community. All guidelines developed in accordance with this section shall be approved by the Attorney General and, where applicable, shall be consistent with guidelines issued pursuant to section 101C of the Intelligence Reform and Terrorism Protection Act of 2004 (Public Law 108-458) (IRTPA).

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

(i) Shall protect, preserve, prioritize, and enhance for the Intelligence Community the secure timely and effective collection, processing, analysis, and dissemination of intelligence, of whatever nature and from whatever source

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

Services;

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

(c) Shall oversee and provide advice to the President and the IBC with respect to all ongoing and proposed foreign action programs;

(d) In regard to our involvement and conduct of intelligence exchanges and agreements with foreign governments and international organizations;

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

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

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

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

(e) Shall establish common security and access standards for reception and handling intelligence systems, information, and products, with special emphasis on facilitating;

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

(A) The follow-on EODD program agreed to and dissemination of information and intelligence practitioners, assigning the highest priority to detecting, preventing, suppressing, and disrupting terrorist threats and activities against the United States, its interests, and allies; and

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

(C) Shall ensure that appropriate prosecutive and agencies have access to intelligence and needed the support needed to perform independent analysis;

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

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

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

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

(C) May, only with respect to intelligence Community sources, and after consultation with the head of the

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

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

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

(iii) May establish Special and Manager and Chief of Bureaus, and designate officers or employees of the United States to serve in these positions.

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

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

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

(vii) The Director of the National

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

Geospatial-Intelligence Agency is designated the functional manager for geospatial intelligence.

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

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

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

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

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

(G) Shall determine requirements and priorities

*

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

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

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

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

(e) Shall fulfill the responsibilities in section 1.5(b)(12) and (13) of this order, consistent with applicable law and with full consideration of the rights of United States persons, whether information is to be collected inside or outside the United States;

(f) Shall ensure, through appropriate policies and procedures, the coordination, coordination, and integration of all intelligence activities conducted by an Intelligence Community element or funded by the National Intelligence Program, in accordance with these policies and procedures;

(g) The Director of the Federal Bureau of

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

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

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

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

(D) All policies and procedures developed under this section shall be harmonized with the needs of affected departments and intelligence community elements;

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

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

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

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

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

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

(c) The Director's exercise of authority in the Act and this order shall not abrogate the statutory or other responsibilities of the heads of departments of the United States Government or the Director of the Central Intelligence Agency. Directives issued and actions taken by the Director in the exercise of the Director's authority and responsibilities to integrate, coordinate, and ensure the Intelligence Community more effective in providing intelligence related to national security shall be implemented by the elements of the Intelligence Community, provided that any department head whose department contains an element of the Intelligence Community and who believes that a directive or action of the Director violates the requirements of section 1016 of the INTEA or this subsection shall bring the issue to the attention of the Director, the DDC, or the President for resolution in a manner that does not unduly interfere with existing responsibilities of the head of the department.

(d) Appointments to certain positions.

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

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

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

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

11. Removal from certain positions.

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

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

for Intelligence and Research, and the Assistant Secretary for Intelligence and Analysis of the Department of the Treasury. At the Director's request, the department head or his agent or assistant, or recommendation for removal, action may make a recommendation to the President for the removal of the individual.

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

(3) Nothing in this subsection shall be construed to limit or diminish either the authority of the President to remove, appoint, resign, or terminate the appointment or assignment of any individual, with or without a consultation, recommendation, or concurrence.

(4) The Intelligence Community, consistent with applicable Federal law and with the other provisions of this order, and

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

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

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

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

(c) Analyze, produce, and disseminate intelligence;

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

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

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

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

- (g) Take into consider source, intel, and tribal governments' and, as appropriate, private sector entities' information needs relating to national and homeland security;
 - (h) Deconflict, corroborate, and integrate all intelligence activities and other information gathering to coordinate with section 1.3(b)(10) of this order; and
 - (i) Coordinate with other entities and offices related to intelligence activities as the Director may direct.
- 1.3 *Values and Responsibilities of the Heads of Executive Branch Departments and Agencies.* The heads of all departments and agencies shall:
- (a) Provide the Director access to all information and intelligence relevant to the national security or that otherwise is required for the performance of the Director's duties, to include administrative and other support and management information, except such information withheld by law, by the President, or by the Executive orders acting under that power as the direction of the President;
 - (b) Provide all programmatic and budgetary information necessary to support the Director in developing the National Intelligence Program;
 - (c) Coordinate development and implementation of intelligence systems and architectures and, as appropriate, operational systems and architectures of their departments, agencies, and other elements with the Director in response to national intelligence requirements and all applicable information sharing and security policies, information privacy, and other legal requirements;
 - (d) Provide, to the maximum extent permitted by law, subject to the availability of appropriations and not inconsistent with the mission of the department or agency, such further support to the Director as the Director may request.

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

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

(c) Respond to requests coming from the Director under section 1.4(a)(1) of this order to the greatest extent possible, in accordance with applicable policies established by the head of the responding department or agency;

(d) Ensure that all persons within the department or agency comply with the provisions of Part I of this order, regardless of Intelligence Committee affiliation, when performing foreign intelligence and counterintelligence activities;

(e) Coordinate, supervise, and integrate all intelligence activities in accordance with section 1.3(b)(1), and intelligence and counterintelligence in accordance with section 1.4(a)(2) of this order;

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

11. Systems to be developed by the head of the department or agency and the Director of the Central Intelligence Agency and approved by the Director, inform the Director and the Director of the Central Intelligence Agency, either directly or through his designee serving outside the United States, as appropriate, of clandestine collection of foreign intelligence collected through human sources or through unannounced means outside the United States that has not been coordinated with the Central Intelligence Agency; and

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

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

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

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

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

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

(c) Report to the Intelligence Oversight Board, consistent with Executive Order 12958 of February 19, 1995, and provide copies of all such reports to the Director, concerning any intelligence activities of their elements that they have reason to believe may be unlawful or contrary to executive order or presidential directives;

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

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

(f) Disseminate information or intelligence to domestic

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

governments and international organizations under intelligence or counterintelligence arrangements or agreements established in accordance with section 1.5(a)(4) of this order.

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

(h) Ensure that the Inspector General, general counsels, and agency officials responsible for privacy or civil liberties protection in their respective organizations take actions to any information on intelligence necessary to perform their official duties.

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

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

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

(2) conduct counterintelligence activities without violating or interfering any internal security functions within the United States;

(3) conduct administrative and logistical support activities within and outside the United States as necessary for

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

cover and preliminary arrangements;

(b) Conduct covert action activities approved by the President. No agency except the Central Intelligence Agency for the Armed Forces of the United States in time of war declared by the Congress or during any period covered by a report from the President to the Congress consistent with the War Powers Resolution, Public Law 92-140, may conduct any covert action activity unless the President determines that another agency is more likely to achieve a particular objective;

(c) Conduct foreign intelligence liaison relationships with intelligence or security services of foreign governments or international organizations consistent with section 1.71k(4) of this code;

(d) Under the direction and guidance of the Director, and in accordance with section 1.71k(1) of this code, coordinate the implementation of intelligence and counterintelligence relationships between elements of the Intelligence Community and the intelligence or security services of foreign governments or international organizations; and

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

10. THE DEFENSE INTELLIGENCE AGENCY. The Director of the Defense Intelligence Agency shall:

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

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

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

- (a) Conduct counterintelligence activities;
 - (b) Conduct administrative and technical support activities within and outside the United States as necessary for overt and proprietary arrangements;
 - (c) Conduct foreign defense intelligence liaison relationships and defense intelligence exchange programs with foreign defense establishments, intelligence or security services of foreign governments, and international organizations in accordance with sections 1.4.1.1.1, 1.4.1.1.2, and 1.4.1.1.3 of this order;
 - (d) Manage and coordinate all activities related to the Defense Accounts system; and
 - (e) Provide foreign intelligence and technical intelligence staff support as directed by the Secretary of Defense.
- (c) THE NATIONAL SECURITY AGENCY. The Director of the National Security Agency shall:
- (a) Conduct, including through clandestine means, recruit, process, analyze, produce, and disseminate signals intelligence information and make for foreign intelligence and counterintelligence efforts to disrupt national and departmental relations;
 - (b) Establish and operate an effective unified organization for signals intelligence activities, except for the delegation of operational control over certain operations that are considered lawful, other elements of the Intelligence Community. No other department or agency may engage in signals intelligence activities except pursuant to a delegation by the Secretary of Defense, after consultation with the Director;
 - (c) Conduct signals intelligence collection and processing activities, including assignment of resources to an appropriate agent for each mission and task as required for the

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

direct support of military operations;

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

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

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

(g) formulate, consistent with section 1004(g) of the Army, within the field of authorized operations, security regulations covering operating practices, involving the collection, marking, and dissemination of signals intelligence and communications security material within and among the elements under control of the Director of the Overseas Security Agency, and exercise the necessary supervisory control to ensure compliance with the regulations; and

(h) conduct foreign signals intelligence related activities in accordance with sections 1.4101(a), 1.7101(f), and 1.8001 of this order.

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

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

(2) develop foreign signals intelligence relating to the above missions, in accordance with sections 1.4101(a), 1.7101(f), and 1.8001 of this order.

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

(e) THE NATIONAL GEOGRAPHIC-INTELLIGENCE AGENCY. The Director of the National Geographic-Intelligence Agency shall:

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

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

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

(4) Conduct foreign geospatial intelligence liaison relationships in accordance with sections 1.2101(d), 1.2101(e), and 1.1011 of this guide.

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

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

(2) Develop counterintelligence services;

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

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

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

Sections 1.1(a)(3), 1.1(a)(3), and 1.1(a) of this order.

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

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

(2) Conduct counterintelligence activities and

(3) Conduct foreign intelligence and

counterintelligence liaison relationships with intelligence, security, and law enforcement agencies of foreign governments or international organizations in accordance with sections 1.1(a)(4) and 1.1(a)(5) of this order.

(e) THE INTELLIGENCE AND COUNTERINTELLIGENCE ELEMENTS OF THE COAST GUARD, the Commandant of the Coast Guard shall:

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

(2) Conduct counterintelligence activities;

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

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

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

organizations in accordance with sections 1.3.1(a)(1), 1.3.1(a)(2), and, when operating as part of the Department of Defense, 1.3.1(a) of this order.

(1) THE BUREAU OF INTELLIGENCE AND RESEARCH, DEPARTMENT OF STATE; THE OFFICE OF INTELLIGENCE AND ANALYSIS, DEPARTMENT OF THE TREASURY; THE OFFICE OF NATIONAL SECURITY INTELLIGENCE, JOINT CHIEFS OF STAFF; THE OFFICE OF INTELLIGENCE AND ANALYSIS, DEPARTMENT OF HOMELAND SECURITY; AND THE OFFICE OF INTELLIGENCE AND COUNTERINTELLIGENCE, DEPARTMENT OF DEFENSE. The heads of the Bureau of Intelligence and Research, Department of State; the Office of Intelligence and Analysis, Department of the Treasury; the Office of National Security Intelligence, Joint Chiefs of Staff; the Office of Intelligence and Analysis, Department of Homeland Security; and the Office of Intelligence and Counterintelligence, Department of Defense shall:

(i) Collect directly or through publicly available sources; analyze, produce, and disseminate information, intelligence, and counterintelligence to support intelligence and counterintelligence priorities; and

(ii) Conduct and participate in analysis or information exchanges with foreign partners and international organizations in accordance with sections 1.3.1(c) and 1.3.1(d) of this order.

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

1.3 The Department of State. In addition to the authorities

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

exercised by the Bureau of Intelligence and Research under sections 1.1 and 1.711 of this order, the Secretary of State shall:

(a) Collect covertly or through publicly available sources: information relevant to United States foreign policy and national security interests;

(b) Disseminate, to the maximum extent possible, reports received from United States diplomatic and consular posts;

(c) Transmit reports, correspondence and editorial comment of the Intelligence Community to the Chiefs of United States Mission abroad; and

(d) Support Chiefs of United States Missions in discharging their responsibilities pursuant to law and presidential direction.

1.8 The Department of the Treasury. In addition to the authorities exercised by the Office of Intelligence and Analysis of the Department of the Treasury under sections 1.4 and 1.11, if authorized by the Secretary of the Treasury shall collect covertly or through publicly available sources: foreign financial information and, in consultation with the Department of State, transfer economic information.

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

(a) Collect (including through clandestine means), analyze, process, and disseminate information and intelligence and be responsible for all action taking and activity taking by the Service;

(b) Collect (including through clandestine means), analyze, process, and disseminate defense and defense-related intelligence and counterintelligence, as required for execution of the Secretary's responsibilities;

(c) Conduct programs and missions necessary to fulfill

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

national, governmental, and criminal intelligence requirements;

iii. Manage counterintelligence activities in support of Department of Defense components and coordinate counterintelligence activities in accordance with section 1.4(h)(20) and (21) of this order;

iv. Act, in coordination with the Director, as the executive agent of the United States Government for signals intelligence activities;

v. Provide for the timely transmission of cultural intelligence, as defined by the Director, within the United States Government;

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

vii. Ensure the security of Department of Defense installations, activities, information, property, and employees by appropriate means, including such associations of applicants, employees, contractors, and other persons with duties associated with the Department of Defense as are necessary;

viii. Establish and maintain defense intelligence relationships and defense intelligence exchange programs with selected or potential foreign defense and intelligence intelligence or security services or foreign governments, and international organizations, and ensure that such relationships and programs are in accordance with sections 1.3(b)(4), 1.4(h)(21) and 1.4(v)(1) of this order;

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

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

Defense; and

(b) Use the intelligence community elements within the Department of Defense identified in section 1.1(b) through (d) and, when the Coast Guard is operating as part of the Department of Defense.

(c) Have no carry out the Secretary of Defense's responsibilities assigned in this section or other regulations, agreements, or orders within the Department of Defense, as appropriate, to conduct the intelligence divisions and responsibilities assigned to the Secretary of Defense.

1.11 *The Department of Homeland Security.* In addition to the authority exercised by the Office of Intelligence and Analysis of the Department of Homeland Security under sections 1.1 and 1.1(b) of this order, the Secretary of Homeland Security shall conduct, through the United States Secret Service, activities to evaluate the relevance and capability of surveillance equipment being used against the President of the United States, the Vice President of the United States, the Executive Office of the President, and, as authorized by the Secretary of Homeland Security or the President, other Federal Service personnel and United States officials. No interception shall be acquired intentionally through such activities except to protect against use of such surveillance equipment, and those activities shall be conducted pursuant to procedures agreed upon by the Secretary of Homeland Security and the Attorney General.

1.12 *The Department of Energy.* In addition to the authority exercised by the Office of Intelligence and Counterintelligence of the Department of Energy under sections 1.1 and 1.1(b) of this order, the Secretary of Energy shall:

(a) Provide expert scientific, technical, analytic, and research capabilities to other agencies within the Intelligence Community, as appropriate;

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

(b). Participate in formulating intelligence collection and analysis requirements where the special expert capability of the Department can contribute; and

(c). Participate with the Department of State in overtly collecting information with respect to foreign energy matters.

1.13 The Federal Bureau of Investigation. In addition to the authorities exercised by the intelligence elements of the Federal Bureau of Investigation, of the Department of Justice under sections 1.4 and 1.7(g) of this order and under the supervision of the Attorney General and pursuant to such special laws as the Attorney General may enact, the Director of the Federal Bureau of Investigation shall, by written instructions, assign or assign the United States, or foreign, intelligence and law enforcement services, consistent with section 1.3(b)(1) and 1.3(c) of this order, as may be necessary to support national or departmental missions.

PART 2 *Function of Intelligence Activities*

2.1 Need. Timely, accurate, and insightful information about the activities, capabilities, plans, and intentions of foreign persons, organizations, and persons, and their assets, is essential to informed decisionmaking in the areas of national security, national defense, and foreign relations. Collection of such information is a priority objective and will be pursued in a timely, innovative, and responsive manner that is consistent with the Constitution and applicable law and respectful of the principles upon which the United States was founded.

2.2 Purpose. This Order is intended to enhance human and technical collection techniques, especially those conducted abroad, and the acquisition of significant foreign intelligence, as well as the detection and monitoring of international terrorist activities, the spread of weapons of mass destruction,

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

and espionage conducted by foreign powers. The tests below are derived generally, principles that, in addition to and consistent with applicable laws, are intended to achieve the proper balance between the acquisition of essential information and protection of individual interests. Nothing in this Order shall be construed to apply to or interfere with any authorized civil or criminal law enforcement responsibility of any department or agency.

2.3 Collection of Information. Elements of the Intelligence Community are authorized to collect, retain, or disseminate information concerning covered issues persons may in accordance with procedures established by the laws of the Intelligence Community without concern or by the need of a department containing such element and approved by the Attorney General, consistent with the authorities provided by Part 1 of this Order, after consultation with the Director. These provisions shall permit collection, retention, and dissemination of the following types of information:

(a) Information that is publicly available or collected with the consent of the person concerned;

(b) Information constitutive foreign intelligence or counterintelligence, including such information on visiting expeditions or other commercial organizations. Collection within the United States of foreign intelligence not otherwise obtainable shall be undertaken by the Federal Bureau of Investigation (FBI) or, when significant foreign intelligence is sought, by other authorized elements of the Intelligence Community, provided that no foreign intelligence collection by such elements may be undertaken for the purpose of acquiring information concerning the domestic activities of United States persons;

(c) Information obtained in the course of a lawful foreign

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

intelligence, counterintelligence, threat-related, and/or international terrorism intelligence;

(d) Information needed to protect the safety of any persons or organizations, including those who are targets, victims, or witnesses of international terrorist transactions;

(e) Information needed to protect domestic intelligence or counterintelligence sources, methods, and activities from unauthorized disclosure. Collection within the United States shall be undertaken by the FBI except that other elements of the Intelligence Community may also collect such information concerning present or former employees, present or former intelligence element contractors or their present or former employees, or applicants for such employment or contracting;

(f) Information concerning persons who are associated or believed to be potential sources or contacts for the purpose of evaluating their suitability or reliability;

(g) Information arising out of a lawful perimeter, physical, or communications security investigation;

(h) Information required by overseas organizations or directed at specific United States persons;

(i) Incidentally obtained information that may indicate involvement in activities that may violate Federal, state, local, or foreign laws; and

(j) Information necessary for public defense purposes.

In addition, elements of the Intelligence Community may disseminate information to each appropriate element within the Intelligence Community for purposes of allowing the recipient element to determine whether the information is relevant to its responsibilities and can be retained by it, except that information derived from signals intelligence may only be disseminated or made available to Intelligence Community elements in accordance with procedures established by the

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

Director in consultation with the Secretary of Defense and approved by the Attorney General.

2.4 Collection Techniques. Elements of the Intelligence Community shall use the least intrusive collection techniques feasible within the United States or directed against United States persons abroad. Elements of the Intelligence Community are not authorized to use such techniques as electronic surveillance, computerized pipeline searches, mail surveillance, physical surveillance, or monitoring devices unless they are in accordance with procedures established by the head of the Intelligence Community element concerned or the head of a department containing such element and approved by the Attorney General, after consultation with the Director. Such procedures shall protect constitutional and other legal rights and limit use of such information to lawful governmental purposes. These procedures shall not authorize:

i. The Central Intelligence Agency (CIA) to engage in electronic surveillance within the United States except for the purpose of training, testing, or conducting countermeasures to hostile electronic surveillance;

ii. Unconsented physical searches in the United States by elements of the Intelligence Community other than the FBI, except that:

iii. Searches by communications intelligence elements of the military services directed against military personnel within the United States or abroad for intelligence purposes, when authorized by a military commander empowered to approve physical searches for law enforcement purposes, based upon a finding of probable cause to believe that such persons are acting as agents of foreign powers; and

iv. Searches by CIA of personal property of non-United States persons lawfully in its possession;

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

(c) Physical surveillance of a United States person in the United States by elements of the Intelligence Community other than the FBI, except for:

(i) Physical surveillance of present or former employees, present or former intelligence element connections or their present or former employees, or applicants for any such employment or contracting; and

(ii) Physical surveillance of a military person employed by a nonintelligence element of a military service; and

(iii) Physical surveillance of a United States person abroad to collect foreign intelligence, except to obtain significant information that cannot reasonably be acquired by other means. *2.4 Attorney General Approval.* The Attorney General hereby is delegated the power to approve the use for intelligence purposes, within the United States or against a United States person abroad, of any technique for which a warrant would be required if undertaken for law enforcement purposes, provided that such techniques shall not be undertaken unless the Attorney General has determined in each case that there is probable cause to believe that the technique is directed against a foreign power or an agent of a foreign power. The authority delegated pursuant to this paragraph, including the authority to approve the use of electronic surveillance as defined in the Foreign Intelligence Surveillance Act of 1978, as amended, shall be exercised in accordance with that Act.

2.5 Assistance to Law Enforcement and Other Civil Authorities. Elements of the Intelligence Community are authorized to:

(a) cooperate with appropriate law enforcement agencies for the purpose of processing the employee, information, property, and facilities of any element of the Intelligence Community;

(b) obtain resources provided by law or this order,

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

participate in law enforcement activities to investigate or prevent clandestine intelligence activities by foreign powers, or international networks or clandestine activities;

(c) Provide specialized equipment, technical knowledge, or assistance of expert personnel for use by any department or agency, or when funds are undesignated, to support local law enforcement activities. Provision of assistance by expert personnel shall be provided to such use by the United States of the providing agency or department and

(d) Render any other assistance and cooperation to law enforcement or other civil authorities not prohibited by applicable law.

2.7 Contracting. Elements of the Intelligence Community are authorized to enter into contracts or arrangements for the provision of goods or services with private companies or institutions in the United States and need not reveal the sponsorship of such contracts or arrangements for authorized intelligence purposes. Contracts or arrangements with academic institutions may be executed only with the consent of appropriate officials of the institution.

2.8 Consistency with other laws. Nothing in this Order shall be construed to authorize any activity in violation of the Constitution or statutes of the United States.

2.9 Unauthorized Participation in Organizations Within the United States. No one acting on behalf of elements of the Intelligence Community may join or otherwise participate in any organization in the United States on behalf of any element of the Intelligence Community without disclosing such person's intelligence affiliation to appropriate officials of the organization, except in accordance with procedures established by the head of the Intelligence Community or any element thereof or the head of a department concerning such matters and approved by

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

the Attorney General, after consultation with the Director. Such participation shall be authorized only if it is essential to achieving lawful purposes as determined by the Intelligence Community element head or designee. No such participation may be undertaken for the purpose of influencing the activity of the organization or its members except in cases where:

1a) The participation is undertaken in behalf of the FBI in the course of a lawful investigation; or

1b) The organization concerned is composed primarily of individuals who are not trained armed persons and is reasonably believed to be acting on behalf of a foreign power.

2.1d Human Experimentation. No element of the Intelligence Community shall conduct, sponsor, fund, or conduct research on human subjects except in accordance with guidelines issued by the Department of Health and Human Services. The subjects informed consent shall be documented as required by these guidelines.

2.1f Assassination or Assassination. No person employed by or acting on behalf of the United States Government shall engage in or conspire to engage in assassination.

2.1g Independent Participation. No element of the Intelligence Community shall participate in or attempt any action to undertake activities prohibited by this Guide.

2.1h Interference or Coercion. No person shall engage in conduct which is intended to influence United States political processes, public opinion, policies, or media.

PART 3 General Provisions

3.1 Congressional Oversight. The duties and responsibilities of the Director and the heads of other departments, services, elements, and offices engaged in intelligence activities in cooperation with the Congress in the conduct of its oversight duties for oversight of intelligence activities shall

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

be implemented in accordance with applicable law, including title V of the Act. The requirements of applicable law, including title V of the Act, shall apply to all covert action activities as defined in this order.

3.1 Implementation. The President, supported by the NSC, and the Director shall issue such appropriate directives, procedures, and guidance as are necessary to implement this order. Heads of elements within the Intelligence Community shall issue appropriate procedures and supplementary guidance consistent with this order. No procedure or implement part 2 of this order shall be issued without the Attorney General's approval, after consultation with the Director. The Attorney General shall provide a statement of reasons for not approving any procedures established by the head of an element in the Intelligence Community for the use of the department containing such elements under the FBI. In instances where the element head or department head and the Attorney General are unable to reach agreement on other than constitutional or other legal grounds, the Attorney General, the head of department concerned, or the Director shall refer the matter to the NSC, and proceed. The activities herein authorized that require procedures shall be conducted in accordance with existing procedures or requirements established under Executive Order 12858. New procedures, as required by Executive Order 12858, as further amended, shall be established as expeditiously as possible. All new procedures promulgated pursuant to Executive Order 12858, as amended, shall be made available to the Select Committee on Intelligence of the Senate and the Permanent Select Committee on Intelligence of the House of Representatives.

3.4 Reference and Transition. References to "Security Guidelines of the Intelligence Community" or "SCGCs" in executive orders or

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

other Presidential guidance, shall be deemed reference to the needs of elements in the Intelligence Community, unless the President otherwise directs; reference to Intelligence Community or Intelligence Community element policies or guidance, shall be deemed to be reference to the needs of elements of the Intelligence Community, unless the President or the Director otherwise directs.

3.1 Definitions. For the purposes of this order, the following terms shall have these meanings:

(a) Counterintelligence means information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations committed for or in behalf of foreign powers, organizations, or persons, or their agents, or international terrorist organizations or activities.

(b) Covert action means an activity or activities of the United States Government to influence political, economic, or military conditions abroad, where it is intended that the role of the United States Government will not be apparent or acknowledged publicly, but does not include:

(i) Activities the primary purpose of which is to acquire intelligence, traditional counterintelligence activities, traditional activities to improve or maintain the operational security of United States Government programs, or administrative activities;

(ii) Traditional diplomatic or military activities or activities support to such activities;

(iii) Traditional law enforcement activities conducted by United States Government law enforcement agencies or police support to such activities; or

(iv) Activities to provide routine support to the overseas activities rather than activities described in

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

paragraph 11. 0.3, to call or text called parties who are not located abroad.

(c) Electronic surveillance means acquisition of a reproducible communication by electronic means without the consent of a person who is a party to an electronic communication or, in the case of a non-electronic communication, without the consent of a person who is visibly present at the place of communication, but not including the use of audio direction finding equipment solely to determine the location of a transmitter.

(d) Employee means a person employed by, assigned or detailed to, or acting for an element within the Intelligence Community.

(e) Foreign intelligence means information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, foreign persons, or international movements.

(f) Intelligence includes foreign intelligence and counterintelligence.

(g) Intelligence activities mean all activities that elements of the Intelligence Community are authorized to conduct pursuant to this order.

(h) Intelligence Community and elements of the Intelligence Community refers to:

- (1) The Office of the Director of National Intelligence;
- (2) The Central Intelligence Agency;
- (3) The National Security Agency;
- (4) The Defense Intelligence Agency;
- (5) The National Geospatial-Intelligence Agency;
- (6) The National Reconnaissance Office;
- (7) The other offices within the Department

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

of Defense for the collection of special source national foreign intelligence through surveillance programs;

(e) The intelligence and counterintelligence elements of the Army, the Navy, the Air Force, and the Marine Corps;

(f) The intelligence elements of the Federal Bureau of Investigation;

(g) The Office of National Security Intelligence of the Drug Enforcement Administration;

(h) The Office of Intelligence and Counterintelligence of the Department of Energy;

(i) The Bureau of Intelligence and Research of the Department of State;

(j) The Office of Intelligence and Analysis of the Department of the Treasury;

(k) The Office of Intelligence and Analysis of the Department of Homeland Security;

(l) The intelligence and counterintelligence elements of the Coast Guard; and

(m) Such other elements of any department or agency as may be designated by the President, or designated jointly by the Director and the head of the department or agency concerned, as an element of the Intelligence Community.

(1) *National Intelligence and Intelligence Related to Domestic Security* means all intelligence, regardless of its source area which is collected and including information gathered within or outside the United States, with personnel, as determined consistent with any guidance issued by the President, or that is determined for the purpose of access to information by the Director in accordance with section 1.3(a)(3) of this order, to provide to more than one United States Government agency; and that involves threats to the United States, its

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

people, property, or interests; the development, production, or use of weapons of mass destruction; or any other matter bearing on United States national or homeland security.

(g) The National Intelligence Program covers all programs, projects, and activities of the Intelligence Community, as well as any other programs of the Intelligence Community designated jointly by the Director and the head of a United States department or agency or by the President. Such term does not include programs, projects, or activities of the military departments to acquire intelligence solely for the planning and conduct of national military operations of United States Armed Forces.

(h) United States person means a United States citizen, or alien known by the intelligence element concerned to be a permanent resident alien, an unincorporated association substantially composed of United States citizens or permanent resident aliens, or a corporation incorporated in the United States, except for a corporation directed and controlled by a foreign government or governments.

3.6 Incorporation. Executive Orders issued and dated August 17, 1956, and November 1, 1956, and paragraphs 1.4(c), (d), and (e) of Part 1 supersede provisions within Executive Order 12958, as amended, to the extent such provisions in Executive Order 12958, as amended, are inconsistent with this Order.

3.7 General Provisions.

(a) Consistent with section 1.3(c) of this Order, nothing in this Order shall be construed to impair or otherwise affect:

- (i) Authority provided by law to a department or agency, or the head thereof; or
- (ii) Functions of the Director of the Office of Management and Budget relating to budget, administration, or legislative proposals.

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

(n) This order shall be implemented consistent with applicable law and subject to the availability of appropriations.

(o) This order is intended only to improve the internal management of the executive branch and is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity, by any party against the United States, its departments, agencies or entities, its officers, employees, or agents, or any other person.

Paul Ronald Reagan

THE WHITE HOUSE
December 4, 1981

This Page is Intentionally Blank.

C APPENDIX C: (U//~~FOUO~~) USE AND TARGETING OF A FEDERAL PRISONER HELD IN THE CUSTODY OF THE BOP OR USMS DURING AN FBI PREDICATED INVESTIGATION; INTERVIEW OF A FEDERAL PRISONER HELD IN THE CUSTODY OF THE BOP OR USMS DURING AN FBI ASSESSMENT OR PREDICATED INVESTIGATION

C.1 (U) OVERVIEW/SUMMARY

(U//~~FOUO~~) **Use and Targeting a Federal Prisoner:** During an FBI predicated investigation, it may be necessary and appropriate to: 1) use a cooperating federal prisoner to gather and obtain evidence and intelligence; or 2) target a federal prisoner. This policy sets forth the approval process for the use of and targeting of a federal prisoner held in the custody of the Bureau of Prisons (BOP) or the United States Marshals Service (USMS).

(U//~~FOUO~~) **Interview a Federal Prisoner:** During an FBI Assessment or predicated investigation, it may be necessary and appropriate to interview a federal prisoner in the custody of the BOP or USMS. This policy sets forth the approval process for the interview of a federal prisoner held in the custody of the BOP or the USMS during an FBI Assessment or predicated investigation.

(U//~~FOUO~~) **Exclusions from this Policy:** This policy does not apply to:

A)

(U//~~FOUO~~)

b7E

C.2 (U) LEGAL AUTHORITY

(U) The FBI is authorized by the Department of Justice (DOJ) to use and target a federal prisoner for investigative purposes and interview a Federal Prisoner (DOJ Memorandum “Use and Targeting of Federal Prisoners in Investigations,” January 22, 2009).

C.3 (U) DEFINITIONS

(U) **Federal Prisoner:** For purposes within this section, a federal prisoner is one who is held in the custody of either the BOP or the USMS pursuant to an order of a court in connection with a criminal matter, regardless of where the person is housed.

(U) **Use of a Federal Prisoner:** Use of a federal prisoner means to employ a federal prisoner during an investigation in such a manner that the prisoner will interact with others who are not members of law enforcement (e.g., the prisoner will engage in a consensually monitored telephone call with a target) or the prisoner will be taken out of the custody of BOP or USMS (e.g., the prisoner is removed from the prison to assist the FBI in locating a hide-out) or law enforcement will interact covertly with the prisoner (e.g., an undercover agent engages with the prisoner in the visiting room of the prison).

(U) **Targeting a Federal Prisoner:** "Targeting" a federal prisoner means that the federal prisoner is the target of the investigation and that investigative activity will directly interact with either the prisoner or the federal facility (e.g., as part of a money laundering investigation targeting a prisoner, the FBI wishes to engage in a consensually monitored conversation with the prisoner).

(U) **Interview of a Federal Prisoner:** Interview of a federal prisoner means to interact with a federal prisoner, overtly representing oneself as an FBI employee, in order to gather information.

C.3.1 (U) *USE AND TARGETING A FEDERAL PRISONER*

(U//~~FOUO~~) An FBI employee may request the use of or the targeting of a federal prisoner in an FBI predicated investigation [REDACTED]

b7E

[REDACTED] See subsection C.4.1 for approval requirements.

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

b7E

C.3.2 (U) *INTERVIEW A FEDERAL PRISONER*

(U//~~FOUO~~) An FBI employee may request to interview a federal prisoner in an FBI Assessment or predicated investigation [REDACTED]

b7E

C.4 (U) *APPROVAL REQUIREMENTS*

C.4.1 (U) *APPROVAL - USE AND TARGETING OF A FEDERAL PRISONER*

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

b7E

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

b7E

[REDACTED] The process is as follows:

A) (U//~~FOUO~~) The FBI field office employee must:

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

b7E

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

b7E

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

b7E

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

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

b7E

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

b7E

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

b7E

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

b7E

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

b7E

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

b7E

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

b7E

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

b7E

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

b7E

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

b7E

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

b7E

(U//~~FOUO~~) Note: The DOJ Memorandum governing the Use and Targeting of Federal Prisoners is labeled “Sensitive Investigative Matter.” This is not a SIM as defined in DIOG Section 10. [REDACTED]

b7E

C.4.2 (U) *APPROVAL - INTERVIEW A FEDERAL PRISONER*

(U//~~FOUO~~) The FBI employee must:

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

b7E

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

b7E

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

b7E

C.5 (U) EXEMPTIONS TO DOJ APPROVAL REQUIREMENT

(U//~~FOUO~~)

b7E

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

b7E

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

b7E

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

b7E

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

b7E

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

b7E

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

b7E

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

b7E

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

b7E

(U)

b7E

(U//~~FOUO~~)

b7E

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

b7E

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

b7E

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

b7E

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

b7E

C.6 (U) EXTENSION REQUESTS

(U//~~FOUO~~) Agents may request extensions of the authority to use or target a prisoner in an FBI investigation

b7E

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

b7E

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

b7E

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

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

b7E

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

b7E

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

b7E

C.7 (U) TRANSPORTATION OF FEDERAL PRISONER

(U//~~FOUO~~) If it is necessary to remove the federal prisoner from the detention facility in which he/she is housed as a part of the investigation [REDACTED]

b7E

[REDACTED]

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

b7E

[REDACTED]

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

b7E

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

b7E

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

b7E

[REDACTED]

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

b7E

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

b7E

[REDACTED]

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

b7E

[REDACTED]

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

b7E

This Page is Intentionally Blank.

**D APPENDIX D: (U) DEPARTMENT OF JUSTICE
MEMORANDUM ON COMMUNICATIONS WITH THE
WHITE HOUSE AND CONGRESS, DATED MAY 11, 2009**

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



Office of the Attorney General
Washington, D. C. 20530

May 11, 2009

MEMORANDUM FOR HEADS OF DEPARTMENT COMPONENTS
ALL UNITED STATES ATTORNEYS

FROM:  THE ATTORNEY GENERAL

SUBJECT: Communications with the White House and Congress

The rule of law depends upon the evenhanded administration of justice. The legal judgments of the Department of Justice must be impartial and insulated from political influence. It is imperative that the Department's investigatory and prosecutorial powers be exercised free from partisan consideration. It is a fundamental duty of every employee of the Department to ensure that these principles are upheld in all of the Department's legal endeavors.

In order to promote the rule of law, therefore, this memorandum sets out guidelines to govern all communications between representatives of the Department, on the one hand, and representatives of the White House and Congress, on the other, and procedures intended to implement those guidelines. (The "White House," for the purposes of this Memorandum, means all components within the Executive Office of the President.) These guidelines have been developed in consultation with, and have the full support of, the Counsel to the President.

1. Pending or Contemplated Criminal or Civil Investigations and Cases

The Assistant Attorneys General, the United States Attorneys, and the heads of the investigative agencies in the Department have the primary responsibility to initiate and supervise investigations and cases. These officials, like their superiors and their subordinates, must be insulated from influences that should not affect decisions in particular criminal or civil cases. As the Supreme Court said long ago with respect to United States Attorneys, so it is true of all those who exercise the Department's investigatory and prosecutorial powers: they are representatives "not of an ordinary party to a controversy, but of a sovereignty whose obligation to govern impartially is as compelling as its obligation to govern at all; and whose interest, therefore, in a criminal prosecution is not that it shall win a case, but that justice shall be done." *Berger v. United States*, 295 U.S. 78, 88 (1935).

a. In order to ensure the President's ability to perform his constitutional obligation to "take care that the laws be faithfully executed," the Justice Department will advise the White House concerning pending or contemplated criminal or civil investigations or cases when—but only when—it is important for the performance of the President's duties and appropriate from a law enforcement perspective.

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

Memorandum for Head of Department Components
All United States Attorneys
Subject: Communications with the White House and Congress

Page 2

b. Initial communications between the Department and the White House concerning pending or contemplated criminal investigations or cases will involve only the Attorney General or the Deputy Attorney General, from the side of the Department, and the Counsel to the President, the Principal Deputy Counsel to the President, the President or the Vice President, from the side of the White House. If the communications concern a pending or contemplated civil investigation or case, the Associate Attorney General may also be involved. If continuing contact between the Department and the White House on a particular matter is required, the officials who participated in the initial communication may designate subordinates from each side to carry on such contact. The designating officials must monitor subsequent contacts, and the designated subordinates must keep their superiors regularly informed of any such contacts. Communications about Justice Department personnel in reference to their handling of specific criminal or civil investigations or cases are expressly included within the requirements of this paragraph. This policy does not, however, prevent officials in the communications, public affairs, or press offices of the White House and the Department of Justice from communicating with each other to coordinate efforts.

c. In order to ensure that Congress may carry out its legitimate investigatory and oversight functions, the Department will respond as appropriate to inquiries from Congressional Committees consistent with policies, laws, regulations, or professional ethical obligations that may require confidentiality and consistent with the need to avoid publicity that may undermine a particular investigation or litigation. Outside the context of Congressional hearings or investigations, all inquiries from individual Senators and Members of Congress or their staffs concerning particular contemplated or pending criminal investigations or cases should be directed to the Attorney General or the Deputy Attorney General. In the case of particular civil investigations or cases, inquiries may also be directed to the Associate Attorney General.

d. These procedures are not intended to interfere with the normal communications between the Department and its client departments and agencies (including agencies within the Executive Office of the President when they are the Department's clients) and any meetings or communications necessary to the proper conduct of an investigation or litigation.

2. National Security Matters

It is critically important to have frequent and expeditious communications relating to national security matters, including counter-terrorism and counter-espionage issues. Therefore communications from (or to) the Deputy Counsel to the President for National Security Affairs, the staff of the National Security Council and the staff of the Homeland Security Council that relate to a national security matter are not subject to the limitations set out above. However, this exception for national security matters does not extend to pending adversary cases in litigation that may have national security implications. Communications related to such cases are subject to the guidelines for pending cases described above.

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

Memorandum for Head of Department Components
All United States Attorneys
Subject: Communications with the White House and Congress

Page 3

3. White House Requests for Legal Advice

All requests from the White House for formal legal opinions shall come from the President, the Counsel to the President, or one of the Deputy Counsels to the President, and shall be directed to the Attorney General and the Assistant Attorney General for the Office of Legal Counsel. The Assistant Attorney General for the Office of Legal Counsel shall report to the Attorney General and the Deputy Attorney General any communications that, in his or her view, constitute improper attempts to influence the Office of Legal Counsel's legal judgment.

4. Communications Involving the Solicitor General's Office.

Matters in which the Solicitor General's Office is involved often raise questions about which contact with the Office of the Counsel to the President is appropriate. Accordingly, the Attorney General and Deputy Attorney General may establish distinctive arrangements with the Office of the Counsel to govern such contacts.

5. Presidential Pardon Matters

The Office of the Pardon Attorney may communicate directly with the Counsel to the President and the Deputy Counsels to the President, concerning pardon matters. The Counsel to the President and the Deputy Counsels to the President may designate subordinates to carry on contact with the Office of the Pardon Attorney after the initial contact is made.

6. Personnel Decisions Concerning Positions in the Civil Service

All personnel decisions regarding career positions in the Department must be made without regard to the applicant's or occupant's partisan affiliation. Thus, while the Department regularly receives communications from the White House and from Senators, Members of Congress, and their staffs concerning political appointments, such communications regarding positions in the career service are not proper when they concern a job applicant's or a job holder's partisan affiliation. Efforts to influence personnel decisions concerning career positions on partisan grounds should be reported to the Deputy Attorney General.

7. Other Communications Not Relating to Pending Investigations or Criminal or Civil Cases

All communications between the Department and the White House or Congress that are limited to policy, legislation, budgeting, political appointments, public affairs, intergovernmental relations, or administrative matters that do not relate to a particular contemplated or pending investigation or case may be handled directly by the parties concerned. Such communications should take place with the knowledge of the Department's lead contact regarding the subject

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

Memorandum for Head of Department Components
All United States Attorneys
Subject: Communications with the White House and Congress

Page 4

under discussion. In the case of communications with Congress, the Office of the Deputy Attorney General and Office of the Assistant Attorney General for Legislative Affairs should be kept informed of all communications concerning legislation and the Office of the Associate Attorney General should be kept informed about important policy communications in its areas of responsibility.

As Attorney General Benjamin Civiletti noted in issuing a similar memorandum during the Carter Administration, these guidelines and procedures are not intended to wall off the Department from legitimate communication. We welcome criticism and advice. What these procedures are intended to do is route communications to the proper officials so they can be adequately reviewed and considered, free from either the reality or the appearance of improper influence.

Decisions to initiate investigations and enforcement actions are frequently discretionary. That discretion must be exercised to the extent humanly possible without regard to partisanship or the social, political, or interest group position of either the individuals involved in the particular cases or those who may seek to intervene against them or on their behalf.

This memorandum supersedes the memorandum issued by Attorney General Mukasey on December 19, 2007, titled *Communications with the White House*.

This Page is Intentionally Blank.

**E APPENDIX E: (U//~~FOUO~~) ATTORNEY GENERAL
MEMORANDUM – REVISED POLICY ON THE USE OR
DISCLOSURE OF FISA INFORMATION, DATED
JANUARY 10, 2008**

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

~~FOR OFFICIAL USE ONLY~~



U.S. Department of Justice
National Security Division

Office of the Assistant Attorney General

Washington, D.C. 20530

January 10, 2008

TO: All United States Attorneys
All National Security Division Attorneys
All Anti-Terrorism Coordinators

CC: Assistant Attorney General, Criminal Division
Assistant Attorney General, Civil Division
Director, Federal Bureau of Investigation

FROM: Kenneth L. Wainstein *KLW*
Assistant Attorney General for National Security

SUBJECT: Revised FISA Use Policy as Approved by the Attorney General

We are pleased to provide the Department of Justice's revised policy on the use or disclosure of information obtained or derived from collections under the Foreign Intelligence Surveillance Act of 1978 (FISA), as approved by the Attorney General today. Also attached is a form for use with respect to notifications that are required under Section I of the revised policy.

This revised policy includes significant changes from current practice that will streamline the process for using FISA information in certain basic investigative processes, while still ensuring that important intelligence and law enforcement interests are protected.

You will note that the revised policy authorizes the use or disclosure of FISA information, under the specific circumstances described in the policy, with notification to NSD and after consultation with the FBI (or other Intelligence Community agencies) for the following investigative processes:

•



b7E

~~FOR OFFICIAL USE ONLY~~

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

~~FOR OFFICIAL USE ONLY~~

-
-
-

b7E

b7E

b7E

As described in the revised policy, the Department continues to require prior authorization from the Assistant Attorney General for National Security (AAG/NSD) for the use or disclosure of FISA information in order to file criminal charges or in post-charge criminal proceedings, as well as in connection with certain investigative processes (*e.g.*, criminal search warrants under Rule 41 of the Federal Rules of Criminal Procedure). The revised policy also requires the prior authorization of the AAG/NSD or his designee for the use or disclosure of FISA information in non-criminal proceedings.

The revised policy was drafted by a Justice Department working group that included representatives from the Attorney General's Advisory Committee of United States Attorneys (AGAC), National Security Division (NSD), Federal Bureau of Investigation (FBI), and Office of Legal Policy (OLP). The working group also consulted with the Office of the Director of National Intelligence (ODNI) in the course of the development of this policy.

The revised policy requires that it be reviewed one year from its effective date and requires NSD to issue guidance on what constitutes information "derived from" FISA collections by March 31, 2008.

As noted in the policy, prosecutors are encouraged to contact the National Security Division at any time in order to obtain guidance regarding this policy and to expedite resolution of any issues.

~~FOR OFFICIAL USE ONLY~~

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

~~FOR OFFICIAL USE ONLY~~



U.S. Department of Justice

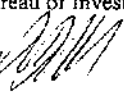
Office of the Attorney General

Washington, D.C. 20530

January 10, 2008

TO: All Federal Prosecutors

CC: Assistant Attorney General, National Security Division
Assistant Attorney General, Criminal Division
Assistant Attorney General, Civil Division
Director, Federal Bureau of Investigation

FROM: Michael B. Mukasey 
Attorney General

SUBJECT: Revised Policy on the Use or Disclosure of FISA Information

As a general matter, it is the policy of the Department of Justice to use all lawful processes in the investigation and prosecution of cases involving terrorism, intelligence, and national security, and to undertake all efforts necessary to protect the American people from the threat posed by foreign powers and their agents, while also exercising due regard for the protection of intelligence sources, methods, and collections, and the privacy and civil liberties of United States persons.

There are important purposes to be served by consultation and coordination with respect to the use or disclosure of FISA information¹ in investigations, criminal prosecutions, and other proceedings. First, because FISA information is almost always classified, the use or disclosure of such information will normally require declassification by the originating agency in accordance with the originating agency's policies and procedures. Second, the use of such information could directly or indirectly compromise intelligence sources, methods, or collections, or disclose the existence or nature of or otherwise compromise an investigation. Third, FISA requires the Government to notify the court and an "aggrieved person" of its intent

¹ The term "FISA information," as used in this policy, means any information acquired, obtained, or derived from collection authorized pursuant to FISA. Whether specific information qualifies as "derived from" FISA collection may be a fact-bound question that depends, at least in part, on the attenuation of the information to be used from the original FISA acquired or obtained information and whether the information was also obtained from an independent source, as well as other factors. Where such a question arises, the application of this policy should be discussed among the USAO, FBI, and NSD, and if consensus is not reached, a determination will be made by the Assistant Attorney General for National Security. Separate guidance regarding what constitutes information "derived from" FISA collection will be issued by the National Security Division no later than March 31, 2008.

~~FOR OFFICIAL USE ONLY~~

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

~~FOR OFFICIAL USE ONLY~~

to use or disclose any FISA information before it is used against such person in a broad range of proceedings. Fourth, the Government is required to ensure that complete and accurate filings are made with the Foreign Intelligence Surveillance Court (FISC), and that the Government complies with all of FISA's statutory requirements. Fifth, it is important to ensure that litigation risks, if any, are properly assessed. Finally, in certain cases, it may be appropriate to make disclosures to a United States District Court regarding classified facts before legal process is obtained.

Given these purposes, it is essential that coordination take place in connection with the use or disclosure of FISA information. Such coordination should be streamlined in order to promote efficient, nimble, and useful investigative activities. The risk of compromising the purposes described above varies depending on the stage of the investigation, criminal prosecution, or other proceeding. As a general matter [REDACTED]

b7E

[REDACTED] federal prosecutors should consider alternative approaches for taking action.

Prosecutors are encouraged to contact the National Security Division at any time in order to obtain guidance regarding this policy and to expedite resolution of any issues.

The following policy is therefore adopted and supersedes any existing Attorney General policies with respect to the use and disclosure of FISA information to the extent that they are inconsistent with this policy:

- (a) the Assistant Attorney General for National Security may act as the Attorney General, as provided for under FISA, *see* 50 U.S.C. § 1801(g), for the purpose of authorizing the use or disclosure of FISA information pursuant to this policy;² and
- (b) federal prosecutors and all others who may seek to use or disclose FISA information in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States, in coordination with NSD and FBI, are authorized to do so pursuant to the terms of this policy, shall coordinate with NSD [REDACTED] and shall comply with the following procedures in matters that involve the use or disclosure of FISA information:³

b7E

² Such authorization may also be provided by the Attorney General, Acting Attorney General, and the Deputy Attorney General. *See* 50 U.S.C. § 1801(g).

³ Nothing in this policy is intended to supersede or replace existing policies for prosecutors regarding notification, consultation, and approval for certain investigative and prosecutive steps, including consultation with other districts where related matters may be under investigation. For example, the United States Attorneys' Manual sets forth when a prosecutor must obtain prior approval for various court actions in national security prosecutions. *See, e.g.,* United States Attorneys' Manual (USAM) §§ 9-2.131 ("Matters Assumed by Criminal Division or Higher

~~FOR OFFICIAL USE ONLY~~

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

~~FOR OFFICIAL USE ONLY~~

I. Use or Disclosure of FISA Information Requiring Consultation with FBI or other Intelligence Community Agencies and Notification to NSD

- A. Certain investigative processes present only moderate risks. As a result, where FISA information is used or disclosed in connection with the processes described below, consultation with FBI (or other Intelligence Community agencies, as appropriate)⁴ and notice to NSD is required:

1.

b7E

2.

b7E

3.

b7E

4.

b7E

- B. Where FISA information is used or disclosed in connection with the processes described above, the following notification process shall be followed:

1.

b7E

Authority"); 9-2.136 ("Investigative and Prosecutive Policy for International Terrorism Matters"); 9-2.155 ("Sensitive Matters"); 9-2.400 ("Prior Approvals Chart").

⁴ For the purposes of this document, the term "Intelligence Community agencies" refers to the appropriate agencies within the Intelligence Community, including the Office of the Director of National Intelligence. Consultation with Intelligence Community agencies other than the FBI is typically appropriate when the sources, methods, or collections involve Intelligence Community agencies other than the FBI. Prosecutors are encouraged to contact the National Security Division, as needed, to assist with the consultation process with the FBI or other Intelligence Community agencies.

⁵ Some courts require a significant measure of information with respect to [redacted] beyond the disclosure of [redacted] To the extent that applications in such districts require the disclosure of additional FISA information [redacted] advance authorization as provided for in Section II of this policy is required prior to such applications being made to the court.

b7E

~~FOR OFFICIAL USE ONLY~~

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

~~FOR OFFICIAL USE ONLY~~

2. As provided on the attached draft [redacted] the federal prosecutor must indicate that he or she has [redacted]
[redacted] b7E
3. [redacted] b7E
above—to ensure that NSD complies with potential obligations to notify the Foreign Intelligence Surveillance Court.
- C. Where consultations with the FBI (or other Intelligence Community agencies, as appropriate) demonstrate that [redacted] b7E
[redacted]
further consultation that includes NSD (working with Intelligence Community agencies, as appropriate) shall take place prior to the use of such processes.
1. [redacted] b7E
- D. This section does not permit the use or disclosure of FISA information obtained [redacted] b7E
[redacted] Federal prosecutors must seek specific, separate use authority from the Assistant Attorney General for National Security prior to initiating any criminal proceedings.
- II. Use or Disclosure of FISA Information Requiring the Advance Authorization of the Assistant Attorney General for National Security
- A. The advance authorization of the Assistant Attorney General for National Security is required where FISA information is [redacted] b7E
[redacted]

[redacted] b7E

~~FOR OFFICIAL USE ONLY~~

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

~~FOR OFFICIAL USE ONLY~~

1. *Investigative Processes Requiring Advance Authorization*

- a. [redacted] As a result, authorization of the Assistant Attorney General for National Security is required before FISA information is used or disclosed in connection with the processes described below:

b7E

i. [redacted]

b7E

ii. [redacted] Title 18, Chapter 119, United States Code;

b7E

iii. [redacted] Title 18, Chapter 121, United States Code;

b7E

iv. [redacted] Rule 41 of the Federal Rules of Criminal Procedure;

b7E

v. [redacted] 18 U.S.C. § 3144;

b7E

vi. [redacted]

b7E

vii. [redacted]

b7E

2. *Criminal Indictments and Post-Indictment Proceedings*

- a. The use or disclosure of FISA information [redacted]
[redacted] As a result, the advance authorization of the Assistant Attorney General for National Security is required before such use or disclosure.

b7E

- b. This advance authorization requirement applies to [redacted]

b7E

[redacted]

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

~~FOR OFFICIAL USE ONLY~~

3. Among the factors that will be considered with respect to granting use authority are: [REDACTED]

b7E

4. Because the process of obtaining advance authorization will require NSD to coordinate with Intelligence Community agencies, federal prosecutors should seek such advance authorization at the earliest juncture possible. In addition, because the use of such information will normally require

b7E

- a. Prosecutors are encouraged to contact NSD at any time in order to obtain guidance regarding this policy and to expedite resolution of any issues.
- b. Where advance authorization involving [REDACTED] [REDACTED] NSD shall provide notice of such request to ODNI.

b7E

III. Use or Disclosure of FISA Information In Non-Criminal Proceedings

- A. [REDACTED] Therefore, authorization of the Assistant Attorney General for National Security or his designee is required before such use or disclosure.

b7E

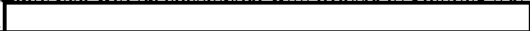
1. [REDACTED]

b7E

~~FOR OFFICIAL USE ONLY~~

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

~~FOR OFFICIAL USE ONLY~~

2. Among the factors that will be considered with respect to granting use authority are: 

3. Because the process of obtaining advance authorization will require NSD to coordinate with Intelligence Community agencies, the attorney for the government should seek such advance authorization at the earliest juncture possible. In addition, because the use of such information will normally require 

 - a. Prosecutors are encouraged to contact NSD at any time in order to obtain guidance regarding this policy and to expedite resolution of any issues.
 - b. Where advance authorization involving particularly sensitive sources, methods, or collections is requested, NSD shall provide notice of such request to ODNI.
- This policy shall be reviewed one year from its effective date to evaluate its effectiveness.

b7E

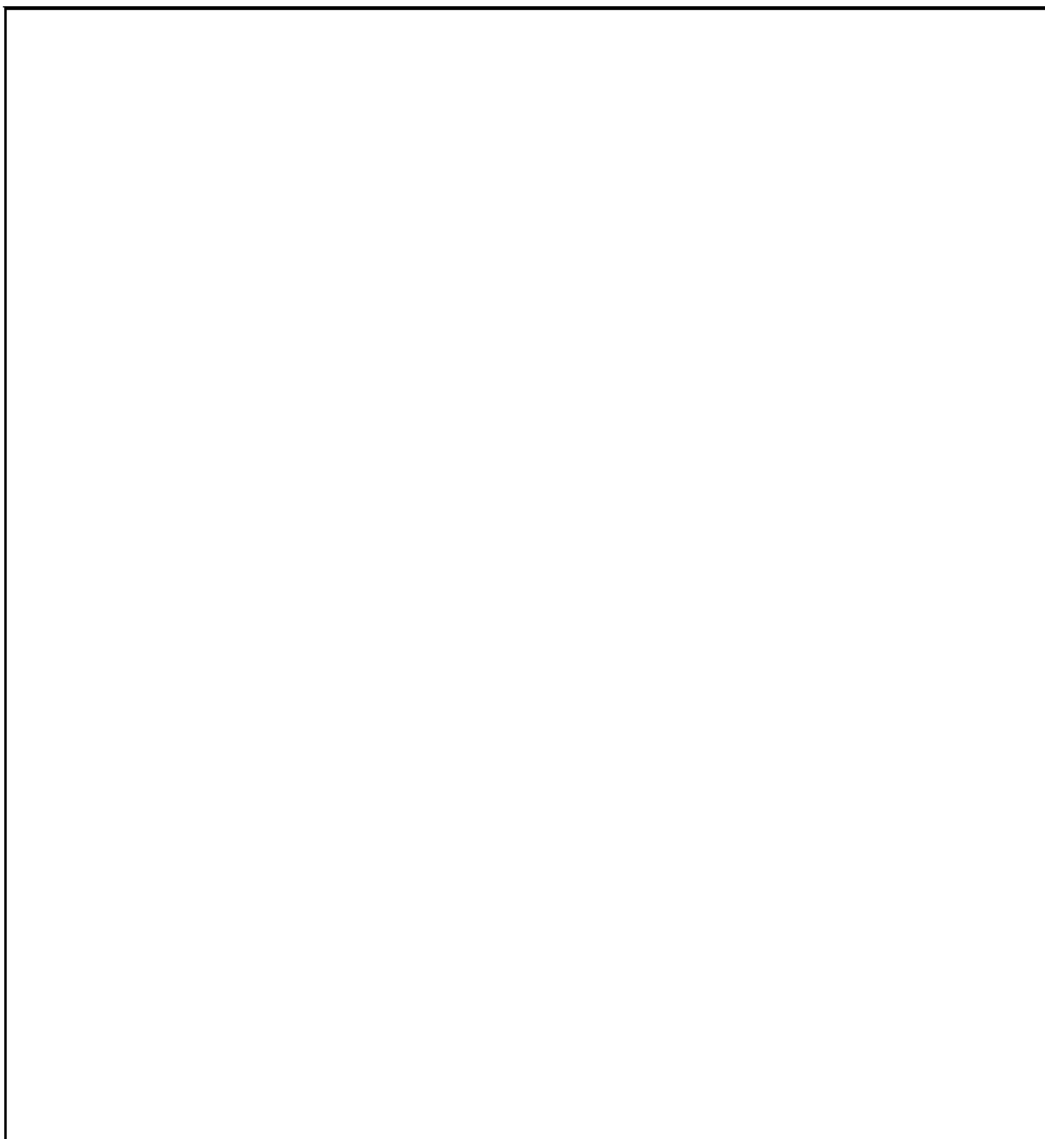
b7E

~~FOR OFFICIAL USE ONLY~~

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

Classification:

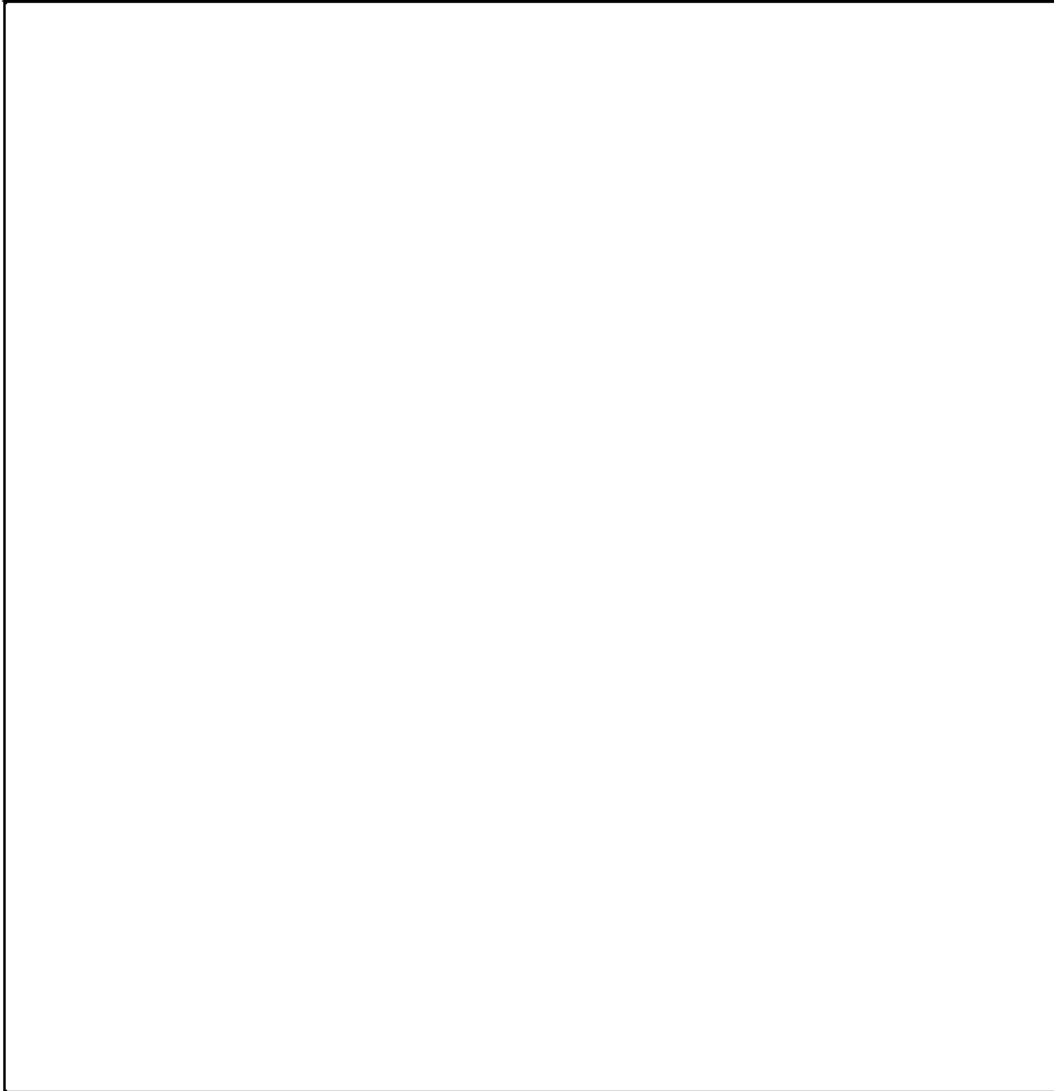
NOTIFICATION OF USE OR DISCLOSURE OF FISA INFORMATION FORM



b7E

Classification:

Classification:



b7E

Classification:

This Page is Intentionally Blank.

F APPENDIX F: (U) DOJ POLICY ON USE OF FORCE

F.1 (U) USE OF LESS-THAN-LETHAL DEVICES

(U) Deputy Attorney General's Memorandum on Use of Less-than-Lethal Devices dated 4/21/2011.

F.2 (U) USE OF DEADLY FORCE

(U) Deadly Force Policy, dated 7/1/2004.

F.3 (U) TRAINING

A) (U) Deadly Force Policy Training Material, dated 7/29/2004.

B) (U) Instructional Outline and Use of Force Scenarios

F.1 (U) USE OF LESS-THAN-LETHAL DEVICES

(U) Deputy Attorney General's Memorandum on Use of Less-than-Lethal Devices dated 4/21/2011.

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



U.S. Department of Justice
Office of the Deputy Attorney General

The Deputy Attorney General

Memorandum

May 18, 2011

MEMORANDUM FOR: Robert S. Mueller III
Director
Federal Bureau of Investigation

Michael M. Antonetti
Administrator
Drug Enforcement Administration

Kenneth F. Melsen
Acting Director
Bureau of Alcohol, Tobacco, Firearms and Explosives

Kevin A. Gynon
Director
United States Marshals Service

Thomas R. Kane
Acting Director
Federal Bureau of Prisons

FROM: James M. Cole
Deputy Attorney General

SUBJECT: Enforcement of Law of Law Enforcement Detainees

Attached is the Department's Policy on the Use of Law-Enforcement Detainees, approved by the Attorney General on April 21, 2011. Please ensure that this policy is distributed to every affected employee within your component.

Attachment

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

DEPARTMENT OF JUSTICE POLICY STATEMENT
ON THE USE OF LESS-THAN-LETHAL DEVICES

- I. Department of Justice (DOJ) law enforcement officers/officers are authorized to use less-than-lethal devices only as consistent with this policy statement.
- II. Pursuant to this policy statement, less-than-lethal devices:
 - a. Are synonymous with "less lethal," "non-lethal," "non-deadly," and other terms referring to devices used in situations covered by this policy statement; and
 - b. Include, but are not limited to:
 1. Impact Devices (e.g., batons, bean bag projectiles, bean launchers, rubber projectiles, etc.);
 2. Stimulus Agents (e.g., tear gas, pepper spray, pyrotechnics); and
 3. Conducted Energy Device (e.g., electronic stunbatons, etc.).
- III. DOJ officers are authorized to use less-than-lethal devices only in those situations where reasonable force, based on the totality of the circumstances at the time of the incident, is necessary to effectuate an arrest, obtain lawful compliance from a subject, or protect any person from physical harm. Use of less-than-lethal devices must cease when it is no longer necessary to achieve the law enforcement objective.
- IV. DOJ officers are authorized to use only those less-than-lethal devices authorized by their department and that they are trained to use, absent exigent circumstances.
- V. DOJ officers are not authorized to use less-than-lethal devices if doing so would be likely to cause death or serious physical injury to any person. DOJ officers are prohibited from using less-than-lethal devices to punish, harass, or abuse any person.
- VI. Less-than-lethal devices are used with a reasonable expectation that death or serious bodily injury will not

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

result. They are, however, recognized as having the potential to cause death or serious bodily injury, and OIG officers may use less-than-lethal devices as deadly weapons only when authorized under the OIG Policy Statement on the use of deadly force.

- VII. OIG officers must make necessary medical assistance available to subjects of less-than-lethal device use as soon as practicable.
- VIII. OIG components must establish rules and procedures implementing this policy statement. Each component will ensure that state/local officers participating in joint task force operations are aware of and adhere to the policy and its limits on OIG officers.
- IX. OIG components must establish training programs and procedures for using less-than-lethal devices that are consistent with this policy statement and federal law.
- X. OIG components must individually establish procedures for documenting, reporting, reviewing, and investigating (as warranted), all incidents involving the use of less-than-lethal devices.
- XI. This policy statement is not intended to, nor does it, create any right or benefit, substantive or procedural, enforceable at law or in equity, against the United States, its departments, agencies, or other entities, its officers or employees, or any other person.

F.2 (U) USE OF DEADLY FORCE

(U) Deadly Force Policy, dated 7/1/2004.

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

POLICY STATEMENT USE OF DEADLY FORCE
Approved by the Attorney General July 1, 2004

GENERAL PRINCIPLES

- I. Law enforcement officers and correctional officers of the Department of Justice may use deadly force only when necessary, that is, when the officer has a reasonable belief that the subject of such force poses an imminent danger of death or serious physical injury to the officer or to another person.
 - A. Deadly force may not be used solely to prevent the escape of a fleeing suspect.
 - B. Firearms may not be fired solely to disable moving vehicles.
 - C. If feasible and if to do so would not increase the danger to the officer or others, a verbal warning to submit to the authority of the officer shall be given prior to the use of deadly force.
 - D. Warning shots are not permitted outside of the prison context.
 - E. Officers will be trained in alternative methods and tactics for handling resisting subjects, which must be used when the use of deadly force is not authorized by this policy.

CUSTODIAL SITUATIONS

- II. Unless force other than deadly force appears to be sufficient, deadly force may be used to prevent the escape of a prisoner committed to the custody of the Attorney General or the Bureau of Prisons
 - A. if the prisoner is effecting his or her escape in a manner that poses an imminent danger to the safety of the officer or another person; or
 - B. if the prisoner is escaping from a secure facility or is escaping while in transit to or from a secure facility.
- III. If the subject is in a non-secure facility, deadly force may be used only when the subject poses an imminent danger of death or serious physical injury to the officer or another person.
- IV. If the subject is in transit to or from a non-secure facility and is not accompanied by a person who is in transit to or from a secure facility, deadly force may be used only when the subject poses an imminent danger of death or serious physical injury to the officer or to another person.

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

- V. After an escape from a facility or vehicle and its immediate environs has been effected, officers attempting to apprehend the escaped prisoner may use deadly force only when the escaped prisoner poses an imminent danger of death or serious physical injury to the officer or another person.
- VI. Deadly force may be used to maintain or restore control of a prison or correctional facility when the officer reasonably believes that the intended subject of the deadly force is participating in a disturbance in a manner that threatens the safety of the officer or another person.
- VII. In the prison context, warning shots may be fired within or in the immediate environs of a secure facility if there is no apparent danger to innocent persons: (A) if reasonably necessary to deter or prevent the subject from escaping from a secure facility; or (B) if reasonably necessary to deter or prevent the subject's use of deadly force or force likely to cause serious physical injury.

APPLICATION OF THE POLICY

- VIII. This policy is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or equity, against the United States, its departments, agencies, or other entities, its officer or employees, or any other person.

F.3 (U) TRAINING

A) (U) Deadly Force Policy Training Material, dated 7/29/2004.

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

(Rev 01-31-2003)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 07/29/2004

To: All Divisions

Attn: AD
ADIC
SAC
CDC
PFI
FBIHQ, Manuals Desk
FBIHQ, Manuals Desk

From: General Counsel
Legal Instruction Unit
Contact: [REDACTED]

Approved By: Caproni, Valerie E
[REDACTED]

Drafted By: [REDACTED]

Case ID #: 66F-HQ-1312253
66F-HQ-C1384970
66F-HQ-C1384970

Title: REVISIONS TO THE DEPARTMENT OF
JUSTICE DEADLY FORCE POLICY -
DISSEMINATION OF TRAINING MATERIALS

Synopsis: This Electronic Communication (EC) provides recipients with training materials incorporating the revisions approved on July 1, 2004 to the Department of Justice (DOJ) Deadly Force Policy.

Reference: 66F-HQ-1312253 Serial 8

Enclosure(s): One copy of an instructional outline and one copy of use of force scenarios provided to all recipients for training purposes.

Details: As discussed in the referenced EC, dated 7/7/2004, on July 1, 2004, the Attorney General approved a revised Policy Statement on the use of Deadly Force. In order to assist Field Offices in providing training and guidance on the practical application of the Deadly Force Policy in light of the revised language, the Legal Instruction Unit (LIU), Office of the General Counsel, revised training materials used with the prior Policy Statement to reflect the changes approved by the Attorney General.

b6
b7C
b7E

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

To: All Divisions From: General Counsel
Re: 66F-HQ-1312253, 07/29/2004

The training materials consist of an Instructional Outline and a set of 13 factual scenarios with a discussion of the use of force within the scenario and whether its use violates the policy. This material is similar to what was used for instructional purposes since 12/1/1995. The revised material reflects what was noted in the EC, that the revised policy does not expand or contract the current justification for the use of deadly force. Nonetheless, revisions to the training materials were necessary in order to describe the application of deadly force consistent with the new more succinct policy statement.

The revisions to the training materials primarily relate to the elimination of the "safe alternative" language as a function of the "necessity" for use of deadly force and elimination of language addressing the use of deadly force to prevent the escape of a fleeing felon. For a more detailed discussion of the nature of the revised Policy Statement and the basis for these revisions, refer to the referenced EC.

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

To: All Divisions From: General Counsel
Re: 66F-HQ-1312253, 07/29/2004

LEAD(s):

Set Lead 1: (Action)

ALL RECEIVING OFFICES

It is requested that this communication be distributed
to all appropriate personnel.

♦♦

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

DEADLY FORCE POLICY
TRAINING MATERIAL - 7-29-2004

DEPARTMENT OF JUSTICE DEADLY FORCE POLICY¹

Law enforcement officers of the Department of Justice may use deadly force only when necessary, that is, when the officer has a reasonable belief that the subject of such force poses an imminent danger of death or serious physical injury to the officer or to another person.

- A. **Deadly force may not be used solely to prevent the escape of a fleeing suspect.**
- B. **Firearms may not be fired solely to disable moving vehicles.**
- C. **If feasible and to do so would not increase the danger to the officer or others, a verbal warning to submit to the authority of the officer shall be given prior to the use of deadly force.**
- D. **Warning shots are not permitted²**
- E. **Officers will be trained in alternative methods and tactics for handling resisting subjects which must be used when the use of deadly force is not authorized by this policy.**

This policy is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity, against the United States, its departments, agencies, or other entities, its officers or employees, or any other person.

¹Department of Justice Policy Statement Use of Deadly Force (07-01-2004) in pertinent part (Language relating to Custodial Situations has been intentionally omitted pursuant to FBI policy. See, 66F-HQ-1312253, EC from the Director's Office to All Divisions, titled "REVISIONS TO THE DEPARTMENT OF JUSTICE DEADLY FORCE POLICY", dated 07-07-2004).

²Not included in the above description is the policy relating to the use of deadly force to prevent the escape of a prisoner committed to the custody of the Attorney General or the Bureau of Prisons. Because Agents will seldom find themselves in a position to apply the custodial aspect of the policy, the FBI will adhere to the policy decision set forth in the Airtel from the Director to All Field Offices, titled "Deadly Force Policy Matters," dated 1-5-95, which states "A policy decision has been made that except in cases of prison unrest which would principally involve HRT and/or SWAT, FBI Agents should adhere to the policy and training principles governing the use of deadly force in non-custodial situations."

F.4 (U) TRAINING

B) (U) Instructional Outline and Use of Force Scenarios.

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

07/29/2004

INSTRUCTIONAL OUTLINE

I. INTRODUCTION

The following general principles shall guide the interpretation and application of this policy:

- A. This policy shall not be construed to require Agents to assume unreasonable risks to themselves.
- B. The reasonableness of an Agent's decision to use deadly force must be viewed from the perspective of the Agent on the scene without the benefit of 20/20 hindsight.
- C. Allowance must be made for the fact that Agents are often forced to make split-second decisions in circumstances that are tense, uncertain, and rapidly evolving.

II. DEFINITIONS

- A. "DEADLY FORCE": Is force that is reasonably likely to cause death or serious physical injury.
- B. "REASONABLE BELIEF": Is synonymous with "Probable Cause". It is determined by a totality of the facts and circumstances known to Agents at the time, and the logical inferences that may be drawn from them.
- C. "NECESSARY": The necessity to use deadly force based on the existence of a reasonable belief that the person against whom such force is used poses an imminent danger of death or serious physical injury to the Agent or other persons.
- D. "IMMINENT DANGER": "Imminent" does not mean "immediate" or "instantaneous", but that an action is pending. Thus, a subject may pose an imminent danger even if he is not at that very moment pointing a weapon at the Agent. For example, imminent danger may exist if Agents have probable cause to believe any of the following:

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

1. The subject possess a weapon, or is attempting to gain access to a weapon, under circumstances indicating an intention to use it against the Agents or others; or.
2. The subject is armed and running to gain the tactical advantage of cover; or.
3. A subject with the capability of inflicting death or serious physical injury--or otherwise incapacitating agents--without a deadly weapon, is demonstrating an intention to do so; or.
4. The subject is attempting to escape from the vicinity of a violent confrontation in which the suspect inflicted or attempted the infliction of death or serious physical injury.

III APPLICATION OF DEADLY FORCE

In assessing the necessity to use deadly force, the following practical considerations are relevant to its proper application:

A. Inherent Limitation on Abilities to Assess the Threat and Respond.

1. Limited Time (Action v. Reaction) - there will always be an interval of time between a subject's action and an Agent's ability to perceive that action, to assess its nature, and to formulate and initiate an appropriate response. The inherent disadvantage posed by the action reaction factor places a significant constraint on the time frame within which Agents must perceive, assess and react to a threat.
2. Limited Means (Wound Ballistics) - When the decision is made to use deadly force, Agents have *no guaranteed means of instantaneously stopping the threat*. The human body can sustain grievous - even ultimately fatal - injury and continue to function for a period of time (from several seconds to several minutes) depending on the location, number, and severity of the wounds. The lack of a reliable means of instantaneously stopping the threat, may extend the time that imminent danger can persist. This factor further constrains the time frame within which Agents must respond to a perceived threat.

B. Achieving Intended Purpose.

1. Deadly force may only be applied for the intended purpose of bringing an imminent danger of death or serious physical injury to a timely halt either through the surrender of the subject or through physiological incapacitation.

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

If the subject does not surrender, the only reliable means of achieving that goal is to cause physiological incapacitation of the subject(s) as quickly as possible. Attempts to do anything else - such as shooting to cause minor injury - are unrealistic and can risk exposing Agents or others to continued danger of death or serious physical injury.

2. When the circumstances justify the use of deadly force, Agents should continue its application until the imminent danger is ended through the surrender or physiological incapacitation of the subject(s).

C. Consideration of Risk to Other Parties.

Even when deadly force is permissible, Agents should assess whether its use creates a danger to third parties that outweighs the likely benefits of its use.

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

SCENARIO #1:

b5
b7E

DISCUSSION:

b7E

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

SCENARIO #2:

b5
b7E

DISCUSSION:

b7E

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

SCENARIO #3:

b5
b7E

DISCUSSION:

b7E

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

SCENARIO #4:

b5
b7E

DISCUSSION:

b7E

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

SCENARIO #5:

b5
b7E

DISCUSSION:

b7E

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

SCENARIO #6:

b5
b7E

DISCUSSION:

b7E

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

SCENARIO #7:

b5
b7E

DISCUSSION:

b7E

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

SCENARIO #8:

b5
b7E

DISCUSSION:

b7E

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

SCENARIO #9:

b5
b7E

DISCUSSION:

b7E

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

SCENARIO #10:

b5
b7E

DISCUSSION:

b7E

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

SCENARIO #11:

b5
b7E

DISCUSSION:

b7E

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

SCENARIO #12:

b5
b7E

DISCUSSION:

b7E

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

SCENARIO #13:

b5
b7E

DISCUSSION:

b7E

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

SCENARIO #14:

b5
b7E

DISCUSSION:

b7E

This Page is Intentionally Blank.

~~SECRET//NOFORN~~

Domestic Investigations and Operations Guide

§G



CLASSIFIED BY: NSICG
REASON: 1.4 (C,D)
DECLASSIFY ON: 12-31-2045
DATE: 06-14-2022

b6
b7C

(U) DOMESTIC INVESTIGATIONS AND OPERATIONS GUIDE

(U) Appendix G

(U) Classified Provisions

(U) Version Dated: March 31, 2020

(U) Updated: February 24, 2022

~~SECRET//NOFORN~~

APPENDIX G: (U) CLASSIFIED PROVISIONS

(U) This Part supplements the unclassified provisions of the AGG-Dom and DIOG.

(U) Table of Contents

G.1	(U) Limitation on Certain Searches	3
G.2	(U) Circumstances Warranting a Preliminary or Full Investigation.....	4
G.3	(U) Determination of United States Person (USPER) Status	5
(U) G.4	(S//NF) Attorney General Threat Country List.....	6
G.5	(U) Assistance to and/or from Foreign Agencies in the United States	7
G.6	(U) Consensual Monitoring.....	8
G.7	(U) Sensitive Investigative Matters (SIM).....	9
G.8	(U) Data Analysis.....	11
G.9	(U) Notice Requirements for the DOJ National Security Division (NSD).....	12
G.10	(U) [REDACTED]	13
G.11	(U) [REDACTED] (CIA and NSA).....	14
G.12	(U) National Security Letters for Telephone Toll Records of Members of the News Media or News Organizations	15
G.13	(U) Other Investigative Resources.....	18
G.14	(U// FOUO) Counterintelligence Subject Type 5 Assessment (Formerly Recruitment-in-Place [RIP] Type 5 Assessments).....	19

b7E

~~Derived from: Multiple Sources~~

~~Declassify on: December 1, 2033~~

G.1 (U) LIMITATION ON CERTAIN SEARCHES

G.1.1 (U) *CLASSIFIED AGG-DOM PROVISION*

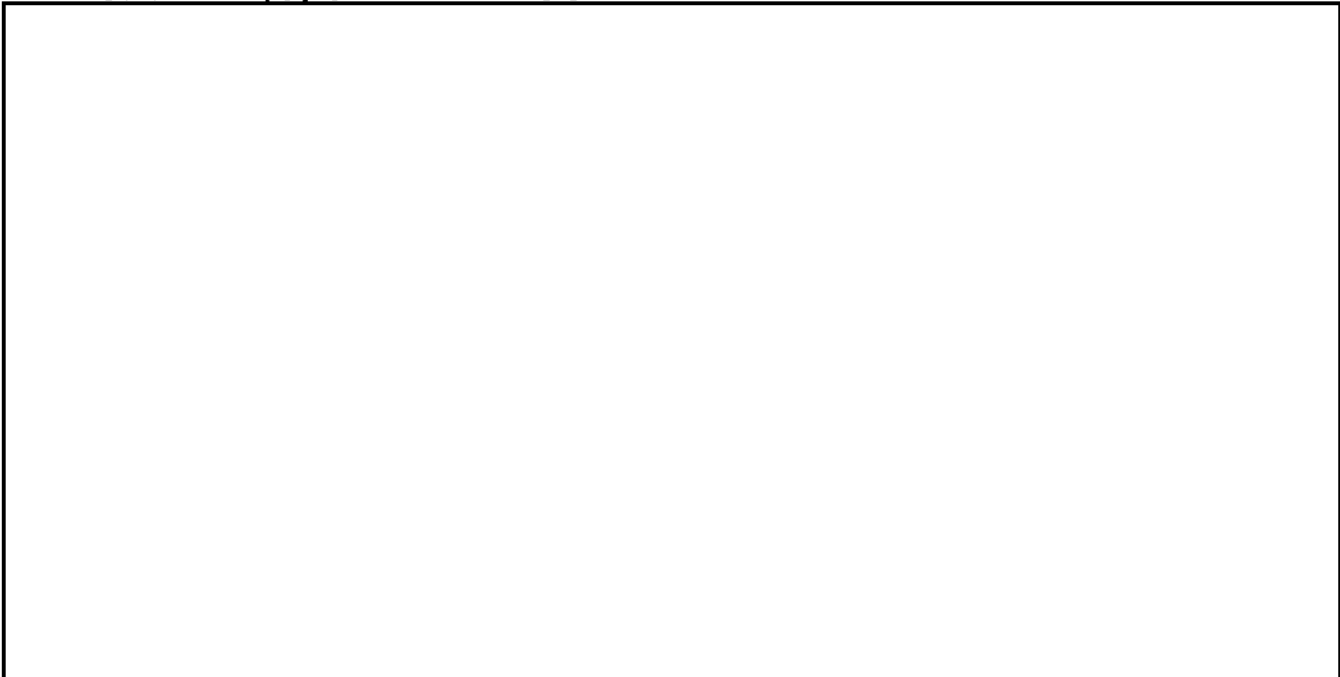
b1
b3

G.1.2 (U) *DIOG CLASSIFIED PROVISION*

(U) Refer to the Domestic Investigations and Operations Guide (DIOG) Section 18.7.1 for procedures to obtain a FISA search warrant.

G.2 (U) CIRCUMSTANCES WARRANTING A PRELIMINARY OR FULL INVESTIGATION

G.2.1 (U) CLASSIFIED AGG-DOM PROVISION



b1
b3

G.2.2 (U) DIOG CLASSIFIED PROVISION

(U) The provisions of DIOG Sections 6 (Preliminary Investigations) or 7 (Full Investigations) with regard to the purpose, approval and notification requirements apply fully to investigations predicated under this provision.

G.3 (U) DETERMINATION OF UNITED STATES PERSON (USPER) STATUS

G.3.1 (U) *CLASSIFIED AGG-DOM PROVISION*

b1
b3



G.4 ~~(S//NF)~~ ATTORNEY GENERAL THREAT COUNTRY LIST

G.4.1 ~~(S//NF)~~ (U) CLASSIFIED AGG-DOM PROVISION

[Redacted Content]

b1
b3

G.4.2 (U) DIOG CLASSIFIED PROVISION

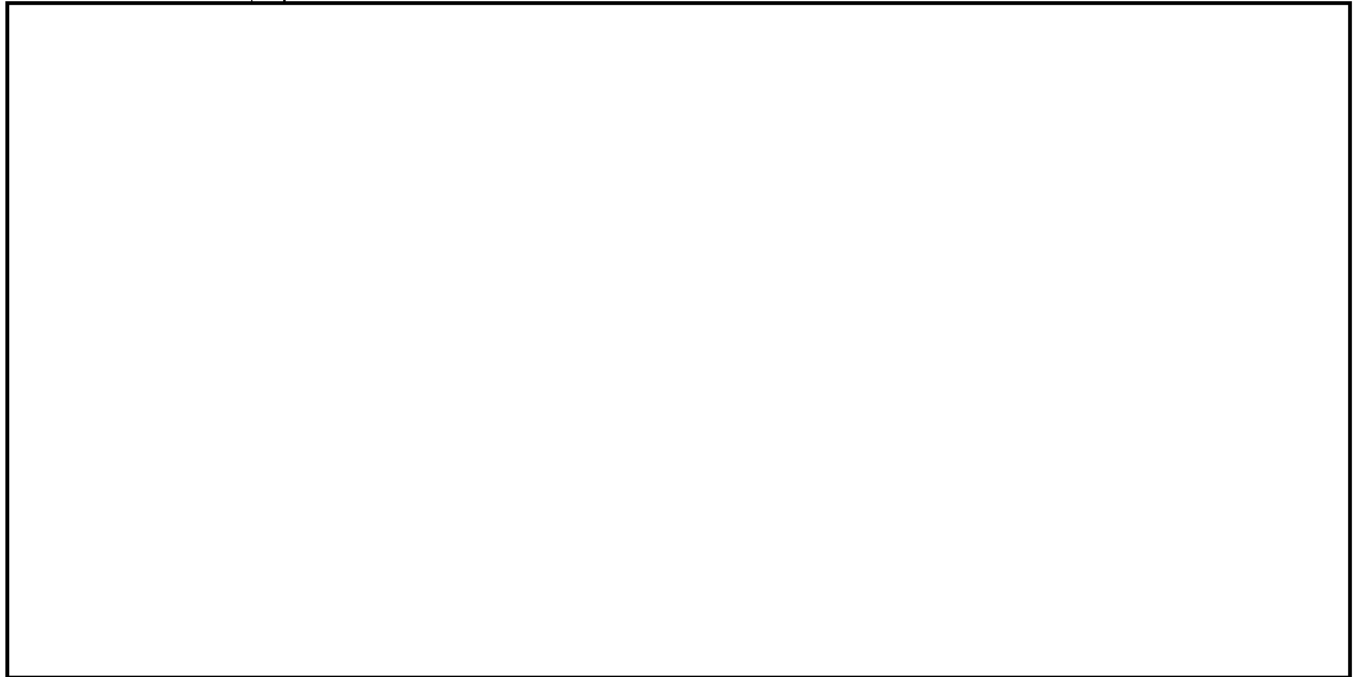
[Redacted Content]

b1
b3

G.5 (U) ASSISTANCE TO AND/OR FROM FOREIGN AGENCIES IN THE UNITED STATES

G.5.1 (U) *DIOG CLASSIFIED PROVISION*

b1
b3



G.6 (U) CONSENSUAL MONITORING

G.6.1 (U) *DIOG CLASSIFIED PROVISION*



b1
b3

G.7 (U) SENSITIVE INVESTIGATIVE MATTERS (SIM)

G.7.1 (U) DIOG CLASSIFIED PROVISION

b1
b3G.7.1.1 (U//~~FOUO~~) MEMBER OF THE NEWS MEDIA OR A NEWS ORGANIZATION

(U//~~FOUO~~) DIOG Section 10.1.2.2.5 defines a member of the news media or a news organization as a SIM. It further defines a member of the news media or a news organization as:

(U//~~FOUO~~) "News media" includes persons and organizations that gather, report or publish news, whether through traditional means (e.g., newspapers, radio, magazines, news service) or the on-line or wireless equivalent. A "member of the media" is a person who gathers, reports, or publishes news through the news media.

(U//~~FOUO~~) The term "News Media" also includes an entity organized and operated for the purpose of gathering, reporting or publishing news. The definition does not, however, include a person or entity who posts information or opinion on the Internet in blogs, chat rooms or social networking sites, such as YouTube, Facebook, or MySpace, unless that person or entity falls within the definition of a member of the media or a news organization under the other provisions within this section (e.g., a national news reporter who posts on his/her personal blog).

(U//~~FOUO~~) Examples of news media entities include television or radio stations broadcasting to the public at large and publishers of newspapers or periodicals that make their products available to the public at large in print form or through an Internet distribution. A freelance journalist may be considered to work for a news organization if the journalist has a contract with the news entity or has a history of publishing content. Publishing a newsletter or operating a website does not by itself qualify an individual as a member of the news media. Businesses, law firms, and trade associations offer newsletters or have websites; these are not considered news media. As the term is used in the DIOG, "news media" is not intended to include persons and entities that simply make information available. Instead, it is intended to apply to a person or entity that gathers information of potential interest to a segment of the general public, uses editorial skills to turn raw materials into a distinct work, and distributes that work to an audience, as journalism professional. If there is doubt about whether a particular person or entity should be considered part of the "news media," the doubt should be resolved in favor of considering the person or entity to be the "news media."

G.7.1.1.

b1
b3

G.7.1.2 (U) ACADEMIC NEXUS

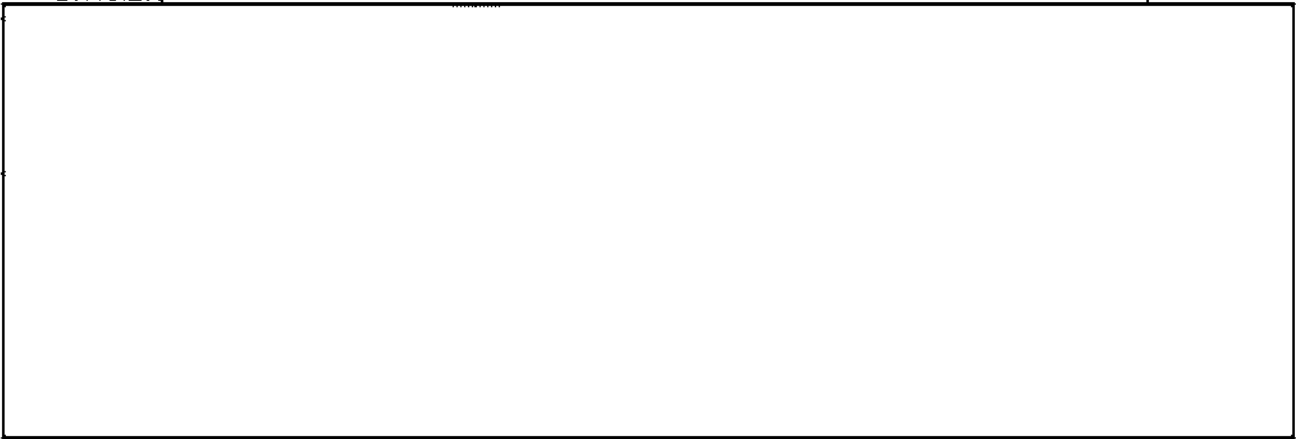
(U//~~FOUO~~) DIOG Section 10.1.2.2.6 states:

(U ~~FOUO~~) *Academic Nexus* As a matter of FBI policy, an investigative activity having an "academic nexus" is a SIM if:

(i) (U ~~FOUO~~) the investigative activity involves matters related to the responsibilities of an administrator or faculty member employed by any college or university that is located inside the United States, provided the matter under Assessment investigation is related to the individual's position at the institution; or

(ii) (U ~~FOUO~~) the matter involves any student association recognized and approved by a college or university at which the student association at issue is located, and the college or university is located inside the United States.

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


G.7.1.2.1 

G.8 (U) DATA ANALYSIS

G.8.1 (U) *DIOG CLASSIFIED PROVISION*

(U) ~~(S//NF)~~ Data analysis conducted by the FBIHQ Counterintelligence Division, such as [REDACTED] must be coordinated with the FBIHQ Office of the General Counsel, Privacy and Civil Liberties Unit and the National Security Law Branch regarding the proper documentation and disposition of such analysis.

b1
b3

G.9 (U) NOTICE REQUIREMENTS FOR THE DOJ NATIONAL SECURITY DIVISION (NSD)**G.9.1 (U) DIOG CLASSIFIED PROVISION**

- (U) C) ~~(S)~~ **Sensitive Investigative Matter:** For a national security investigation or "assistance to other agencies" involving a sensitive investigative matter that is classified "Secret," the appropriate FBIHQ section must send electronic notice to DOJ NSD at [REDACTED] For a national security investigation or "assistance to other agencies" involving a sensitive investigative matter that is classified "Top Secret," the appropriate FBIHQ section must send electronic notice to DOJ NSD at [REDACTED] Notices to DOJ NSD must contain only the Letterhead Memorandum (LHM); the electronic communication (EC) should not be sent to DOJ NSD. b7E
- (U) D) ~~(S)~~ **National Security Full Investigation of a United States Person (USPER):** For a Full Investigation of a USPER relating to a threat to the national security (this reporting requirement does not apply to full positive foreign intelligence investigations) that is classified "Secret," the appropriate FBIHQ section must send electronic notice to DOJ NSD at [REDACTED] For a Full Investigation of a USPER relating to a threat to the national security that is classified "Top Secret," the appropriate FBIHQ section must send electronic notice to DOJ NSD at [REDACTED] Notices to DOJ NSD must only contain the LHM; the EC should not be sent to DOJ NSD. b7E
- (U) E) ~~(S)~~ **Assistance to a Foreign Agency:** When FBIHQ approval is required to provide assistance to a foreign agency in a matter involving a threat to the national security, notice must be provided to DOJ NSD. For a foreign assistance matter that is classified "Secret," the appropriate FBIHQ division approving the investigative method must send electronic notice to DOJ NSD at [REDACTED] For a foreign assistance matter that is classified "Top Secret," the appropriate FBIHQ division approving the investigative method must send electronic notice to DOJ NSD at [REDACTED] Notices to DOJ NSD must only contain the LHM; the EC should not be sent to DOJ NSD. b7E

G.10 (U) [REDACTED]

b7E

(U)

~~(S//NF)~~ [REDACTED]
[REDACTED]

b7E

G.11 (U) [REDACTED] (CIA AND NSA)

G.11.1 (U) *DIOG CLASSIFIED PROVISION*

(U) ~~(S)~~ Procedures for conducting a [REDACTED] United States Intelligence Community (USIC) Agencies:

(U) G.11.1.1 ~~(S)~~ CENTRAL INTELLIGENCE AGENCY HEADQUARTERS (CIAHQ)

~~(S)~~

b1
b3

(U) G.11.1.2 ~~(S)~~ NATIONAL SECURITY AGENCY HEADQUARTERS (NSAHQ)

~~(S)~~

b1
b3

G.12 (U) NATIONAL SECURITY LETTERS FOR TELEPHONE TOLL RECORDS OF MEMBERS OF THE NEWS MEDIA OR NEWS ORGANIZATIONS

G.12.1 ~~(S//NF)~~ MEMBERS OF THE NEWS MEDIA OR NEWS ORGANIZATIONS

~~(S//NF)~~ (U) An investigation of members of the news media or news organizations is a sensitive investigative matter (SIM). A member of the news media or a news organization is defined in DIOG Section 10.1.2.2.5 and Appendix G.7.1. [REDACTED]

b1
b3

G.12.2 (U) LAW ENFORCEMENT TOOLS OTHER THAN NATIONAL SECURITY LETTERS

(U) Department of Justice policy with regard to the issuance of law enforcement tools such as subpoenas, 2703(d) orders, PR/TTs, and search warrants, is found at 28 C.F.R. § 50.10. The regulation concerns only law enforcement tools, not National Security Letters (NSLs).

G.12.3 (U) APPROVAL REQUIREMENTS FOR AN NSL SEEKING RECORDS OF A MEMBER OF THE NEWS MEDIA

The following approval requirements and specific procedures apply to the issuance of an NSL

b7E

(U//~~FOUO~~) In addition to the approval requirements for NSLs set out in DIOG Section 18.6.6.3.3, [REDACTED]

b7E

(U//~~FOUO~~) Example 1: [REDACTED]

b7E

(U//~~FOUO~~) Example 2: [REDACTED]

b7E

G.12.4 ~~(U//FOUO)~~ **APPROVAL REQUIREMENTS FOR AN NSL SEEKING RECORDS RELATED TO THE NEWS MEDIA OR NEWS ORGANIZATION**

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

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

[REDACTED]

b7E

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

[REDACTED]

~~(U)~~ G.12.5 ~~(S//NF)~~ **APPROVAL REQUIREMENTS FOR AN NSL SEEKING RECORDS OF A MEMBER OF THE NEWS MEDIA** [REDACTED]

b1
b3

~~(S//NF)~~

[REDACTED]

~~(S//NF)~~ If an NSL is seeking communications or business records of an individual who is a member of the news media or news organization and [REDACTED]

[REDACTED] there are no additional approval requirements other than those set out in DIOG Section 18.6.6.3.3 [REDACTED]

b1
b3
b7E

~~(S//NF)~~

[REDACTED]

G.12.1 *(U)SPECIFIC PROCEDURES FOR REQUESTING AN NSL*

(U) The procedures for creating an NSL

b7E

[REDACTED]

[REDACTED] are the

same as set out in DIOG Section 18.6.6.3.7

[REDACTED]

[REDACTED]

G.13 (U) OTHER INVESTIGATIVE RESOURCES

G.13.1 (U) *DIOG CLASSIFIED PROVISION*

G.13.1.1 (U//~~FOUO~~) SENSITIVE TECHNICAL EQUIPMENT

(U) ~~(S)~~ **Definition:** The term “Sensitive Technical Equipment” (STE) includes [redacted] STE is a) any technolog [redacted]
~~(S)~~ [redacted] c) technology that has been jointly developed with or developed by another U.S. Government (USG) agency such that the FBI is not the sole owner and on which originator controls have been placed. The Assistant Director of the OTD after consultation with the relevant operational division is authorized to determine whether particular equipment is (or is not) STE.

b1
b3
b7E

(U) ~~(S//NF)~~ **Authorized Investigative Activity:** Any use of [redacted]
[redacted]
[redacted] For additional guidance, refer to the Extraterritorial Guidelines (see DIOG Section 13). [redacted]

b1
b3
b7E

~~(S)~~ [redacted]

G.14 (U//~~FOUO~~) [REDACTED] **TYPE 5 ASSESSMENT**
(FORMERLY RECRUITMENT-IN-PLACE [RIP] TYPE 5 ASSESSMENTS)

b7E

(U//~~FOUO~~) See the [REDACTED] *Type 5 Assessment Quick Reference Guide*
(links to a ~~SECRET//NOFORN~~ document).

(U//~~FOUO~~) **Summary:** A Type 5 Assessment provides the authority for identifying, evaluating, and recruiting a potential confidential human source (PCHS). The provisions outlined herein integrate guidance regarding PCHS recruitment from relevant subsections of the *Domestic Investigations Operations Guide (DIOG)*, the *Counterintelligence Division Policy Guide (CDPG)*, and the *Confidential Human Source Policy Guide (CHSPG)* [REDACTED]

b7E

(U//~~FOUO~~) In accordance with the *Attorney General's Guidelines for Domestic FBI Operations (AGG-Dom)* Part II.A.3.c and as defined by DIOG § 5.6.3.4, the purpose of a Type 5 Assessment is to “seek information to identify potential human sources, assess the suitability, credibility, or value of individuals as human sources, validate human sources, or maintain the cover or credibility of human sources, who may be able to provide or obtain information relating to criminal activities in violation of federal law, threats to the national security, or matters of foreign intelligence interest...” [REDACTED]

b7E

[REDACTED] Type 5 Assessments
(formerly Recruitment-in-Place [RIP] Type 5 Assessments)

b1

b3

G.14.1 (U//~~FOUO~~) [REDACTED] **TYPE 5 ASSESSMENT APPLICABILITY**

b7E

b1
b3

G.14.2 ~~(U//FOUO)~~ AUTHORIZED INVESTIGATIVE METHODS IN
TYPE 5 ASSESSMENTS

b7E

b1
b3

G.14.3

b1
b3

b1
b3

b1
b3

b7E

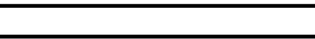
b7E

G.14.4 (U//~~FOUO~~) *TYPE 5 APPROACH METHODS*

(U//~~FOUO~~) All authorized Type 5 Assessment approach methods defined in the CHSPG 

G.14.4.1 (U//~~FOUO~~) COVERT APPROACH AND UNDERCOVER ACTIVITY ARE NOT THE SAME

(U//~~FOUO~~) 

² (U//~~FOUO~~)  Type 5 Assessment 

~~SECRET//NOFORN~~

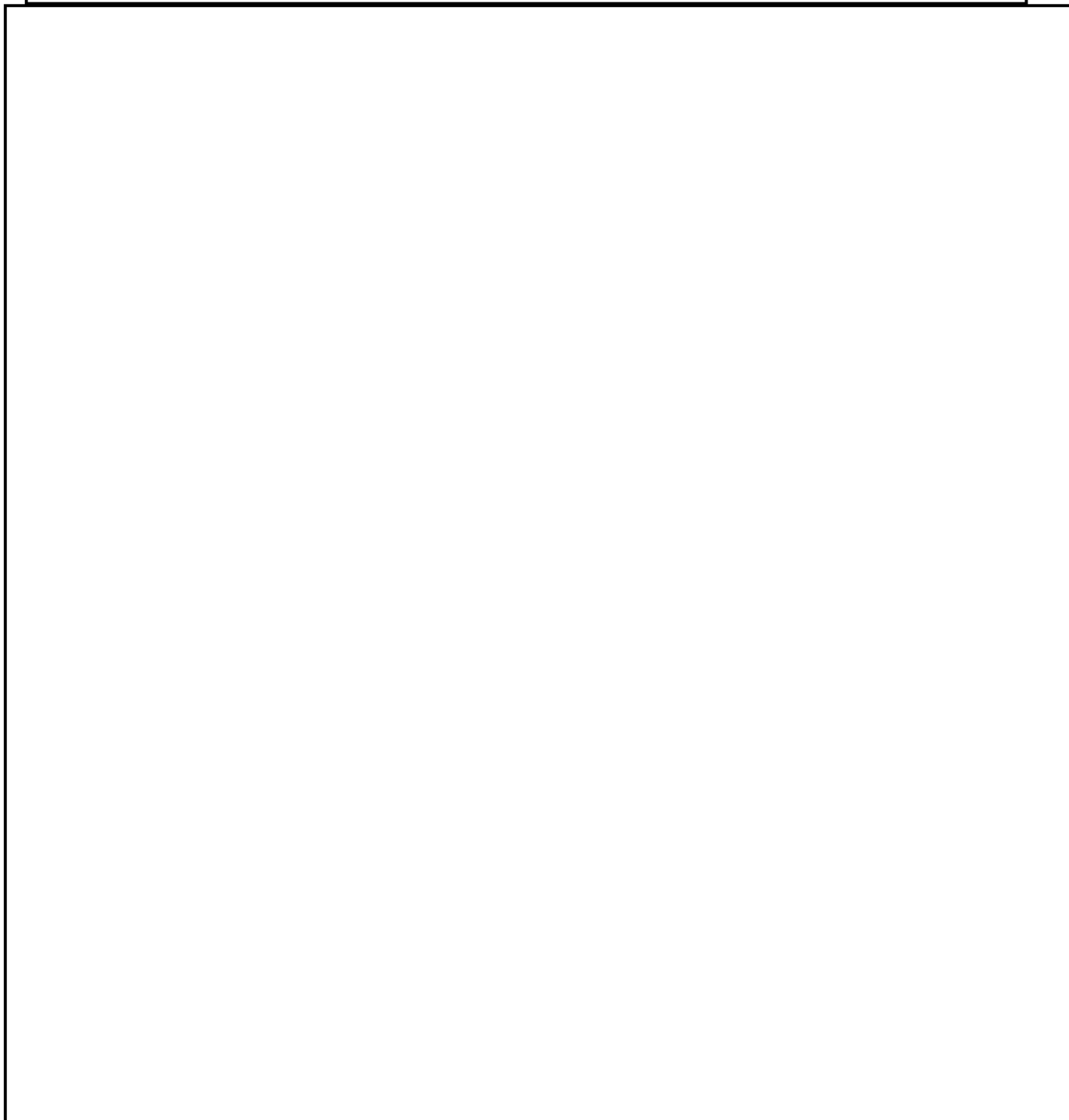
Domestic Investigations and Operations Guide

§G

b7E



b1
b3



~~SECRET~~

~~SECRET//NOFORN~~

b1
b3

G.14.4.2 (U//~~FOUO~~) APPROVALS FOR [REDACTED] TYPE 5 APPROACHES

b7E

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

b7E

G.14.5 (U//~~FOUO~~) RECRUITMENT PLAN APPROVALS

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

b7E

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

b1
b3

b1
b3



G.14.5.1



b1
b3



~~(S)~~

b1
b3

G.14.6 ~~(U//FOUO)~~ [REDACTED] *TYPE 5 ASSESSMENT PROCESS AND
REQUIRED DOCUMENTATION*

b7E

~~(S)~~

b1
b3

(U) Opening EC Basic Information:

1. (U) Details of the purpose and clearly-defined objective(s):

- a. ~~(U//FOUO)~~ [REDACTED]
[REDACTED]

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

- a. (U) [REDACTED]
b. ~~(U//FOUO)~~ [REDACTED]
[REDACTED]
c. ~~(U//FOUO)~~ [REDACTED]
d. ~~(U//FOUO)~~ [REDACTED]
[REDACTED]
e. ~~(U//FOUO)~~ [REDACTED]
f. ~~(U//FOUO)~~ [REDACTED]
[REDACTED]
g. ~~(U//FOUO)~~ [REDACTED]

b7E

(U) [REDACTED]

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

b7E

[REDACTED]
[REDACTED]

b1
b3

- b. ~~(U//FOUO)~~ [REDACTED]
[REDACTED]

b6
b7C

~~(S)~~

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

[Redacted]

b7E

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

[Redacted]

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

[Redacted]

~~(S)~~

[Redacted]

b1
b3

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

[Redacted]

[Redacted]

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

[Redacted]

b7E

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

[Redacted]

[Redacted]

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

[Redacted]

[Redacted]

~~(S)~~

[Redacted]

b1
b3

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

[Redacted]

[Redacted]

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

[Redacted]

[Redacted]

b7E

(U) Recruitment Plan:

1. (U//~~FOUO~~) A detailed explanation of

[Redacted]

[Redacted]

~~(S)~~

b1
b3
b7E

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

b7E

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

[REDACTED]

b1
b3

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

b7E

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

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

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

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

viii. [REDACTED]

b1
b3

G.14.7 (U//~~FOUO~~) [REDACTED] **TYPE 5 ASSESSMENTS**

b7E

(U//~~FOUO~~) Pursuant to an authorized [REDACTED] Type 5 Assessment and in accordance with the

b7E

[REDACTED]

1. (U) [REDACTED]

2. (U//~~FOUO~~) [REDACTED]
3. (U//~~FOUO~~) [REDACTED]
4. (U//~~FOUO~~) [REDACTED]
5. (U//~~FOUO~~) [REDACTED]
6. (U//~~FOUO~~) [REDACTED]

b7E

G.14.8 (U//~~FOUO~~) CLOSING A [REDACTED] *TYPE 5 ASSESSMENT*

(U//~~FOUO~~) A [REDACTED] Type 5 Assessment must be closed via EC to the sub file with SSA approval. The [REDACTED]

G.14.9 (U) [REDACTED] *TYPE 5 ASSESSMENT STATUS AS A POLICY EXCEPTION*

[REDACTED]

b1
b3
b7E

~~SECRET//NOFORN~~

Domestic Investigations and Operations Guide

§G

b1
b3

G-14.10

G-29

~~SECRET//NOFORN~~

Revised
12/07/2020

~~SECRET//NOFORN~~

Domestic Investigations and Operations Guide

§G

G-30

~~SECRET//NOFORN~~

H APPENDIX H: (U) PRE-TITLE III ELECTRONIC SURVEILLANCE (ELSUR) SEARCH POLICY

H.1 (U) SCOPE

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

H.1.1 (U) COMPLIANCE WITH THE PREVIOUS APPLICATION PROVISION

(U) Although a failure to comply with § 2518(1)(e) will not always result in suppression of evidence, deliberate noncompliance likely will.

(U) To comply with this requirement, the affiant and affiant’s supervisor must ensure all pre-Title III electronic surveillance searches (hereinafter “ELSUR searches”) of the ELSUR Data Application (EDA) system have been properly completed by an ELSUR Operations Technician (EOT) prior to submission of the Title III application and affidavit to the court.

H.1.1.1 (U) WHEN TO SEARCH

(U) Original Title III Application/Affidavit: For both sensitive and non-sensitive Title IIIs, ELSUR searches for all target subjects, facilities, and/or places must be completed within 45 calendar days prior to the date the application and affidavit are filed with the court.⁸⁴

(U) Extension and Renewal Title III Applications/Affidavit: For both sensitive and non-sensitive Title IIIs, ELSUR searches for all target subjects, facilities, and/or places previously searched for the same investigation must be completed within 90 calendar days prior to the date the new application and affidavit are filed with the court.

(U) However, any newly identified person, facility, and/or place named in an extension/renewal must be searched within 45 calendar days prior to the date the new application and affidavit are filed with the court.

(U) If an individual named by an alias, partial name, nickname, street name, and/or code name in a previous application is subsequently identified by at least a first initial and a last name, a search must be conducted for the now-identified individual prior to seeking any new application naming that person.

H.1.1.2 (U) HOW TO SEARCH

(U) The EDA must be searched for previously submitted Title III applications involving any of the persons, facilities, and/or places specified in the current Title III application. There is no obligation to search for prior interceptions.

⁸⁴ This requirement also applies to what is sometimes referred to as a “spin-off” Title III which is actually a new application to begin surveillance at or of additional facilities arising from an existing investigation in which one or more Title IIIs have already been authorized. As such “spin-off” Title IIIs are considered to be an “original” request, even though some or all of the named persons are also named in the prior Title III(s).

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

H.1.1.2.1 **(U) PERSONS**

(U) In submitting a Pre-Title III ELSUR Search Request, FD-940, list the true names or best known names of individuals for whom there is probable cause to believe that: (1) they are involved in the specified criminal activity, or (2) their criminal communications are expected to be intercepted over the target facility or within the target premises.⁸⁵ These individuals are often identified in the application and affidavit as the “Target Subjects,” “Target Violators,” and/or “Target Interceptees.”

- A) (U) A minimum of a first initial and last name is required for an ELSUR search. Biographical data such as date of birth, FBI Number, and/or Social Security Account Number, if known, must be included in the search request, even if not listed in the affidavit. Aliases, partial names, nicknames, street names, and/or code names may also be included as further identifying information on the FD-940. However, they must only be searched if they otherwise meet minimum ELSUR search requirements. For example, if an alias is a full name alias, it must be included and will be searched (e.g., John Smith a/k/a “William Johnson” or William Smith a/k/a “Liam Smith”). However, if the subject is identified as John Smith a/k/a “Big Buddy,” “Big Buddy” may be included as further identifying information, but will not be the subject of a separate ELSUR search.
- B) (U) Persons not fully identified by at least a first initial and a last name who are identified in the application and affidavit as “John Doe,” “Jane Doe,” or “FNU LNU” need not be the subject of an ELSUR search. For example, FNU LNU a/k/a “El Jefe” need not be included in an ELSUR search, or listed in the FD-940 search request.
- C) (U) An ELSUR search must be conducted for the subscriber or service provider of the target facility only if the subscriber or service provider is believed to be involved in the specified criminal offense(s).
- D) (U) Any additional persons, facilities, and/or places mentioned in the affidavit, **but not also specified in the application as a person, facility, and/or place for which authorization to intercept is being sought**, need not be searched or listed in the FD-940.

H.1.1.2.2 **(U) FACILITIES**

(U) In submitting the FD-940, list available numeric and/or alphanumeric values directly associated with the targeted device, equipment, or instrument over or from which the subjects are communicating (e.g., a telephone, pager, computer, etc.), and over or from which interceptions are being sought. Such values may include, but are not limited to, the telephone number of a land line phone, cell phone, or pager; Personal Identification Number (PIN), Cap Code, Electronic Serial Number (ESN), International Mobile Subscriber Identity (IMSI) Number, International Mobile Equipment Identifier (IMEI) Number, and/or Internet account information (including, but not limited to, screen name, online identity, ICQ number, and/or IP address).

- A) (U) Names of businesses, organizations, or agencies must be searched only if there is probable cause to believe the business, organization, or agency is culpable in the specified criminal offense(s).

⁸⁵ (U) All individuals listed in the application and affidavit as being involved in the specified criminal activity should be searched in EDA.

Domestic Investigations and Operations Guide

- B) (U) Searches need not be conducted for telephone numbers or other facilities subscribed to, leased, or owned by the FBI for use in the investigation for which the ELSUR is being sought.
- C) (U) Any additional facilities mentioned in the affidavit, but not also specified in the application as a person, facility, and/or place for which authorization to intercept is being sought, need not be searched or listed in the FD-940. For example, telephone numbers identified as calling or being called by the Target Telephone, and set out in the pen register section of a Title III affidavit need not be the subject of an ELSUR search.

H.1.1.2.3 (U) *PLACES*

(U) In submitting the FD-940, list: (1) each address of a targeted landline phone or computer terminal which will be subject to the Title III order, and/or (2) [REDACTED]

b7E

[REDACTED]
[REDACTED] Do not include addresses of subscribers or proprietors of mobile installations such as cell phones, pagers, vehicles, boats or planes, etc.

H.1.1.2.4 (U) *ADDITIONS*

(U) Persons, facilities, and/or places added to an application and affidavit during the course of the review process and after the initial pre-Title III search request must be searched prior to submitting the application and affidavit to the court.⁸⁶

H.1.1.3 (U) *WHERE TO SEARCH*

(U) A search of the FBI's EDA must be conducted for each item named in the search request. DOJ policy requires a search of the Drug Enforcement Administration (DEA) and Immigration and Customs Enforcement (ICE) EDA for all Title 21 predicate offenses. As a matter of FBI policy, a DEA and ICE ELSUR search is automatically conducted by FBIHQ for all [REDACTED] and [REDACTED] investigative classifications, and any other application involving a Title 21 offense.

b7E

- A) (U) The EDA of any other federal, state, or local law enforcement agency that is actively participating in a joint investigation with the FBI (as opposed to mere task force participation) or as to which there is reason to believe may have previously sought to intercept wire, oral, or electronic communications involving any of the persons, facilities, and/or places specified in the instant application, should be searched. Where a search of state and/or local law enforcement ELSUR records is requested, the request should include a point of contact from the outside agency, if known.
- B) (U) If there is reason to believe that any of the persons, facilities, and/or places specified in the current application have been the target of Title III electronic surveillance by another federal agency, that agency must be requested to conduct an ELSUR search of its records.

⁸⁶ Occasionally, during the course of their review, DOJ's Office of Enforcement Operations, will suggest that an additional name be added as a "Target Subject" (or similar) in a Title III application and affidavit prior to the grant of DOJ approval. If that name is added, it must be searched through EDA prior to submitting the application and affidavit to the court.

H.1.1.4 (U) HOW TO INITIATE A SEARCH REQUEST

(U) The FD-940 must be used for requesting pre-Title III ELSUR searches of the EDA of the FBI and any other federal, state, or local law enforcement agency. The form is designed to assist personnel requesting a search by guiding them through the process. The requesting agent must submit a lead to the ELSUR Technology Management Unit (ETMU) and the field office EOT. Use of the form will ensure search requirements are met, and must be submitted with adequate time for the EOT to conduct the search and document the results.

(U) If an emergency situation exists, as defined by 18 U.S.C. § 2518(7), an ELSUR search may be requested telephonically to the field office EOT.

H.1.1.4.1 (U) SEARCH PROCEDURE

(U) The EOT must conduct a search of the EDA for records of previous applications only as specified in the FD-940. Records retrieved as a result of the search must be furnished to the requesting agent, and documented in the appropriate investigative ELSUR subfile.

(U) It is the responsibility of the requesting agent to use reasonable efforts to determine whether the persons, facilities, and/or places identified in the search are the same persons, facilities, and/or places specified in the current application. If there is reason to believe they are, offices identified as having filed previous applications must be contacted and the EOT in that office must ensure a review of the pertinent investigative file(s) was conducted to determine whether the persons, facilities, and/or places identified in the search are, in fact, the same as those specified in the current application.

(U) It is not necessary to contact other offices regarding common names for which no special identifying data is available unless there is reason to believe there is a nexus between the current investigation and the investigation conducted by the other field offices.

(U) Documentation confirming the conduct of all ELSUR searches must be electronically placed in the appropriate investigative ELSUR subfile.

H.1.1.5 (U) AFFIDAVIT LANGUAGE EXAMPLES**A) (U) NO PREVIOUS APPLICATIONS:**

(U) “Based upon a search of the records of the Federal Bureau of Investigation [and any other agency requested], no previous applications have been filed for an order authorizing the interception of wire, oral, or electronic communications involving any of the persons, facilities, and/or places specified herein for which authorization to intercept is being sought.”

B) (U) PREVIOUS APPLICATIONS:

(U) “John Doe was named in a previous application for an order authorizing the interception of wire and electronic communications. The order was [signed or denied] on [date], by U.S. District Judge [name], of the District of [Name of District], authorizing the interceptions for a period of thirty (30) days. An extension of the order was signed by Judge [name] on [date], authorizing the continued interception for an additional 30-day period.” (Include relevance, if any, of the previous applications to the current investigation).

H.1.1.6 (U) **DOCUMENTATION PROVIDED TO EOT**

(U) The EOT and the ELSUR supervisor must confirm that ELSUR searches were properly conducted as set forth in the final applications submitted to the court. Because this review is not conducted until after the application and order have been submitted to the court, the SA and SSA must verify that all required ELSUR searches have been conducted prior to submission of the application and affidavit to the court. Within 10 calendar days of obtaining court authority for the original and all extensions/renewals of the Title III intercept, the case agent must also submit to the EOT a signed copy of the application and order. The EOT must email a copy of these documents to [REDACTED]. The ETMU must index and upload these documents into the EDA system. These requirements also apply to the joint Title III operations discussed in section 18.7.2.13.

b7E

H.1.1.7 **ROLE OF SPECIAL OPERATIONS DIVISION (SOD) AND [REDACTED]**
[REDACTED] SEARCHES

b7E

(U//FOUO) [REDACTED]

b7E

[REDACTED]

(U//FOUO) [REDACTED]

b7E

[REDACTED]

This Page is Intentionally Blank.

I APPENDIX I: (U) ACCESSING STUDENT RECORDS MAINTAINED BY AN EDUCATIONAL INSTITUTION ("BUCKLEY AMENDMENT")

I.1 (U) SUMMARY

(U) The Family Educational Rights and Privacy Act (FERPA) of 1974 (20 U.S.C. § 1232g, as amended by Public Law 107-56 (USA Patriot Act)), commonly referred to as the "Buckley Amendment," restricts the ability of educational agencies or institutions (collectively "schools") to release educational records or personally identifiable information contained in such records without the consent of the student or the student's parent.

(U) FERPA defines "education records" as those records, files, documents and other materials which:

- A) (U) contain information directly related to a student; and
- B) (U) are maintained by an educational agency or institution or by a person acting for such agency or institution. (20 U.S.C. § 1232g(a)(4)(A)(i)).

(U//~~FOUO~~) If operationally feasible, FBI employees should request the consent of the student or parent, as appropriate, in order to obtain covered records. During an Assessment, the FBI may ask school officials to provide certain information without the consent of the student or parent (see Section 18.5.6); during a predicated investigation, the FBI may compel production of education records, as set forth below.

I.2 (U//~~FOUO~~) ACCESSING STUDENT INFORMATION OR RECORDS DURING AN ASSESSMENT

(U//~~FOUO~~) During an Assessment, FBI employees may seek **voluntary disclosure** of certain student records and information about students from schools without the consent of the student or parent.

I.2.1 (U) DIRECTORY INFORMATION

(U//~~FOUO~~) "Directory information" is information contained in an education record of a student "that would not generally be considered harmful or an invasion of privacy." (34 CFR § 99.3) Specifically, "directory information" includes, but is not limited to: the student's name, address, telephone listing, electronic mail address, photograph, date and place of birth, major field of study, dates of attendance, grade level, enrollment status (e.g., undergraduate or graduate, full-time or part-time), participation in officially recognized activities or sports, weight and height of members of athletic teams, degrees, honors and awards received, and the most recent educational agency or institution attended. A school may disclose "directory information" from its records without prior consent if: (1) it has a directory information policy to disclose such information and (2) it has provided its students notice of the policy and the opportunity to opt out of having "directory information" disclosed. (See 34 CFR § 99.37)

(U//~~FOUO~~) The scope of information that can be released as directory information may be narrowed by the school. For instance, if a college chooses not to categorize students' names and addresses as directory information, it must not voluntarily disclose such information to the FBI

(*Krauss v. Nassau Community College*, 469 N.Y.S. 2d 553 (N.Y. Sup. 1983)). Schools are also required to afford students (or parents, if the student is under 18) the opportunity to prohibit the release of directory information without their prior consent (or a court order). *Note*: the Buckley Amendment *permits* schools to release directory information (absent an objection from the student); it does *not require* them to do so. Directory information may be sought orally or in writing.

1.2.2 (U) *OBSERVATIONS*

(U//~~FOUO~~) FERPA governs the release of educational records. It does not govern the release of information gathered by a school official, based on his or her own observations. Accordingly, notwithstanding Buckley, a school official may disclose activity or behavior observed by the official.

1.2.3 (U) *LAW ENFORCEMENT UNIT RECORDS*

(U//~~FOUO~~) Under FERPA, schools may disclose information from “law enforcement unit records” without the consent of the parent or student. This exemption is limited to records that a law enforcement unit of a school creates and maintains for a law enforcement purpose. “Law enforcement record” is narrowly defined as a record that is: (i) created by the law enforcement unit; (ii) created for a law enforcement purpose; and (iii) maintained by the law enforcement unit. (34 CFR § 99.8(b)) If another component of the school discloses a student education record to the school’s law enforcement unit, that record is not a “law enforcement unit record” because it was not *created* by the law enforcement unit. Thus, a law enforcement unit cannot disclose, without student consent, information obtained from education records created by other component of the school, even if the record has been shared with the law enforcement unit.

1.2.4 (U) *HEALTH OR SAFETY EMERGENCY*

(U//~~FOUO~~) FERPA does not restrict the disclosure of educational records in connection with a health or safety emergency. The regulations provide that schools may disclose information from an education record “to appropriate parties in connection with an emergency if knowledge of the information is necessary to protect the health or safety of the student or other individuals” and that the exception is to be “strictly construed.” As is the case with other emergency disclosure provisions (see 18 U.S.C. § 2702), it is up to the school to determine in the first instance whether disclosure is necessary to protect the health or safety of the student or another individual. If it makes that determination, it is permitted to disclose educational records voluntarily and without the consent of the student or parent.

1.2.5 (U) *NON-STUDENTS*

(U//~~FOUO~~) FERPA governs records of “students.” A “student” is defined as a person on whom a school maintains educational records or personally identifiable information but does not include someone who has not attended that school. Files retained on rejected applicants may be provided without prior permission or notification. (*Tarka v. Franklin*, 891 F.2d 102 (5th Cir. 1989))

I.3 (U//~~FOUO~~) ACCESSING STUDENT INFORMATION OR RECORDS IN PREDICATED INVESTIGATIONS

(U//~~FOUO~~) In addition to seeking voluntary production of records that can be voluntarily produced (see I.2 above), in a predicated investigation, FBI employees may **compel production** of education records without notice to the student or the student's parents as follows:

I.3.1 (U) *FEDERAL GRAND JURY SUBPOENA*

(U//~~FOUO~~) Schools shall disclose education records in response to a federal grand jury subpoena. In addition, the court may order the institution not to disclose to anyone the existence or contents of the subpoena or the institution's response. If the court so orders, then neither the prior notification requirements of 34 CFR § 99.31(a)(9) nor the recordation requirements at 34 CFR § 99.32 would apply (see DIOG Section 18.6.5).

I.3.2 (U) *ADMINISTRATIVE SUBPOENAS*

(U//~~FOUO~~) Schools may disclose education records in response to an administrative subpoena. Administrative subpoenas may be issued in narcotics investigations (see DIOG Section 18.6.4.3.2.1), sexual exploitation or abuse of children investigations (see DIOG Section 18.6.4.3.2.2), and health care fraud investigations (see DIOG Section 18.6.4.3.2.3). As with federal grand jury subpoenas, the issuing agency may, for good cause shown, direct the school not to disclose the existence or contents of the subpoena or the institution's response. If the subpoena includes a nondisclosure directive, the school is permitted to request a copy of the good cause determination.

I.3.3 (U) *FISA ORDER FOR BUSINESS RECORDS*

(U//~~FOUO~~) See DIOG Section 18.6.7.

I.3.4 (U) *EX PARTE ORDERS*

(U//~~FOUO~~) The USA Patriot Act amended FERPA to permit schools to disclose personally identifiable information from the student's education records to the Attorney General or his designee without the consent or knowledge of the student or parent in response to an *ex parte* order issued in connection with a terrorism investigation. Such disclosures are also exempt from the Buckley Act requirements that disclosure of information from a student's records be documented in the student's file.

This Page is Intentionally Blank.

J APPENDIX J: (U) CASE FILE MANAGEMENT AND INDEXING

J.1 (U) INVESTIGATIVE FILE MANAGEMENT

J.1.1 (U) OFFICE OF ORIGIN (OO)

(U//~~FOUO~~) Generally, the Office of Origin (OO) is determined by:

- A) (U//~~FOUO~~) The residence, location or destination of the subject of the investigation;
- B) (U//~~FOUO~~) The office in which a complaint is first received;
- C) (U//~~FOUO~~) The office designated by FBIHQ as OO in any investigation;
- D) (U//~~FOUO~~) The office in which the Foreign Police Cooperation investigation is opened (163 classification);
- E) (U//~~FOUO~~) The office in which the Domestic Police Cooperation investigation is opened (343 classification);
- F) (U//~~FOUO~~) The office in which the recovery of the vehicle occurred in an Interstate Transportation of Stolen Motor Vehicles (ITSMV) investigations;
- G) (U//~~FOUO~~) The office in which the contempt of court occurred;
- H) (U//~~FOUO~~) The office in which there is a violation of an order, judgment, or decree issued from any judicial district in an FBI civil Racketeer Influenced and Corrupt Organizations (RICO) investigation;
- I) (U//~~FOUO~~) The office in which the subject was convicted in investigations involving parole, probation, and mandatory release violators;
- J) (U//~~FOUO~~) The office in which the escape occurred, in Escaped Federal Prisoner and escaped deserter investigations;
- K) (U//~~FOUO~~) The New York Field Office in courier investigations;
- L) (U//~~FOUO~~) FBIHQ in all applicant, Background Investigation - Pardon Attorney's Office (73 classification) investigations;
- M) (U//~~FOUO~~) FBIHQ in OPM security referral (140A and 140C classification) investigations;
- N) (U//~~FOUO~~) FBIHQ, Counterterrorism Division (CTD), Counterterrorism Watch Unit in all Counterterrorism Major Cases (900 classification);
- O) (U//~~FOUO~~) FBIHQ, Critical Incident Response Group (CIRG) in all National Center for the Analysis of Violent Crime (NCAVC) cases (252A through 252E classifications); and
- P) (U//~~FOUO~~) FBIHQ, Office of Professional Responsibility (OPR) in OPR matters (263 classification).

(U//~~FOUO~~) When special circumstances exist, however, the origin may be assumed by the field office which has the most compelling interest. Uncertainties and disagreements must be resolved by the appropriate FBIHQ operational division.

J.1.2 **(U) INVESTIGATIVE LEADS AND LEAD OFFICE (LO)**

(U//~~FOUO~~) Leads are sent by EC, or a Lead Request document, to offices and assigned to individuals/organizations in order to aid investigations. When the OO sets a lead to another office, that office is considered a Lead Office (LO).

(U//~~FOUO~~) There are only two types of investigative leads: “Action Required” and “Information Only.”

J.1.2.1 **(U) ACTION REQUIRED LEAD**

(U//~~FOUO~~) An action required lead must be used if the sending office requires the receiving LO to take some type of investigative action.

(U//~~FOUO~~) An action required lead may only be set out of an open investigative file, including an:

- A) (U) Assessment file;
- B) (U) Predicated investigation file;
- C) (U) pending inactive investigation file; or
- D) (U) unaddressed work file.

(U//~~FOUO~~) An action required lead cannot be set out of a closed investigative file, a zero (0) or double zero (00) file.

(U//~~FOUO~~) An action required lead must be assigned, and it must be covered before the underlying investigation has been completed/closed.

J.1.2.2 **(U) INFORMATION ONLY LEAD**

(U//~~FOUO~~) An information only lead must be used when no specific action is required or necessary from the receiving LO.

(U//~~FOUO~~) An information only lead may be set out of an opened or closed investigative file, including a:

- A) (U) zero (0) file;
- B) (U) double zero (00) file;
- C) (U) Assessment file;
- D) (U) Predicated investigation file;
- E) (U) pending inactive investigation file; or
- F) (U) unaddressed work file.

(U//~~FOUO~~) An information only lead does not have to be assigned in order to be covered, and they can be covered while they are in the "Set" status.

J.1.3 **(U) OFFICE OF ORIGIN'S SUPERVISION OF CASES**

(U//~~FOUO~~) The OO is responsible for proper supervision of Assessments and investigations in its own territory and being conducted in a LO. The FBI employee, usually an FBI Special Agent, to whom an investigation is assigned, is often referred to as the “Case Agent.” An FBI employee

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

is personally responsible for ensuring all logical investigation is initiated without undue delay, whether the employee is assigned in the OO or in an LO; this includes setting forth Action Required or Information Only leads as appropriate for other offices or other FBI employees in his/her own office. The OO Case Agent has overall responsibility for supervision of the investigation. When an LO has a delayed or delinquent investigation, it is the responsibility of the OO Case Agent to notify the LO (orally or in writing by email or EC, depending on the urgency of the situation) of its delinquency.

(U) Investigative information that may be within another field office's AOR can generally be obtained by setting an investigative lead to that field office. However, investigative circumstances may require employees to travel to another office's AOR to conduct investigative activity. In such circumstances, an employee, with the approval of his or her supervisor and the prior concurrence of the relevant SSA in the other field office, may enter that office's AOR and conduct the necessary investigative activity (e.g. interview). However, if unplanned investigative activities or exigent circumstances prevent an employee from obtaining advance SSA approval and advance SSA concurrence before entering another field office's AOR, notification should be made as soon as practicable to the employee's SSA and relevant SSA in the other office's AOR, including the type of investigative activity(s) that occurred and the circumstances that made obtaining prior approval and concurrence unfeasible.

J.1.4 (U) INVESTIGATION AND OTHER FILES

(U//~~FOUO~~) There are several types of non-investigative files used in the FBI, including zero files, double zero files, administrative files, and control files. Additionally, there are several types of investigative files used in the FBI, including Assessment files, Preliminary Investigation files, Full Investigation files, Full Enterprise Investigation files, positive foreign intelligence Full Investigation files, and unaddressed work files. Additionally, investigative files may have sub-files, named as specified in the DIOG and IMD policy. FBI files may be opened, closed, or placed in pending inactive status as specified below. Note that in each of these files, all communications related to previous communication must note the existing communication's FBI's central recordkeeping system serial numbers in the reference fields.

(U//~~FOUO~~) Certain records may be restricted based on the classification of the records, e.g., on the sensitivity of the investigation. See the *Automatic Restriction of Access to Data in FBI Case Support Systems Based on Standard File Classification Designators Policy Directive, 0243D*, dated October 13, 2009, and the *Manual Restriction of Access to Data in FBI Case Files Policy Notice, 0758N*.

(U//~~FOUO~~) The types of files are:

J.1.4.1 (U) ZERO "O" FILES

(U//~~FOUO~~)

b7E

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

J.1.4.2 (U) DOUBLE ZERO “OO” FILES

(U//~~FOUO~~) Double Zero files may be opened in all file classifications. Double Zero files may contain documentation, such as instructions, statutes, and decisions applicable to the classification, that do not require investigation. The documents contained within a double zero file must be electronically placed into the file

b7E

J.1.4.3 (U) ADMINISTRATIVE “A” FILES

(U//~~FOUO~~) Administrative files may be used only for administrative purposes; they cannot be used for investigative purposes. Administrative files may be used for documenting non-investigative matters, such as training matters (1 classification), administrative matters (319 classification), personnel files (67 classification), Laboratory assistance, etc. Note:

Investigative activity must not be conducted out of an administrative file. Administrative files are designated with the letter "A" before the case number, e.g., 319X-HQ-A12345.

(U//~~FOUO~~) FBI BUCAR accident files (66A classification) and civil litigation or claim matters (197A-F classifications) are permitted to retain investigative information related to a BUCAR accident or civil matter as an exception to the general rule prohibiting the use of investigative activity in administrative files. The basis for permitting this exception is the investigative document, generally a witness interview on an FD-302 for the car accident, or taking a witness statement on an FD-302 in the civil matter, is intended to support the administrative functions of the organization and is not obtained in support of a law enforcement investigation or an intelligence collection function.

(U//~~FOUO~~) Information Only (non-investigative) Leads may be assigned out of administrative files. When referring to an administrative file in communications, the file number must include the letter "A" before the case number to indicate the file is an administrative file.

J.1.4.4 (U) CONTROL “C” FILES

(U//~~FOUO~~) Control files are separate files established for the purpose of managing programs. Control files may be opened in all file classifications.

(U//~~FOUO~~) Control files may be used only for documenting program management functions and communications, technical or expert assistance to another law enforcement or intelligence agency, or other managerial functions. Program management functions may include liaison contacts, training exercises, training received/provided, written intelligence products⁸⁷ that are prepared for program management purposes, etc. Note: **Investigative activity must not be conducted⁸⁸ out of a control file.** Control files are designated with the letter “C” before the case number, e.g., 29B-NF-C4456.

⁸⁷ (U//~~FOUO~~) A copy of all written intelligence products that are directly related to an investigation must be placed in an INTELPRODS sub-file. See DIOG section 15.6.1.2.

⁸⁸ (U) Section 18 investigative methods may only be conducted out of investigative files.

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

(U//~~FOUO~~) Information Only (non-investigative) Leads can be assigned out of control files. When referring to the file number of a control file in communications, the file number must include the letter "C" before the case number to indicate the file is a control file. The [redacted] control file must follow the [redacted] guidance on setting leads.

b7E

J.1.4.5 (U) INVESTIGATIVE FILES

J.1.4.5.1 (U) ASSESSMENT FILES

J.1.4.5.1.1 (U) TYPE 1 & 2 ASSESSMENT FILES

b7E

(U//~~FOUO~~) Type 1 & 2 Assessments must be maintained in an applicable Assessment file. When completing the Guardian FD-71a or Assessment file lead for an Assessment

[redacted]
[redacted]

(U//~~FOUO~~) Action leads can be set when using an Assessment file. Guardian, the EC, and the Sentinel Lead Request form provide the ability to set action leads.

b7E

**J.1.4.5.1.2 (U) INVESTIGATIVE CLASSIFICATION ASSESSMENT FILES
(FOR TYPE 3, 4 AND 6 ASSESSMENTS) AND POTENTIAL CHS
FILES (FOR TYPE 5 ASSESSMENTS)**

(U//~~FOUO~~) See DIOG Section 5 for the appropriate investigative file classification to be used when opening a Type 3, 4, 5, or 6 Assessment file.

(U//~~FOUO~~) Because these Assessments require prior supervisory approval, an opening EC is required (DIOG Section 5.6.3.2 through 5.6.3.5 type Assessments and DIOG Section 5.7 as discussed above). [redacted]

b7E

[redacted]

J.1.4.5.2 (U) PRELIMINARY AND FULL INVESTIGATION (PREDICATED) FILES

(U//~~FOUO~~) A Preliminary Investigation, Full Investigation, Full Enterprise Investigation, and Full Positive Foreign Intelligence Investigation must be opened as discussed in DIOG Sections 6, 7, 8, and 9, respectively. Investigative information related to these investigations must be placed in the investigative main file or sub-file, spun-off, or referred to another agency as authorized.

J.1.4.5.3 (U) PENDING/INACTIVE FULL INVESTIGATION FILES

(U//~~FOUO~~) A Full Investigation may be placed in a pending-inactive status when all investigation has been completed and only prosecutive action or other disposition remains to

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

be determined and reported, e.g., locating a fugitive outside the United States. [REDACTED]

b7E

[REDACTED]
[REDACTED] A pending-inactive Full Investigation may be assigned to investigative personnel or a squad/unit.

J.1.4.5.4 (U) *NATIONAL INCIDENT-BASED REPORTING SYSTEM*

(U//~~FOUO~~) If prompted, all case agents must complete the National Incident-Based Reporting System (NIBRS) form in Sentinel prior to closing a case or placing a full investigation in pending-inactive status.

J.1.4.5.5 (U) *UNADDRESSED WORK FILES*

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

[REDACTED]

b7E

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

[REDACTED]

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

[REDACTED]

b7E

(U//~~FOUO~~) Guardian incidents cannot be placed in an Unaddressed Work status.

J.1.4.5.6 (U) *SPIN OFF INVESTIGATION FILES*

(U//~~FOUO~~) A spin-off investigation originates from an existing investigation. The spin-off investigation must have all the elements required to establish it as a separate investigation within the appropriate investigative classification.

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

J.1.5 ***(U) SUB-FILES***

(U) The below standardized sub-file names in column one must be used when creating sub-files to document the investigative or administrative activity described in column two. However, employees may create and utilize unique sub-file names to document investigative or administrative activities not already listed in the below standardized sub-file name list. For instance, a sub-file may be opened named “John Doe” with its contents all related to the activities of John Doe.

(U) List of standardized sub-files:

Sub-file Name	Description of Sub-file Contents
ADMIN	Administrative Matters
AFF	Affidavits
ANA	Analytical (not including Written Intelligence Products – see DIOG required INTELPRODS sub-file below)
BC	Background Information Re Subject (FD-160; FD-125)
BIO	Biographical Info (NCIC; CLETS; DMV)
CART	Computer Analysis Response Team
CRIM	Criminal Records
CCTV	Closed Circuit Television/Video Surveillance
CE	Case Expenditures
CD	Classified Documents / Info
CRT	Court Orders
---	“the appropriate investigative ELSUR sub-file” <i>(Note: field offices may continue to use the following listed ELSUR sub-files pending the creation of new sub-file names by OTD and IMD to be reflected in the next DIOG Update.)</i>
ELA	ELSUR Administrative (Criminal and National Security)
ELA1	Title III Administrative
ELA2 (Note: The DIOG requires sub-file “PEN”)	Pen Registers (See DIOG required sub-file “PEN” below)
ELA3	Consensual Monitoring
EL1	ELSUR Original Logs (Criminal and National Security)

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

EL1A	ELSUR Copies of Logs (Criminal and National Security)
EL1B	ELSUR Transcripts (Criminal and National Security)
ELA	Intercepts / Overhears
EMAIL	E-Mail
FA	Financial Analysis
FF	Forfeiture
FISUR	Physical Surveillance Logs
FTP	Federal Taxpayer Information
FUG	Fugitives
GJ	Federal Grand Jury Subpoenas and Materials
INTEL	Intelligence
INTELPRODS	Written Intelligence Products
LAB	Laboratory / Latent Reports
LEADS	Leads
LEGAL	Legal Documents
LIAISON	Liaison and FD-999s
LOC	Locations
MC	Mail Covers (Criminal and National Security)
MEDIA	Media Reports
MISC	Miscellaneous
NC	Newspaper Clippings and Press Releases
NSL	National Security Letters
OGA	Other Government Agencies - Information / Reports
OM	Other Matters

b7E

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

OPS	Operation Plans
PEN	Pen Register / Trap And Trace
PH	Photographs (paper copies only)
PR	Police Reports
RECORDS	Bank / Tax / Financial Records
REPORTS	Reports
S	Suspects / Subjects
SBP	Administrative Subpoenas
SURV	Surveillance
SW	Search Warrants (Criminal)
T3	Consensual Monitoring Calls / Title III
TC	Trash Covers
TEL	Telephone Subscriber / Toll Information / Trap & Trace Calls
TERRFIN	Terrorist Financing-Related Information
TS	Top Secret Documents
TRANS	Transcripts
TVL	Travel
UCO	Undercover Operations (Group I and Group II UCOs)
VOU	Vouchers
1A	1A Exhibit
1B	Evidence Chain of Custody (FD-1087s)
1C	Bulky, Non-Evidence (FD-1087s)
1D	ELSUR
FD302	FD-302s (and other testimonial documents)

(U) When more than one sub-file is needed for a specific category, sequential numbers are to be used adjacent to the described sub-file name. For example, three forfeiture sub-files would be named: FF1, FF2, FF3, etc.

J.2 (U) INDEXING - THE ROLE OF INDEXING IN THE MANAGEMENT OF FBI INFORMATION

(U//~~FOUO~~) The text of FBI-generated records (including, but not limited to, FD-65, FD-786, and nontransitory electronic mail [e-mail] records) must be imported into the FBI's central recordkeeping system to be searchable, retrievable, and sharable through automated means. A full text search of the FBI's central recordkeeping system identifies only information that is available electronically and does not search for information that may be contained in the FBI's paper records. Regardless of whether a record is imported or created in the FBI's central recordkeeping system, it must be indexed.

(U//~~FOUO~~) The purpose of indexing is to record individual's names; non-individual's names, such as corporations; and property which are relevant to FBI investigations so that this information can be retrieved, if necessary. The most common use of indexed information is to respond to executive branch agencies' request name searches as part of their investigations to determine suitability for employment, trustworthiness for access to classified information and eligibility for certain government benefits. If employees do not properly index names and places that arise in FBI investigations, the FBI could provide erroneous information to other federal agencies. Further advice about how to index and what should be indexed can be found on the [IMD Intranet site](#).

This Page is Intentionally Blank.

K APPENDIX K: (U) REQUIREMENT FOR ALL FBI PERSONNEL TO REPORT SUSPECTED ABUSE

K.1 (U) MANDATORY REPORTING

(U) Consistent with the *Attorney General Guidelines for Victim and Witness Assistance* (AGG-VWA),⁸⁹ all FBI personnel – regardless of job function, position, or title – are mandatory reporters of suspected abuse. Accordingly, FBI personnel who suspect that any of the following categories of individuals are being (or have been) subjected to abuse must report the allegations as described in this policy:

- A. (U) Children⁹⁰
- B. (U) Elderly persons⁹¹
- C. (U) Otherwise vulnerable individuals⁹²

(U) Unless an exception is approved in accordance with subsection K.5, all reports of suspected abuse must be made without delay. For the purposes of this policy, “without delay” means initiating the reporting requirements in subsection K.2 without unnecessary or unreasonable deviations and no later than 24 hours after learning of facts that lead the mandatory reporter to suspect that abuse is occurring (or has occurred).

(U) These mandatory reporting requirements apply to all FBI personnel (except when an exception to the prompt reporting is approved in accordance with subsection K.5. FBI personnel need not personally witness or observe (i.e., hear or see) specific activities in order to suspect active or historical abuse. Rather, FBI personnel are required to make reports pursuant to this policy any time that they learn of facts that give reason to suspect abuse – including when such activity inadvertently or incidentally comes to their attention.

(U) The requirements in this policy are consistent with federal law and DOJ policy, but FBI personnel are also subject to applicable state, local, tribal, and territorial (SLTT) laws governing mandatory reporting requirements and procedures in their specific areas of responsibility (AOR). Accordingly, FBI personnel should familiarize themselves with applicable SLTT laws and direct questions about the applicability of these statutory requirements to chief division counsels (CDC) or the Office of the General Counsel (OGC). If an SLTT jurisdiction has more stringent reporting requirements than those contained in this policy, FBI personnel are required to comply with the more stringent SLTT law.

(U) Consistent with DIOG subsection 2.5, this policy is not intended to, does not, and may not be relied upon to create any rights, substantive or procedural, enforceable by law by any party in any matter, civil or criminal, nor does it place any limitation on otherwise lawful investigative and litigative prerogatives of the DOJ and the FBI.

(U) Definitions of terms used in this policy are included below in subsection K.7. FBI personnel who are unsure if an activity qualifies as abuse (and is therefore subject to the reporting requirements in this policy) should contact their CDCs or OGC’s *Investigative Law Unit (ILU)* for

⁸⁹ (U) The AGG-VWA was published in 2011 and updated in May 2012.

⁹⁰ (U) See AGG-VWA Art. III.L.1.c.

⁹¹ (U) See AGG-VWA Art. III.L.3.b.

⁹² (U) See AGG-VWA Art. III.L.3.b.

assistance. Generally, if the requirement to report suspected abuse is unclear, FBI personnel should err on the side of caution and complete the reporting procedures in this policy.

(U) Comprehensive requirements pertaining to other aspects of the victim services program are located in the Victim Services Policy Guide (1010PG).

K.2 (U) REPORTING TO APPLICABLE AGENCIES

(U) As mandatory reporters, all FBI personnel are required to report suspected abuse to the SLTT law enforcement (LE) agency with jurisdiction to investigate the allegations. Additionally, when applicable, all FBI personnel are required to report suspected abuse to the child protective services agency or adult protective services agency with jurisdiction to protect the allegedly abused individual. (These LE and social services agencies are collectively referred to hereafter as “the applicable SLTT agencies”). Generally, the applicable SLTT agencies are articulated in SLTT laws. FBI personnel who are unable to determine the applicable SLTT agencies for a report should consult a CDC or OGC’s ILU for guidance.

(U) When working as part of a squad or multidisciplinary team (MDT), multiple FBI personnel may simultaneously learn of facts giving them reason to suspect abuse. In these circumstances, the individual with the most direct information regarding the allegations is required to make the report to the applicable SLTT agencies. Other personnel on the squad or MDT should not make duplicate reports unless they are augmenting the original report with new facts or distinguishable elements of the suspected abuse.

(U) FBI personnel may consult victim specialists (VS) or other victim services providers (VSP) for guidance on properly making reports to applicable SLTT agencies. However, FBI personnel cannot report allegations to a VS or a VSP in lieu of reporting allegations to applicable SLTT agencies or ask a VS or a VSP to make such a report on their behalf.

(U) Even when there is reason to believe that an incident was previously reported or is otherwise being investigated, FBI personnel should generally err on the side of caution and report the incident to the applicable SLTT agencies without delay. Specifically, FBI personnel are required to report any elements of suspected abuse (e.g., day, time, and place) that they reasonably know to be distinguishable from previous reports and/or investigations (due to the possibility of multiple offenses, unreported victims, or additional perpetrators). However, some allegations of abuse fall within the primary investigative jurisdiction of the FBI (e.g., certain Indian Country matters, special jurisdiction matters, and certain crimes against children matters). If a mandatory reporter definitively knows that suspected abuse is the subject of an FBI investigation, the suspected abuse does not need to be reported to other (i.e., SLTT) law enforcement agencies. FBI personnel still must report the abuse to the applicable child protective services agency or adult protective services agency if such reporting is necessary to further protect the allegedly abused individual. When considering if such reporting is necessary, FBI personnel should consider the nature of the suspected abuse and the likelihood of imminent criminal charges against the alleged abuser. FBI personnel should consult their FO/FBIHQ division heads, their CDCs, or OGC’s ILU to determine whether an additional report is reasonably necessary.

(U) As mandatory reporters, FBI personnel are generally immune from civil and criminal liability arising from reports that they make in good faith.

K.2.1 (U) REPORTING SUSPECTED CHILD ABUSE ON FEDERAL LAND/PROPERTY

(U) The FBI does not have primary investigative jurisdiction for all U.S. government-owned land and property. Pursuant to Title 34 U.S.C. § 20341, the Attorney General (AG) designates specific agencies (including some non-federal entities) to receive and investigate reports of child abuse on federal property (as well as federally operated or contracted facilities in which children are cared for or reside). FBI personnel who suspect that child abuse is taking place (or has taken place) on federal land/property must report the allegations to the applicable AG-designated agencies. If the AG has not designated an agency to investigate child abuse reports in a specific area, FBI personnel must instead report the allegations to the FBI field office in the AOR. FBI personnel who are unable to determine if the AG has designated an agency to receive and investigate child abuse allegations in a specific area should consult their CDCs or OGC's ILU for guidance.

K.2.2 (U) REPORTING SUSPECTED ABUSE IN FOREIGN JURISDICTIONS

(U) FBI personnel assigned outside of the United States or on temporary duty (TDY) assignments in foreign jurisdictions are also required to report suspected abuse:

- A. (U) Suspected abuse involving United States government employees or dependents under the chief of mission of a U.S. embassy must be reported to the State Department regional security officer (RSO) and the FBI legal attaché (LEGAT) (non-delegable).
- B. (U) If the suspected activity involves foreign citizen perpetrators or victims, FBI personnel should consult with the LEGAT and/or the RSO regarding any reporting laws of the foreign country and act accordingly. FBI personnel may request that the LEGAT or RSO report the suspected activity to the host government on their behalf.

(U) FBI personnel outside of the United States on personal travel should also report suspected abuse to the agencies with jurisdiction to investigate such reports and/or to the social services agencies with jurisdiction to protect the allegedly abused individuals. FBI personnel may contact the applicable LEGAT for assistance.

K.3 (U) FBI INTERNAL NOTIFICATION AND DOCUMENTATION PROCEDURES FOR SUSPECTED CHILD ABUSE

(U//~~FOUO~~) In addition to the reporting requirements described in subsection K.2, FBI personnel who learn of facts during the course of their official duties giving them reason to suspect child abuse must also:

1. (U//~~FOUO~~) Notify their FO/FBIHQ division heads as soon as practicable but no later than 48 hours after learning of the facts giving them reason to suspect child abuse;⁹³ and
2. (U//~~FOUO~~) Serialize an electronic communication (EC) in case file number 188D-HQ-A2450935 as soon as practicable but no later than five calendar days after completing the reporting requirements in subsection K.2 (see subsection K.3.1 for complete EC requirements).

⁹³ (U//~~FOUO~~) Each FO/FBIHQ division head may designate a secondary official to whom notifications may be made. For FOs, the designee must be no lower than an ASAC; for HQ divisions or offices, the designee must be no lower than an SC. The appointment of an FO/FBIHQ division head's designee must be documented in an EC to case file number 188D-HQ-A2450935.

(U//~~FOUO~~) FBI personnel who suspect child abuse outside of their official duties (i.e., “off duty”) may also notify their FO/FBIHQ division heads and consult relevant personnel (e.g., VSs) for guidance on properly filing reports pursuant to subsection K.2. However, FBI-specific notification and documentation is not required for “off duty” reports.⁹⁴

(U//~~FOUO~~) Generally, FBI personnel should notify their FO/FBIHQ division heads (or their documented designees) after completing the reporting requirements in subsection K.2. However, if FBI personnel notify their FO/FBIHQ division heads (or their documented designees) before filing reports pursuant to subsection K.2, the FO/FBIHQ division heads (or their documented designees) must ensure that FBI personnel complete the reports. FBI personnel cannot report allegations to their FO/FBIHQ division heads (or their documented designees) in lieu of reporting allegations to applicable SLTT agencies or ask their FO/FBIHQ division heads (or their documented designees) to make such reports on their behalf. FO/FBIHQ division heads (or their documented designees) are also responsible for ensuring completion of the required EC (see subsection K.3.1).

K.3.1 (U) ELECTRONIC COMMUNICATIONS FOR INTERNAL DOCUMENTATION OF CHILD ABUSE REPORTS

(U//~~FOUO~~) As described in subsection K.3, FBI personnel who learn of facts during the course of their official duties giving them reason to suspect child abuse must serialize an EC in case file number 188D-HQ-A2450935. The EC must be drafted as soon as practicable but no later than five calendar days after completing the reporting requirements in subsection K.2.

b7E

(U) The EC must include the following information (to the extent known and applicable):⁹⁵

(U//~~FOUO~~)

(U//~~FOUO~~)

(U//~~FOUO~~)

(U//~~FOUO~~)

(U//~~FOUO~~)

(U//~~FOUO~~)

(U//~~FOUO~~)

(U//~~FOUO~~)

⁹⁴ (U) For FBI policy on reporting misconduct (e.g., allegations of abuse committed by FBI personnel), see the *Office of Professional Responsibility Policy Guide* (116SPG) and the *Self-Reporting Requirements Policy Guide* (1037PG).

⁹⁵ (U) See the *Victim Services Division's (VSD) BuNet site* for a pony EC.

(U//~~FOUO~~) FBI personnel must index and submit this EC for approval as soon as practicable but no later than five calendar days after completing the reporting requirements in subsection K.2.

(U//~~FOUO~~) When the above information is properly documented in an EC to case file number

b7E

K.4 (U) SPECIAL NOTIFICATION REQUIREMENT FOR SUSPECTED HUMAN TRAFFICKING OF FOREIGN NATIONAL MINORS

(U//~~FOUO~~) In accordance with the Trafficking Victims Protection Act (TVPA),⁹⁷ FBI personnel are required to notify the U.S. Department of Health and Human Services (HHS) upon determining that a foreign national child may be the victim of human trafficking. Within 24 hours of making such a determination, FBI personnel must complete form FD-1181, “Notification to HHS of Suspected Trafficking of a Foreign National Child” and send it by UNet e-mail to HHS’ Office on Trafficking in Persons (OTIP) (childtrafficking@acf.hhs.gov). After notifying HHS OTIP, FBI personnel must serialize the completed FD-1181 in the relevant investigative case file in Sentinel

b7E

In the event that FBI personnel are notifying HHS of multiple potential victims at one time, an LHM or a spreadsheet with consolidated victim information may be appended to one FD-1181 form (in lieu of completing multiple FD-1181 forms).

(U//~~FOUO~~) If operational circumstances preclude FBI personnel from completing an FD-1181 within 24 hours, the reporting individual may instead notify HHS OTIP by phone (202-205-4582) or by e-mail (without an attached form). In such circumstances, the reporting individual must serialize a completed FD-1181 (or otherwise consolidated victim information) to the investigative case file (or zero file, if appropriate) in Sentinel as soon as practicable but no later than five business days thereafter. When notifying HHS without an FD-1181, the reporting individual should provide the following information (to the extent known and applicable):

(U)
(U)
(U)

b7E

(U//~~FOUO~~) When the above information is properly documented on an FD-1181 and serialized in Sentinel, FBI personnel are not required to complete an FD-999

“Assistance/Dissemination/Liaison Provided to Other Agencies” form to document the dissemination of victim information to HHS.⁹⁸ Additionally, FBI personnel are not permitted to complete an FD-999 in lieu of completing an FD-1181.

⁹⁶ (U//~~FOUO~~) Consistent with DIOG subsection 12.7.3, this provision establishes a limited exemption from DIOG subsections 12.6 and 12.7.1, which otherwise require the completion of an FD-999 form.

⁹⁷ (U) Including any subsequent reauthorizations of the TVPA.

⁹⁸ (U//~~FOUO~~) Consistent with DIOG subsection 12.7.3, this provision establishes a limited exemption from DIOG subsections 12.6 and 12.7.1, which otherwise require the completion of an FD-999 form.

(U) FBI personnel should contact VSD's Child Victim Services Unit (CVSU) with questions about this notification process.

K.5 (U//~~FOUO~~) AUTHORIZATION TO TEMPORARILY DELAY REPORTING

(U//~~FOUO~~) When FBI personnel suspect abuse based on information gathered during an investigation, they must make reasonable efforts to report the allegations to the applicable SLTT agencies in order to protect the safety of the allegedly abused individual. However, if it is not possible to report the allegations without significantly compromising the investigation, compromising a confidential source, disclosing protected information (e.g., classified information or law enforcement sensitive information), or endangering public safety, FBI personnel must, without delay, seek authorization from their FO/FBIHQ division heads to temporarily delay reporting. Only an FO/FBIHQ division head is authorized to make the determination to temporarily delay reporting (non-delegable). Whenever feasible, FO/FBIHQ division heads should make this determination within 48 hours of receiving a request to temporarily delay reporting.

(U//~~FOUO~~) Prior to requesting a delay in reporting, FBI personnel should consult relevant subject matter experts (e.g., a VS, a child and adolescent forensic interviewer [CAFI], or other VSD employee at FBIHQ) and must obtain a legal opinion from a CDC or ADC, OGC, or DOJ on the basis for the delay – including potential criminal and civil penalties. FBI personnel must include the legal opinion (and any relevant consultative information) in the requests to their FO/FBIHQ division heads. When approving and documenting their decisions to temporarily delay reporting, FO/FBIHQ division heads must include this legal opinion with an EC in case file [REDACTED] FO/FBIHQ division heads must monitor the case, and no later than every 30 days, re-review the case to determine if the abuse can be reported without impacting the investigation. These reviews must be documented in a new EC to case file [REDACTED] The instant that the basis for withholding the report no longer exists, FO/FBIHQ division heads must ensure that the suspected abuse is reported in accordance with subsection K.2 (and subsection K.4, if applicable).

b7E

K.6 (U) TRAINING

(U) On an annual basis, FBI personnel are required to complete training in the Virtual Academy (VA) system on child abuse reporting requirements and procedures. Based on completion reports generated by the Training Division (TD), FO/FBIHQ division heads (or their documented designees) are required to ensure compliance with this requirement.

K.7 (U) DEFINITIONS

(U) Many of the terms used in this appendix have different definitions depending on the context and applicable statutory or regulatory authorities. The following definitions should be used to read, interpret, and contextualize the requirements in this policy. Questions about the applicability of this policy should be directed to VSD, a CDC, or OGC's ILU. Generally, if the requirement to report suspected abuse is unclear, FBI personnel should err on the side of caution and complete the reporting procedures in subsection K.2.

K.7.1 (U) GENERAL DEFINITIONS

(U) **FBI personnel:** Any FBI employee or affiliated person authorized by appropriate authority to participate in an FBI investigation, activity, or mission, who is under the control and authority of the FBI. In accordance with DIOG section 2.11., this “includes, but is not limited to, an operational/administrative professional support person, intelligence analyst, special agent, task force officer (TFO), task force member (TFM), task force participant (TFP), detailee, and FBI contractor,” as well as a CHS “when operating pursuant to the tasking or instructions of an FBI employee.”

(U) **Otherwise vulnerable individuals** includes persons who are developmentally challenged, mentally ill, or physically disabled (see AGG-VWA Art.III.L.3.a and AGG-VWA Art.V.J.2). For example, persons with physical or mental limitations or disabilities that substantially impair their ability to adequately provide for their own care or protection of their person or property.

(U) **Severe form of trafficking**, as defined by the TPVA (22 U.S.C. § 7102(11)), is either of the following:

- (U) Sex trafficking (the recruitment, harboring, transportation, provision, obtaining, patronizing, or soliciting of a person for commercial sex) in which a commercial sex act is induced by force, fraud, or coercion, or in which the person induced to perform such acts has not attained 18 years of age.
- (U) The recruitment, harboring, transportation, provision, or obtaining of a person for labor or services, through the use of force, fraud, or coercion for the purpose of subjection to involuntary servitude, peonage, debt bondage, or slavery.

(U) **Suspected abuse:** The knowledge of facts leading a reasonable person to suspect that a child, elderly person, or otherwise vulnerable individual is subject to (or has been subjected to) actions that knowingly inflict physical or psychological harm or injury. This includes, but is not limited to physical abuse, mental abuse, exploitation (including sexual exploitation), sexual abuse, and negligent treatment. See below for specific statutory definitions of child abuse and elder abuse.

(U) **“Without delay”:** initiating the reporting requirements in subsection K.2 without unnecessary or unreasonable deviations and no later than 24 hours after learning of facts that lead the mandatory reporter to suspect that abuse is occurring (or has occurred).

K.7.2 (U) DEFINITIONS SPECIFIC TO CHILD ABUSE

(U) **Child:** A person under the age of 18 years.

(U) **Child abuse**, as defined by 34 U.S.C. § 20341(c)(1): the physical or mental injury, sexual abuse or sexual exploitation, or negligent treatment of a child.⁹⁹

(U) **Mental injury**, as defined by 34 U.S.C. § 20341(c)(3): harm to a child’s psychological or intellectual functioning which may be exhibited by severe anxiety, depression, withdrawal or outward aggressive behavior, or a combination of those behaviors, which may be demonstrated by a change in behavior, emotional response or cognition.

⁹⁹ (U) Pursuant to 34 U.S.C. § 20341(c)(8), child abuse does not include discipline administered by a parent or legal guardian to his or her child, provided that it is reasonable in manner and moderate in degree and otherwise does not constitute cruelty.

(U) **Negligent treatment**, as defined by 34 U.S.C. § 20341(c)(7): the failure to provide (for reasons other than poverty) adequate food, clothing, shelter, or medical care so as to seriously endanger the physical health of a child.

(U) **Physical injury**, as defined by 34 U.S.C. § 20341(c)(2), includes but is not limited to lacerations, fractured bones, burns, internal injuries, severe bruising or serious bodily harm.

(U) **Sexual abuse**:

- (U) As defined by 34 U.S.C. § 20341(c)(4): the employment, use, persuasion, inducement, enticement, or coercion of a child to engage in, or assist another person to engage in, sexually explicit conduct or the rape, molestation, prostitution, or other form of sexual exploitation of children, or incest with children.
- (U) As defined by 42 U.S.C. § 5106g(a)(4):
 - (U) A. The employment, use, persuasion, inducement, enticement, or coercion of any child to engage in, or assist any other person to engage in, any sexually explicit conduct or simulation of such conduct for the purpose of producing a visual depiction of such conduct; or
 - (U) B. The rape, and in cases of caretaker or inter-familial relationships, statutory rape, molestation, prostitution, or other form of sexual exploitation of children, or incest with children.

(U) **Sexual exploitation**, as defined by Art.III.L.1.b.(2) of the AGG-VWA, is all of the following:

- (U) The production, distribution, receipt, possession, or access of child pornography [child sexual abuse material (CSAM)].
- (U) The commercial sexual exploitation of children (prostitution).
- (U) The employment, use, persuasion, inducement, enticement, or coercion of a child to engage in, or assist another person to engage in, sexual abuse or sexual exploitation of children.

K.7.3 (U) DEFINITIONS SPECIFIC TO ELDER ABUSE

(U) **Abuse**, as defined by 42 U.S.C. § 1397j(1): the knowing infliction of physical or psychological harm or the knowing deprivation of goods or services that are necessary to meet essential needs or to avoid physical or psychological harm.

(U) **Elder** (or elderly person), as defined by 42 U.S.C. § 1397j(5): an individual age 60 or older.

(U) **Elder abuse**, as defined by 34 U.S.C. § 12291(a)(11): any action against a person who is 50 years of age or older¹⁰⁰ that constitutes the willful —

(A) infliction of injury, unreasonable confinement, intimidation, or cruel punishment with resulting physical harm, pain, or mental anguish; or

¹⁰⁰ (U) Although the Elder Justice Act defines an “elder” as “an individual age 60 or older” (see 42 U.S.C. § 1397j(5)), the Violence Against Women Act’s definition of “elder abuse” includes individuals age 50 or older (see 34 U.S.C. § 12291(a)(11)). FBI personnel who are unsure if an allegation constitutes abuse should generally err on the side of caution and complete the reporting procedures in subsection K.2 or consult a CDC or OGC’s ILU for guidance.

Domestic Investigations and Operations Guide

(B) deprivation by a person, including a caregiver, of goods or services with intent to cause physical harm

(U) **Exploitation**, as defined by 42 U.S.C. § 1397j(8): the fraudulent or otherwise illegal, unauthorized, or improper act or process of an individual, including a caregiver or fiduciary, that uses the resources of an elder for monetary or personal benefit, profit, or gain, or that results in depriving an elder of rightful access to, or use of, benefits, resources, belongings, or assets.

This Page is Intentionally Blank.

L APPENDIX L: (U) ON-LINE INVESTIGATIONS

(U) The policy for *Investigative Methods Conducted Online by FBI Employees* is U//~~LES~~. Also see the Quick Reference Guide for Online Investigations.

This Page is Intentionally Blank.



(U) DOMESTIC INVESTIGATIONS AND OPERATIONS GUIDE

Appendix L

(U) Investigative Methods Conducted Online by FBI Employees

(U) Version Dated: March 31, 2020

(U) Updated: June 02, 2021

Table of Contents

1. (U) Introduction	1
2. (U) General	2
2.1. (U) Protecting Civil Liberties.....	2
2.2. (U) Scope of This Appendix	3
2.3. (U) Principles	3
2.3.1. (U) Personal Online Activity	3
2.3.2. (U) Disclosure of FBI Affiliation	3
2.4. (U) Preserving Electronic Communications	5
2.5. (U) Online News Media	5
3. (U//LES) Authorized Activities Conducted Online Prior to Opening an Assessment (i.e., Pre-Assessment) or a Predicated Investigation	6
3.1. (U// LES) Public Information.....	6
3.1.1. (U) Publicly Available Information on the Internet.....	6
3.1.2. (U// LES) [REDACTED] Opening an Assessment or a Predicated Investigation	6
3.1.3. (U) Public Chat Rooms.....	9
3.1.4. (U// LES) Obtaining Identifying Information About Users or Networks	9
3.2. (U// LES) Information Restricted to Law Enforcement.....	10
3.3. (U// LES) [REDACTED]	10
3.3.1. (U) Definitions	11
3.4. (U) Pre-Assessment Documentation Requirements for Existing and Historical Information	11
3.4.1. (U) Processing a Complaint	11
3.4.2. Conducting Proactive Internet Searches of Publicly Available Information 13	
3.5. (U) Prohibited Activities Prior to Opening an Assessment.....	14
4. (U//LES) Authorized Investigative Methods Conducted Online: Assessments. 16	16
4.1. (U) Introduction.....	16
4.2. (U// LES) Publicly Available Information (DIOG 18.5.1)	16
4.3. (U// LES) [REDACTED]	16
4.3.1. (U) [REDACTED] Social Media.....	16
4.3.2. (U) Mandatory review.....	17
4.3.3. (U// LES) [REDACTED]	17
4.3.4. (U// LES) [REDACTED]	18
4.4. (U// LES) Private/Restricted Access	19
4.4.1. (U// LES) Consent Search: Obtaining Access to Restricted Online Web Sites with Consent	19
4.4.2. (U// LES) CHS Use and Recruitment (DIOG 18.5.5)	20
4.5. (U// LES) [REDACTED]	21
4.5.1. (U// LES) Interacting with the Public While in a Nonaffiliated Status	21

b7E

b7E

UNCLASSIFIED//~~LES~~
Domestic Investigations and Operations Guide

4.6.	(U// LES) Monitoring/Recording of Real-Time Communications in Assessments (Distinction Between Public and Private).....	22
4.6.1.	(U// LES) Public Real-Time Communications in Assessments (Recording Permitted if FBI Employee/CHS/Consenting Party is Present).....	22
4.6.2.	(U// LES) Private, Real-Time Online Communications in Assessments (Recording not Permitted).....	23
5.	(U//LES) Investigative Methods Conducted Online: Predicated Investigations	25
5.1.	(U) Introduction.....	25
5.2.	(U// LES) Consensual Monitoring of Communications, Including Electronic Communications (DIOG 18.6.1).....	25
5.2.1.	(U// LES) Private, Real-time Online Communications in Predicated Investigations.....	25
5.3.	(U// LES) Intercepting the Communications of a Computer Trespasser (DIOG 18.6.2).....	26
5.4.	(U// LES) Undercover Activity (DIOG 18.6.13.3).....	26
5.5.	(U// LES) Undercover Operations (DIOG 18.6.13.3).....	27
5.5.1.	(U// LES) Interim Authority to Continue Online Contacts.....	28
5.5.2.	(U// LES) Defining Substantive Undercover Contact in the Online Context	29
5.5.3.	(U// LES) [REDACTED].....	30
5.5.4.	(U// LES) [REDACTED].....	31
5.6.	(U// LES) [REDACTED].....	33
6.	(U//LES) Online Activity Leading to Undisclosed Participation.....	35
7.	(U//LES) Extraterritorial Online Activity	37
7.1.	(U// LES) Overview.....	37
7.2.	(U// LES) [REDACTED].....	38
7.3.	(U// LES) [REDACTED].....	38
7.4.	(U// LES) [REDACTED].....	39
7.5.	(U// LES) [REDACTED].....	40
7.6.	(U// LES) [REDACTED].....	40
8.	(U) DIOG Appendix L -Quick Reference Guide (QRG).....	42
9.	(U) Key Terms and Definitions.....	43

b7E

1. (U) Introduction

(U) **Purpose:** The purpose of this appendix is to assist Federal Bureau of Investigation (FBI) employees apply the Domestic Investigations and Operations Guide (DIOG) to investigative methods conducted online, prior to the opening of an Assessment or predicated investigation and within Assessments and predicated investigations. For guidance on extraterritorial (ET) matters pursuant to this appendix, please see Section 7 herein, entitled “Extraterritorial Online Activity.” See also DIOG Section 13, entitled “Extraterritorial Provisions” and the Foreign Technical Assistance Policy Directive and Policy Guide, 0641DPG.

(U) **Background:** The guidance in this document is derived from various statutes, previous electronic communications (EC), and other policy documents.

(U) This appendix establishes policies for online investigative methods.

(U) Online methods can present challenges and complexities that may not always be present in physical or “real-world” activities. These challenges, and the fast pace of evolving technology, lead to frequent changes in applicable laws. As a result, employees are urged to consult with their chief division counsels (CDC) and/or the FBI/Office of the General Counsel (OGC) before and during any proposed online activities.

(U) **Intended Audience:** The guidance in this appendix applies to all FBI personnel, as defined in DIOG Section 3, including FBI special agents (SA), analysts, other FBI employees, task force officers (TFO), task force members (TFM), FBI contractors, and others who engage in, supervise, or otherwise participate in online investigative activities and are bound by the Attorney General's Guidelines for Domestic FBI Operations (AGG-Dom) and the DIOG.

2. (U) General

2.1. (U) Protecting Civil Liberties

(U) The protections embodied in the DIOG are designed to ensure that the FBI adheres to the Constitution and laws of the United States and respects privacy, civil liberties, and First Amendment rights. These protections are particularly important when applied to online investigative methods because much of the content and many of the activities available or conducted on the Internet fall within some category of constitutionally protected information (e.g., freedom of individuals to associate, freedom to express an unpopular belief or opinion, or freedom to assemble). Accordingly, FBI employees must always carefully assess and analyze all investigative methods and communications conducted online.

(U) All principles stated previously in the DIOG that have been put in place to protect civil liberties also apply to investigative methods conducted online by FBI employees, such as the need to have a legitimate law enforcement purpose for all investigative activities, engaging in the least intrusive methods, sensitive investigative matters (SIM), and undisclosed participation (UDP). Online information, even if publicly available, may still be protected by the First Amendment.

(U) The FBI may only collect, as defined in subsection 3.1, of this appendix, information relating to the exercise of a First Amendment right if (1) the collection is logically related to an authorized investigative purpose, (2) the collection does not materially interfere with the ability of an individual or a group to engage in the exercise of constitutionally protected rights, and (3) the method of collection is the least intrusive alternative that is reasonable, based upon the circumstances of the investigation. The FBI cannot ever base its conduct solely on an individual's legal exercise of his or her First Amendment rights. Further, every FBI employee has the responsibility to ensure that the activities of the FBI are "lawful, appropriate and ethical as well as effective in protecting the civil liberties and privacy of individuals in the United States." (See DIOG 4.1.3.)

(U) Consistent with the DIOG, FBI employees must always ensure that all online investigative activities are "focused in scope, time, and manner to achieve the underlying purpose." (See DIOG 4.1.2.) FBI employees must document this relationship, as necessary, in the case file.

2.2. (U) Scope of This Appendix

(U) This appendix only applies to investigative methods conducted online by FBI employees, as they are defined in DIOG Section 3. This appendix sets out the standards for these investigative methods engaged in while online by FBI employees in both an affiliated and nonaffiliated status and in both public and private forums.

(U//~~FOUO~~) This appendix applies to FBI domestic investigative and intelligence collection activities, and it does not apply to other authorized online activities of the FBI. The authority for other online activities may be derived from the authority of the Attorney General (AG), federal statutes, or executive orders (EO), and those authorities should be relied upon when engaging in such online activities. For example, the FBI has the authority to engage in certain noninvestigative or nonoperational research and training while online, including online administrative searches or checks. The Office of Public Affairs (OPA) is involved in the creation and maintenance of overt FBI-sponsored Web sites and social media sites for public affairs purposes, and that type of online activity is outside the scope of this appendix.

(U//~~FOUO~~)

b7E

2.3. (U) Principles

2.3.1. (U) Personal Online Activity

(U) FBI employees are not permitted to use any personal online accounts to access information for official purposes. Such use may inappropriately associate an employee's identity with official FBI activity and may inappropriately result in access to restricted information.

(U) An FBI employee is generally free to engage in solely personal, appropriate, online pursuits while off duty. If, however, the off-duty online activities of the FBI employee are within the scope of an ongoing investigation, serving the goals of an ongoing investigation, or undertaken for the purpose of developing investigative leads, the FBI employee is bound by the same policies and restrictions for online investigative activities as when he or she is on duty.

2.3.2. (U) Disclosure of FBI Affiliation

(U) When an FBI employee engages in investigative methods online, the same principles apply as in the physical world as they relate to when the individual must provide official identification as an FBI employee and when that requirement does not exist. When interacting with members of the public as part of their official duties, FBI employees must operate openly and consensually (DIOG 18.5.6). The use of the FBI UNet (unclassified network) to access the Internet can reveal government affiliation; however, this is not sufficient to satisfy the requirement to "disclose the employee's affiliation with

~~UNCLASSIFIED//LES~~
Domestic Investigations and Operations Guide

the FBI" when seeking information from witnesses, subjects, or victims. The disclosure of FBI affiliation must be explicit and overt when requesting information from members of the public and from private entities, unless there is an authorized basis for not disclosing FBI affiliation. An employee can achieve this by explicitly stating his or her FBI affiliation within the content of a message.

(U)

1. (U//~~LES~~)

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

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

- (U//~~FOUO~~) Certified undercover employee (UCE) is defined as an employee of the FBI or other federal, state, or local law enforcement agency; another entity of the United States Intelligence Community (USIC); or a foreign intelligence agency, working under the direction and control of the FBI, and whose relationship with the FBI is concealed from third parties by the maintenance of a cover or an alias identity. A UCE's identity and alias must be guarded closely to protect the safety of the UCE and the integrity of the undercover operation (UCO).
- (U//~~FOUO~~) Certified online covert employee (OCE) is defined as an employee of the FBI, or another federal, state, or local law enforcement agency; another entity of the USIC; or a foreign intelligence agency, acting at the behest of the FBI in an online capacity, and whose identity is concealed from third parties by the maintenance of a cover or an alias identity. An OCE's identity and alias must be guarded closely to protect the safety of the OCE and the integrity of the UCO.

(U//~~FOUO~~) When interacting with the public online, employees must take necessary action to ensure they are sufficiently identified in true name/law enforcement affiliation, unless authorized as described above. In order to identify oneself fully when overtly interacting with the public online, the employee must include his or her true name and affiliation with law enforcement with each posted comment. For electronic mail (e-mail) communications, employees must use their fbi.gov e-mail addresses and/or other official, overt, government-sponsored e-mail account addresses and identify themselves by their law enforcement affiliations in the content of the messages. In short, in any overt online communications, enough indicators of name, official title, and the agency must be included such that a reasonable person would understand that he or she is providing information to law enforcement.

(U//~~LES~~) Example:

UNCLASSIFIED//~~LES~~
Domestic Investigations and Operations Guide

(U//~~LES~~) Example

b7E

2.4. (U) Preserving Electronic Communications

(U//~~LES~~) Employees should retain the contents of stored electronic messages, such as e-mails, if they would have retained those messages had they been written on paper.

b7E

 the employee should memorialize any information of investigative value in an FD-302 ("Form for Reporting Information That May Become the Subject of Testimony"). The contents must be preserved in a manner authorized by FBI procedures governing the preservation of electronic communications (e.g., see the Preservation and Disclosure of Electronic Communications in Federal Criminal Cases, 0423D and Electronic Discovery Policy Implementation Guide, 0140PG).

2.5. (U) Online News Media

(U) The DIOG establishes additional oversight and approval requirements for assessments and predicated investigations involving SIMs. Investigations involving the activities of the news media on the Internet are SIMs. (See DIOG 10.1.2.2.5 for the definition of "news media" and DIOG 18.5.6.4.8 for rules on interviews or contact with the news media.)

3. ~~(U//LES)~~ Authorized Activities Conducted Online Prior to Opening an Assessment (i.e., Pre-Assessment) or a Predicated Investigation

3.1. ~~(U//LES)~~ Public Information

~~(U//LES)~~ DIOG 5.1.1.1 authorizes employees to search for and view various forms of online information prior to the initiation of an Assessment or a predicated investigation, including various government systems and paid-for-service databases, as well as information available to the public via the Internet. Employees must be mindful that if they are online prior to opening an Assessment or a predicated investigation, there must be a rational reason—tied to criminal activity or a national security threat—to search for and view the online information or data being sought. As always, to protect the public's constitutional rights, privacy, and civil liberties, employees must review, analyze, and document their investigative activities carefully. For further discussion, see DIOG subsections 4.2 and 5.1.

3.1.1. (U) Publicly Available Information on the Internet

~~(U//LES)~~ FBI employees may conduct Internet searches of “publicly available information” for authorized purposes prior to the initiation of an Assessment or a predicated investigation. To be considered publicly available information, the online content must be available to the employee in the same manner that it is to the general public. Where the online resource requires the employee to register for access, access to that resource is considered available to the public if the registration process is designed to accept all applications from the public and in no other way creates a restriction as to who may access the information.

~~(U//LES)~~ Online information that requires a fee for access is considered publicly available information if anyone in the general public can purchase access to the same information. In this situation, paying a fee for access is comparable to paying for a newspaper that is offered for sale to the public. (See DIOG subsection 18.5.1.1.D.) See also Appendix L, subsection 3.2, “Information Restricted to Law Enforcement,” for guidance related to online subscription services provided to law enforcement or Intelligence Community (IC) agencies.

~~(U//LES)~~ To the contrary, certain online venues or sites, such as social networking sites, allow users to restrict access to their information. Even if a site allows anyone in the general public to establish an account, it does not mean that all information posted by various users is publicly available information. If the information owner restricts access to the information, then it is not publicly available information.

3.1.2. ~~(U//LES)~~ [REDACTED] Opening an Assessment or a Predicated Investigation

~~(U//FOUO)~~ While online prior to opening an Assessment, an FBI employee must generally operate openly and consensually with members of the public [REDACTED]

[REDACTED]

b7E

UNCLASSIFIED//~~LES~~
Domestic Investigations and Operations Guide

(U//~~LES~~)

b7E

(U//~~LES~~)

1) (U//~~LES~~)

2) (U//~~LES~~)

(U//~~LES~~)

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

b7E

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

U//~~FOUO~~

(U//~~LES~~)

¹ (U//~~LES~~) In the context of this appendix

b7E

UNCLASSIFIED//~~LES~~
Domestic Investigations and Operations Guide

b7E

(U//~~FOUO~~)

(U//~~LES~~) Example 1b

(U//~~FOUO~~)

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

UNCLASSIFIED//~~LES~~
Domestic Investigations and Operations Guide

[Redacted]

b7E

(U//~~LES~~)

[Redacted]

(U//~~FOUO~~)

[Redacted]

3.1.3. (U) Public Chat Rooms

(U//~~LES~~) Information contained in a public chat room may fall within the category of publicly available information. Public chat rooms are comparable to attending a public meeting and may be used to review public information prior to the opening of an Assessment or a predicated investigation. (See DIOG subsections 5.1.1.1 and 18.5.1.E.)

[Redacted]

b7E

(U//~~LES~~) Example

[Redacted]

(U//~~LES~~) Response

[Redacted]

3.1.4. (U//~~LES~~) Obtaining Identifying Information About Users or Networks

(U//~~LES~~) There are widely available software tools for obtaining publicly available identifying information about an individual or a host computer on a network. [Redacted]

[Redacted] Employees may use such tools in their intended, lawful manner under the same circumstances that the DIOG authorizes employees to look up similar identifying information (e.g., a telephone number) through nonelectronic means. Employees must be careful to use these information-gathering tools only as

b6
b7C

UNCLASSIFIED//~~LES~~
Domestic Investigations and Operations Guide

conventionally permitted and not in a manner unauthorized by the system, such as by exploiting design flaws in a program or by using software tools to circumvent operating system protections or restrictions placed on system users.

(U//~~LES~~) Example

b7E

(U//~~LES~~) Certain tools, even though commonly and openly available on the Internet and used by the public, are not permitted for use by law enforcement if their use would violate statutory restrictions such as those found in the Electronic Communication and Privacy Act (ECPA) or Title III.

(U//~~LES~~) Example

b7E

3.2. (U//~~LES~~) Information Restricted to Law Enforcement

(U//~~LES~~)

(See the examples at DIOG subsection 5.6.3.1.10.1.)

(U//~~LES~~) Some database providers offer access to the public through subscription while still reserving specific categories of information exclusively for law enforcement access (e.g., Lexis/Nexis). The FBI might contract for access to both the public and restricted portions of the database information.

b7E

3.3. (U//~~LES~~)

(U//~~LES~~)

UNCLASSIFIED//~~LES~~
Domestic Investigations and Operations Guide

3.3.1. (U) Definitions

1. (U//~~LES~~) [REDACTED]

2. (U//~~LES~~) [REDACTED]

b7E

3. (U//~~LES~~) [REDACTED]

(U) [REDACTED]

b7E

(U//~~LES~~) Example [REDACTED]

3.4. (U) Pre-Assessment Documentation Requirements for Existing and Historical Information

(U//~~FOUO~~) Consistent with DIOG subsection 5.1.2, FBI employees may conduct Internet searches of publicly available information for authorized purposes prior to the initiation of an Assessment or a predicated investigation. The following documentation requirements differ, depending on whether the searches are being conducted pursuant to (1) processing a complaint and responding to a tip or a lead, or (2) conducting proactive Internet searches of publicly available information.

3.4.1. (U) Processing a Complaint

(U//~~FOUO~~) FBI employees are permitted to retain records checks and other information collected while processing a complaint or while responding to a tip or a lead by using permitted DIOG 5.1.1 activities. This collection and retention is permitted if, in the judgment of the FBI employee, there is a law enforcement, national security, intelligence, or public safety purpose. This documentation must be completed as soon as practicable,

UNCLASSIFIED//~~LES~~
Domestic Investigations and Operations Guide

but not more than five business days from the receipt of the information. When permitted, such documentation must be retained in one of the following files:

- (A)(U//~~FOUO~~) A zero classification file, when no further investigative activity is warranted
- (B)(U//~~FOUO~~) A relevant, open or closed Assessment
- (C)(U//~~FOUO~~) A relevant, open or closed predicated investigation file
- (D)(U//~~FOUO~~) A new Assessment or predicated investigation file, when further investigative activity is warranted
- (E)(U//~~FOUO~~) An unaddressed work file

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

b7E

(U//~~FOUO~~) Response

b7E

(U//~~FOUO~~) Example 1a:

b7E

(U//~~FOUO~~) Response

3.4.2. Conducting Proactive Internet Searches of Publicly Available Information

(U//~~FOUO~~) FBI employees are permitted to conduct proactive Internet searches (i.e., searches that are not conducted as a result of incoming complaints, tips, leads, or referrals) of publicly available information to process observations or other information for authorized purposes, but they may only collect and retain this information if a law enforcement, national security, intelligence, or public safety purpose exists for doing so and the information is within the scope of an open Assessment or a predicated case, or if it serves as the basis for opening such. See also DIOG, subsection 4.2, “Protection of First Amendment Rights.” This documentation must be completed as soon as practicable, but not more than five business days from the receipt of the information. When documentation of the search is permitted, such documentation must be retained in one of the following files (with a summary narrative tying the information to an FBI criminal or national security purpose):

- (A) (U//~~FOUO~~) A relevant, open assessment
- (B) (U//~~FOUO~~) A relevant, open predicated investigation file
- (C) (U//~~FOUO~~) A new assessment or predicated investigation file, when further investigative activity is warranted

(U//~~FOUO~~) If, however, in the judgment of the FBI employee, the records checks or other information obtained using permitted DIOG 5.1.1 activities does not serve a law enforcement, national security, intelligence, or public safety purpose, then those records checks, data, information, or documents cannot be retained and must be destroyed. This requirement to destroy applies to information printed or stored on removable media, stored within a public database (history of searches and queries), or stored in any other physical or digital location capable of maintaining a search or query history that is within the control of the FBI employee.

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

(U//~~FOUO~~)

UNCLASSIFIED//~~LES~~
Domestic Investigations and Operations Guide

b7E

(U//~~FOUO~~) Response:

b7E

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

(U//~~FOUO~~) Response:

b7E

3.5. (U) Prohibited Activities Prior to Opening an Assessment

The following activities are prohibited prior to opening an assessment:

- (U)

(U) Exception

~~UNCLASSIFIED//LES~~
Domestic Investigations and Operations Guide

b7E

- (U/LES) [redacted]
- (U/LES) [redacted]
- (U/LES) Example [redacted]

(U/LES) **Exception:** The only exception to this rule is that prior to opening an Assessment or a predicated investigation, an employee may employ limited use of his or her official e-mail to conduct a “clarifying interview.” (See DIOG 5.1.1.1, 5.1.1.5, and 5.1.1.6.) In this limited circumstance, the employee must overtly identify himself or herself as being affiliated with the FBI [redacted] When conducting such clarifying interviews online, employees must use their official FBI Internet e-mail accounts (i.e., username@fbi.gov) or any other government-sponsored, overt e-mail account addresses and must identify themselves as FBI employees in the content of the e-mail messages. [redacted]

b7E

4. (U//~~LES~~) Authorized Investigative Methods Conducted Online: Assessments

4.1. (U) Introduction

(U//~~LES~~) All investigative methods authorized prior to the opening of assessments or predicated investigations are authorized during assessments. Consistent with DIOG 18.5, the following online methods are authorized during an assessment.

4.2. (U//~~LES~~) Publicly Available Information (DIOG 18.5.1)

(U//~~LES~~) In addition to the online investigative methods defined in subsection 3.1 of this appendix, once an assessment has been opened, employees may also use automated regular searches (e.g., Google alerts) to conduct regular searches of publicly available information. However, as stated in subsection 3.1, to protect the public's constitutional rights, privacy, and civil liberties, employees must review, analyze, and document their investigative activities carefully. For further discussion, see DIOG 4.2.

4.3. (U//~~LES~~) [REDACTED]

b7E

(U//~~LES~~) Warning [REDACTED]

(U//~~LES~~) [REDACTED] the FBI should generally deal openly with the public during an assessment. It is permissible in an assessment (see DIOG 18.5.6.4.9 and 18.5.6.4.11.1.) [REDACTED]

4.3.1. (U) [REDACTED] Social Media

b7E

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

~~UNCLASSIFIED//LES~~
Domestic Investigations and Operations Guide

4.3.2. (U) Mandatory review

(U//~~FOUO~~) Statements made by subjects of assessments and predicated investigations utilizing social media generally include content protected by the First Amendment. The FBI may only collect, as defined in subsection 3.1 of this appendix, information relating to the exercise of a First Amendment right if (1) the collection is logically related to an authorized investigative purpose, (2) the collection does not materially interfere with the ability of an individual or a group to engage in the exercise of constitutionally protected rights, and (3) the method of collection is the least intrusive alternative that is reasonable, based upon the circumstances of the investigation. While conducting file reviews and assessment justification reviews pursuant to DIOG 3.5.4, supervisory personnel must ensure that collection of content/materials [REDACTED]

b7E

[REDACTED] are consistent with subsection 3.1 of this appendix.

4.3.3. (U//~~LES~~) [REDACTED]

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

[REDACTED]

(See DIOG 18.5.6.4.9.)

(U//~~FOUO~~) For Type 5 assessments, detailed policy requirements regarding an [REDACTED] in the *Confidential Human Source Policy Guide (CHSPG)*, 1116PG.

b7E

(U//~~LES~~) **Warning** [REDACTED]

[REDACTED]

(U//~~LES~~) **Note** [REDACTED]

[REDACTED]

(U//~~LES~~) **Warning** [REDACTED]

[REDACTED]

UNCLASSIFIED//~~LES~~
Domestic Investigations and Operations Guide

[Redacted]

b7E

[Redacted] (See
DIOG 18.5.6.4.9 and 18.5.6.4.11.9 and subsection 4.5.1 of this appendix for
additional information.)

(U//~~LES~~) Example [Redacted]
[Redacted]

4.3.4. (U//~~LES~~) [Redacted]

b7E

(U//~~LES~~) [Redacted]
[Redacted]
[Redacted] (See
DIOG 18.5.6.4.11.1.) [Redacted]
[Redacted] outlined in DIOG 18.5.6.4.9 (D)

[Redacted]

(U//~~LES~~) Example [Redacted]

b7E

[Redacted]

(U//~~LES~~) Example [Redacted]

[Redacted]

[Redacted] (See
DIOG 18.5.6.4.9.D.2.)

(U//~~LES~~) If justification develops to open of a Preliminary Investigation
("information or allegation" indicating the existence of federal criminal activity or
a threat to national security or to protect against such activity or threat [see DIOG
6.5]) the employee may seek oral approval [Redacted]

[redacted] and obtain oral authority for consensual monitoring, consistent with DIOG 18.6.1, if necessary under the circumstances.

b7E

(U//~~LES~~) Example [redacted]

[redacted]

(U//~~LES~~) Note: [redacted]

[redacted] (See DIOG 18.5.6.4.9.)

4.4. (U//~~LES~~) Private/Restricted Access

4.4.1. (U//~~LES~~) Consent Search: Obtaining Access to Restricted Online Web Sites with Consent

(U//~~LES~~) Note: A consenting party is someone with the authorization to “access and control” content on the site. This includes the account holder for a social-networking site, the system administrator, or a company official with authority to direct others regarding site content. An employee may also access a restricted site if the owner makes the site available to a category of Internet users that includes the employee [redacted]

b7E

(U//~~LES~~) In order to access private or restricted-access online forums, as in the physical world, an exception to the search warrant requirement is needed. The most commonly utilized exception during FBI investigative methods conducted online is consent. Internet content not available to the general public is considered restricted access. Access may be restricted to a few select persons [redacted]

[redacted] or may be restricted to a certain class of individuals [redacted]

Such sites are considered restricted sources of online information. An employee is authorized to obtain access to such sites during an assessment if the consenting party [redacted] is fully aware of the employee’s

b7E

affiliation with the FBI and has authority to consent, as demonstrated by the consenting party’s access and control. Written consent must be obtained whenever possible from the consenting party and documented in the case file. For CHSs, this documentation must be maintained in CHS files. If the consenting party declines to provide written consent, oral consent is acceptable, as long as two employees (one of whom must be an FBI agent) witness the consent, and the consent is documented in an FD-302 (“Form for Reporting Information That May Become the Subject of Testimony” [redacted])

[redacted] This activity constitutes a consent search, and it is fully authorized during an assessment. (See DIOG 5.9.1.) As is the case with all consent searches, the employee must always be mindful of the exact consent given and whether the consenting party has the lawful authority to grant the actual consent provided to the employee.

UNCLASSIFIED//~~LES~~
Domestic Investigations and Operations Guide

(U//~~LES~~) Example

[Redacted]

b7E

[Redacted]

(U//~~LES~~) Warning

[Redacted]

[Redacted]

4.4.2. (U//~~LES~~) CHS Use and Recruitment (DIOG 18.5.5)

4.4.2.1. (U//~~LES~~) Tasking a CHS/Nonconfidential Party to Access a Restricted Web Site (Authorized Access)

[Redacted]

b7E

(U//~~LES~~) A CHS/consenting party may be tasked to access a restricted Web site to gather information only if the CHS/consenting party has authorized access (consent) [Redacted]

b7E

[Redacted]

See subsection 5.2

[Redacted]

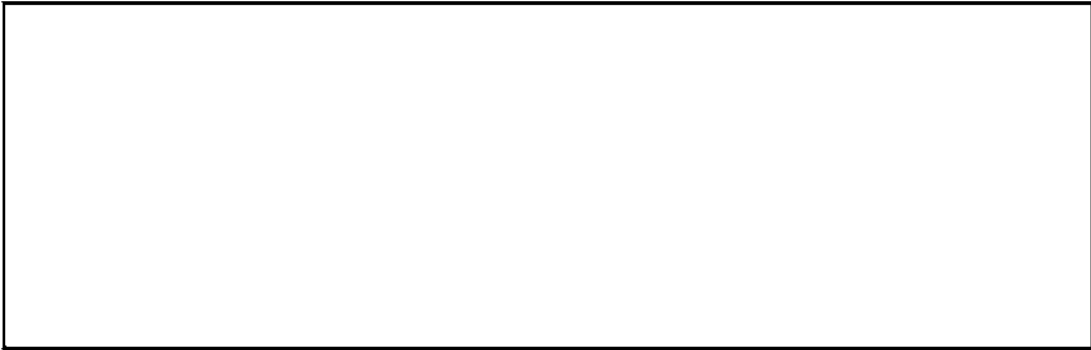
(U//~~LES~~) Example

[Redacted]

b7E

[Redacted]

UNCLASSIFIED//~~LES~~
Domestic Investigations and Operations Guide



b7E

4.5. (U//~~LES~~) [redacted]

b7E

(U//~~LES~~) [redacted] please see subsection 3.3.1. of this appendix.

4.5.1. (U//~~LES~~) Interacting with the Public While in a Nonaffiliated Status

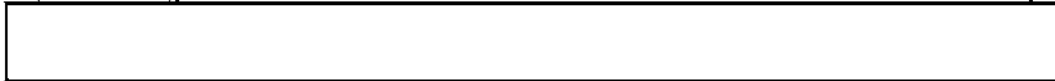
(U//~~LES~~) [redacted]

b7E



DIOG 18.5.6.4.9, as outlined below:

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



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



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



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

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

b7E



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

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



(U//~~LES~~) Example [redacted]



(U//~~LES~~)

4.6. (U//~~LES~~) Monitoring/Recording of Real-Time Communications in Assessments (Distinction Between Public and Private)

4.6.1. (U//~~LES~~) Public Real-Time Communications in Assessments (Recording Permitted if FBI Employee/CHS/Consenting Party is Present)

4.6.1.1. (U//~~LES~~) Definition of Public Real-Time Communication

(U//~~LES~~) A key factor in determining if an exchange is occurring in real time is whether the exchange is preserved and made available on the site to viewers later on. Forums where the communications are preserved for future viewers are generally not real time. Typically, a blog or bulletin board system preserves posted comments to enable future viewers to see the information, meaning that communications posted on these forums are not real time. Further, even when several contributors to a bulletin board site are using it to rapidly engage in an exchange, it is not a real-time forum, as the content enjoys some degree of permanency, even though the information may only be posted online for as little as a week. In contrast, a typical chat room is designed to allow only users currently in the room to view the exchange and does not preserve the exchange for those entering the room at a later point in time.

b7E

(U//~~LES~~) Legal authority: The monitoring/recording of most real-time communications on the Internet is protected by the First and Fourth Amendments and/or statutes such as Title III and the Foreign Intelligence Surveillance Act (FISA). There is a unique section of the Wiretap Act (18 U.S.C. 2511(2)(g)(i)) that allows “any person” to intercept an electronic communication that is readily accessible to the general public (i.e., public real-time communications”).

(U//~~LES~~) Approval requirement: Public real-time communications that are evidentiary in nature should be recorded if it is necessary to achieve the objective of the assessment and is the least intrusive means to do so. Once the public real-time communications are recorded, only pertinent information may be documented/indexed into an FBI

~~UNCLASSIFIED//LES~~
Domestic Investigations and Operations Guide

Recordkeeping System (i.e., serialized via an FD-302). The complete recording must be stored as evidence in the investigative file and the communications must be preserved in a manner authorized by FBI procedures governing the preservation of electronic communications.

(U//~~LES~~) No real-time communications can be recorded if the employee is not present during the recording. While 18 U.S.C. 2511(2)(g)(i) allows the recording of public real-time communications without the presence of a consenting party or without a court order, as a matter of policy, FBI employees must be present to record public real-time communications during an assessment. [REDACTED]

[REDACTED] (See DIOG 18.6.3.5.) Additionally, in order to utilize the least intrusive means and to limit the collection of non-pertinent communications, the employee must observe the communications as they are being recorded.

(U//~~LES~~) Example: [REDACTED]

b7E

(U//~~LES~~) Example: [REDACTED]

(U//~~FOUO~~) The employee must ensure that information to be collected from the Internet is rationally related to his or her authorized purpose and can be lawfully obtained. The employee must properly document this analysis in the investigative file.

(U//~~LES~~) Recording a public, real-time, online communication utilizing a “screenshot” (digital image) or similar technology is permitted in an Assessment because it is not considered consensual monitoring of a private conversation between two individuals under federal law or FBI policy. Such screenshots of public, real-time communications are the equivalent of recording a person speaking before a crowd in a public park and are permitted. [REDACTED]

b7E

4.6.2. (U//~~LES~~) Private, Real-Time Online Communications in Assessments (Recording not Permitted)

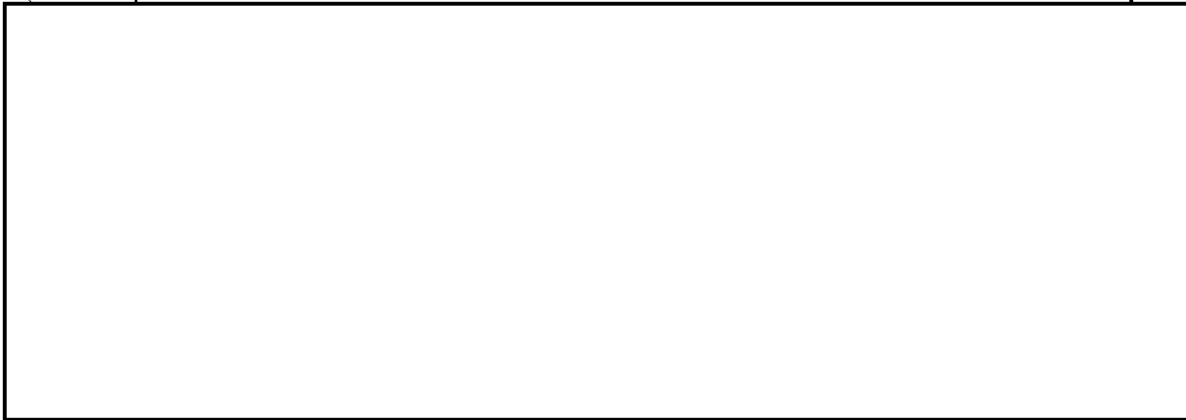
(U//~~LES~~) Significant amounts of real-time online communications are private communications (e.g., instant messaging or restricted chat rooms) requiring consensual monitoring authority to record. The AGG-Dom limits the use of consensual monitoring to predicated cases. In these situations, employees are permitted to monitor private, real-

Domestic Investigations and Operations Guide

time online communications during an assessment (with or through a CHS or non-confidential party only), but cannot electronically record them.

(U//~~LES~~

b7E



5. (U//~~LES~~) Investigative Methods Conducted Online: Predicated Investigations

5.1. (U) Introduction

(U//~~LES~~) In predicated investigations (a Preliminary Investigation, a Full Investigation, an Enterprise Investigation, or a positive foreign intelligence investigation), all online investigative methods authorized prior to the opening of an assessment or during an assessment are authorized. The following online methods are also authorized during predicated investigations.

5.2. (U//~~LES~~) Consensual Monitoring of Communications, Including Electronic Communications (DIOG 18.6.1)

5.2.1. (U//~~LES~~) Private, Real-time Online Communications in Predicated Investigations

(U//~~LES~~) Monitoring of wire, oral, or electronic communications based on the consent of one party to the communication is referred to as consensual monitoring (DIOG 18.6.1.1). In the online environment, the recording of private real-time communications that is restricted from public access is considered consensual monitoring and is only authorized in predicated investigations.

(U//~~LES~~) A restricted online environment is defined as one that is not available to the general public. (See subsection 3.1 of this appendix for further discussion of publicly accessible).

(U//~~LES~~) Example:

(U//~~LES~~) Example:

(U//~~LES~~) There are many real-time online forums that involve many people communicating simultaneously (e.g., chat rooms). While employees are cautioned against recording communications not pertinent to the investigation, where feasible (see DIOG

~~UNCLASSIFIED//LES~~
Domestic Investigations and Operations Guide

18.6.1.5.1.3), it may not be possible to selectively record comments not pertinent to the investigation that have been made by other participants. When nonpertinent communications are intermixed with pertinent communications, recording of the nonpertinent communications is sometimes unavoidable. The employee must always later review the recordings and redact or minimize, as necessary, particularly when disclosing the recording to a third party.

(U//~~LES~~) The employee or OCE must observe/be present during the online communications as they are recorded. No private real-time communications may be recorded if the employee is not present during the recording, that is, to provide the one-party consent.

(U//~~LES~~) As noted in appendix L subsection 4.1.1, the recording of public real-time communications and the collection of information from restricted forums (authorized in both assessments and predicated investigations) that are not real time do not require consensual monitoring authority. Therefore, when operating within a predicated investigation, it is critical to establish if the forum is restricted and real time to determine whether the employee needs consensual monitoring authority.

(U//~~LES~~) **Approval:** The employee must obtain [redacted] and supervisory approval authority to conduct consensual monitoring prior to recording private real-time communications in a restricted forum, in accordance with DIOG 18.6.1. In the FD-759, "Notification of Authority Granted for Use of Electronic Monitoring Equipment Not Requiring a Court Order" (form for consensual monitoring), the employee must articulate how the information to be collected by the recording is relevant to the predicated investigation. When approving the FD-759, the supervisor must consider if recording the communications is the least intrusive method to obtain the evidentiary information, weighing the investigative value of the evidence to be obtained against the potential collection of First Amendment activity. Once recorded, only pertinent information may be uploaded into an FBI Recordkeeping System to minimize the use of non-pertinent information that is only collected because it is commingled with pertinent, case-related information. The complete recording must be stored as evidence.

b7E

(U//~~LES~~) **Extraterritorial Considerations:** [redacted]

b7E

[redacted]
[redacted] DIOG 18.6.1.6.1, entitled "Party Located Outside the United States."

5.3. (U//~~LES~~) Intercepting the Communications of a Computer Trespasser (DIOG 18.6.2)

(U//~~FOUO~~) For a full description of this investigative method and the corresponding approvals, please see DIOG section 18.6.2.

5.4. (U//~~LES~~) Undercover Activity (DIOG 18.6.13.3)

(U//~~LES~~) **Warning** [redacted]

b7E

UNCLASSIFIED//~~LES~~
Domestic Investigations and Operations Guide

(U//~~LES~~)

b7E

(U//~~LES~~)

(U//~~LES~~) Example

b7E

(U//~~LES~~) Example

5.5. (U//~~LES~~) Undercover Operations (DIOG 18.6.13.3)

(U//~~LES~~)

b7E

Attorney General's Guidelines on Federal Bureau of Investigation Undercover Operations (AGG-UCO).

UNCLASSIFIED//~~LES~~
Domestic Investigations and Operations Guide

(U//~~LES~~)

(U//~~LES~~)

(U//~~LES~~)

(U//~~LES~~) **Approval:** The approval process for UCOs is addressed in DIOG 18.6.13. This subsection applies equally to online UCOs

5.5.1. (U//~~LES~~) Interim Authority to Continue Online Contacts

(U//~~LES~~) This subsection is limited to cases governed by the AGG-UCO. (See AGG-UCO IV.I.5.)

If interim authority is granted, the OCE must:

(a) (U//~~LES~~)

(b) (U//~~LES~~)

(c) (U//~~LES~~)

(d) (U//~~LES~~)

(e) (U//~~LES~~)

(f) (U//~~LES~~)

b7E

b7E

b7E

UNCLASSIFIED//~~LES~~
Domestic Investigations and Operations Guide

(U//~~LES~~) Employees must conform to all approval and documentation requirements

b7E

5.5.2. (U//~~LES~~) Defining Substantive Undercover Contact in the Online Context

(U//~~LES~~) The nature of online communications makes counting substantive “undercover contacts” (UCAs) more difficult than in the physical world. Generally, a physical-world contact consists of a single communication or conversation, either face-to-face or over the telephone, naturally circumscribed in time. In the online world, each discrete online conversation between an FBI employee and a subject also constitutes a separate undercover contact

b7E

(U//~~LES~~)

(U//~~LES~~)

(U//~~LES~~) The relevant considerations are:

a. (U//~~LES~~)

b7E

b. (U//~~LES~~)

c. (U//~~LES~~)

d. (U//~~LES~~)

UNCLASSIFIED//~~LES~~
Domestic Investigations and Operations Guide

[Redacted]

e. (U//~~LES~~) [Redacted]

[Redacted]

(U//~~LES~~) [Redacted]

[Redacted]

b7E

(U//~~LES~~) Note [Redacted]

[Redacted]

5.5.3. (U//~~LES~~) [Redacted]

(U//~~LES~~) [Redacted]

[Redacted]

(U//~~LES~~) [Redacted]

[Redacted]

b7E

(U//~~LES~~) Example [Redacted]

[Redacted]

UNCLASSIFIED//LES
Domestic Investigations and Operations Guide

(U//LES)

(U//LES) Approval:

- (U//FOUO)

b7E

- (U//FOUO)

- (U//FOUO)

- (U//FOUO)

(U//FOUO)

5.5.4. (U//LES)

5.5.4.1. (U//LES)

(U//LES)

(U//LES)

b7E

(U//LES) Example:

(U//LES) Example:

UNCLASSIFIED//~~LES~~
Domestic Investigations and Operations Guide

b7E

(U//~~LES~~)

(U//~~LES~~)

The employee should consult with his or her CDC or OGC for additional guidance.

5.5.4.2. (U//~~LES~~)

(U//~~LES~~)

b7E

(U//~~LES~~)

5.5.4.3. (U//~~LES~~)

(U//~~LES~~)

b7E

(U//~~LES~~) Note

(U//~~LES~~)

1. (U//~~LES~~)

2. (U//~~LES~~)

UNCLASSIFIED//~~LES~~
Domestic Investigations and Operations Guide

(U//~~LES~~)

b7E

(U//~~LES~~) **Approval:** (U//~~LES~~) Prior approval to use this method must be obtained from

[Redacted]

[Redacted] For

criminal cases [Redacted] For

national security cases [Redacted]

[Redacted]

(U//~~LES~~) **Emergency**

[Redacted]

[Redacted]

(U//~~LES~~)

[Redacted]

[Redacted]

5.6. (U//~~LES~~)

[Redacted]

b7E

(U//~~LES~~)

[Redacted]

[Redacted]

(U//~~LES~~) **Example**

[Redacted]

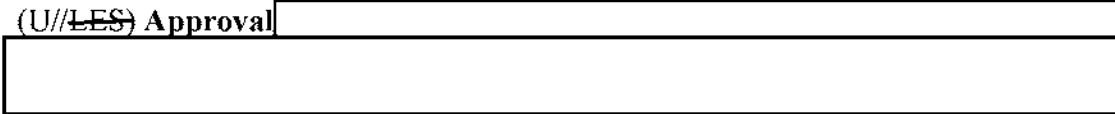
[Redacted]

UNCLASSIFIED//~~LES~~
Domestic Investigations and Operations Guide



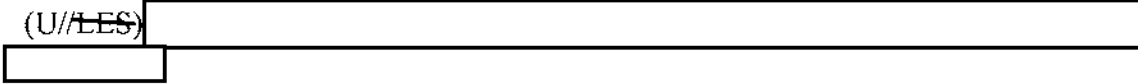
b7E

(U//~~LES~~) Approval



b7E

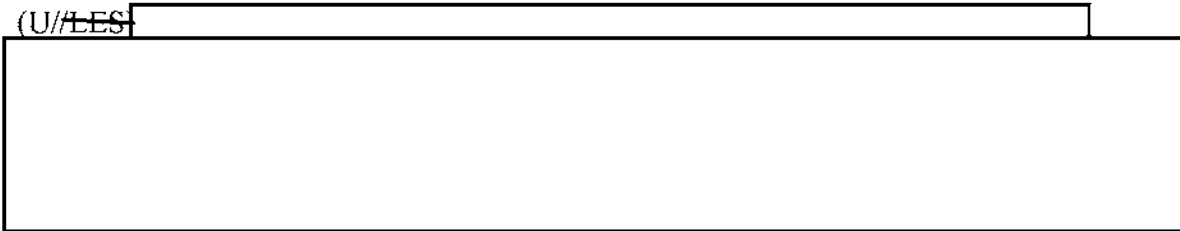
(U//~~LES~~)



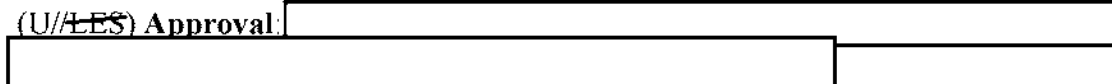
(U//~~LES~~)



(U//~~LES~~)



(U//~~LES~~) Approval



6. (U//~~LES~~) Online Activity Leading to Undisclosed Participation

(U//~~LES~~) UCEs and OCEs engaging in online communications need to be aware of circumstances amounting to UDP. UDP takes place when anyone acting on behalf of the FBI, including a UCE, an OCE, or a CHS, becomes a member of or participates in the activity of a legitimate organization on behalf of the United States government (USG) without disclosing FBI affiliation to an appropriate official of the organization. (See DIOG Section 16 for further discussion on UDP). All employees must understand and be aware of UDP concerns in their online investigations.

(U//~~FOUO~~) Note

- (U//~~FOUO~~)

- (U//~~FOUO~~)

- (U//~~FOUO~~)

- (U//~~FOUO~~)

(U//~~LES~~) Note

(U//~~LES~~) Note

b7E

UNCLASSIFIED//~~LES~~
Domestic Investigations and Operations Guide

(U//~~LES~~) Note: [Redacted]

b7E

[Redacted]

(U//~~LES~~) [Redacted]

[Redacted]

(U//~~LES~~) Example: [Redacted]

[Redacted]

7. (U//~~LES~~) Extraterritorial Online Activity

7.1. (U//~~LES~~) Overview

(U//~~LES~~) This section has limited application to criminal investigations. For all other investigative activity, applicable ET guidance should be sought from DIOG Section 13 (“Extraterritorial Operations”) [REDACTED]. Additionally, DIOG Appendix G [SECRET//NOFORN document] and the [REDACTED] [REDACTED] should be consulted for activities involving the use of technology outside the United States.

b7E

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

1. (U//~~LES~~) [REDACTED]
2. (U//~~LES~~) [REDACTED]
[REDACTED]
3. (U//~~LES~~) [REDACTED]
[REDACTED]
4. (U//~~LES~~) [REDACTED]
[REDACTED]
5. (U//~~LES~~) [REDACTED]
[REDACTED]
6. (U//~~LES~~) [REDACTED]
[REDACTED]

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

b7E

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

(U//~~LES~~) Note: [REDACTED]
[REDACTED]

UNCLASSIFIED//~~LES~~
Domestic Investigations and Operations Guide

b7E

(U//~~LES~~)

(U//~~LES~~) Approval:

(U//~~LES~~) Guidance on ET issues and questions should be sought from

7.2. (U//~~LES~~)

(U//~~LES~~)

b7E

(U//~~LES~~)

(U//~~LES~~) Note:

7.3. (U//~~LES~~)

(U//~~LES~~)

UNCLASSIFIED//~~LES~~
Domestic Investigations and Operations Guide

(U//~~LES~~)

b7E

(U//~~LES~~)

(U//~~LES~~) Note

7.4. (U//~~LES~~)

b7E

(U//~~LES~~)

(U//~~LES~~) Approval

(U//~~LES~~) Note

UNCLASSIFIED//~~LES~~
Domestic Investigations and Operations Guide

7.5. (U//~~LES~~) [Redacted]
[Redacted]

b7E

(U//~~LES~~) [Redacted]
[Redacted]

(U//~~LES~~) [Redacted]
[Redacted]

(U//~~LES~~) Note: [Redacted]
[Redacted]

7.6. (U//~~LES~~) [Redacted]
[Redacted]

(U//~~LES~~) [Redacted]
[Redacted]

(U//~~LES~~) Note: [Redacted]
[Redacted]

b7E

(U//~~LES~~) [Redacted]
[Redacted]

(U//~~LES~~) [Redacted]
[Redacted]

(U//~~LES~~) Note: [Redacted]
[Redacted]

UNCLASSIFIED//~~LES~~
Domestic Investigations and Operations Guide

b7E

(U//~~LES~~) As stated in subsection 7.1 of this appendix, this requirement does not apply to national security investigations.

8. (U) DIOG Appendix L -Quick Reference Guide (QRG)

DIOG Appendix L, Investigations Conducted Online by an FBI Employee QRG

9. (U) Key Terms and Definitions

(U) [REDACTED]

b7E

(U) **Employee:** Employee, as used in this appendix, is intended to be inclusive of FBI SAs, intelligence analysts (IA), OCEs, UCEs, and any other FBI employee engaged in activities authorized by the AGG-Dom and the DIOG, as well as any task force personnel, assignees, or detailees to the FBI who are expected to follow FBI operational policies when working on behalf of the FBI, as delineated by the cooperative agreement, memorandum, or other contract under which they are operating.

(U) [REDACTED]

(U) **Online covert employee:** a trained and certified employee of the FBI or a sworn law enforcement officer of a federal, state, or local law enforcement agency, working under the direction and control of the FBI, whose identity as an employee of the FBI or another law enforcement agency is concealed from third parties (subjects or persons of investigative interest) with whom the OCE is engaged in substantive online interactions and communications, usually in the context of a UCO. [REDACTED]

b7E

(U) [REDACTED]

(U) **Publicly available information:** information that has been published or broadcast for public consumption, is available on request to the public, is available to the public by subscription or purchase, is made available at a meeting open to the public, or is obtained by visiting any place or attending any event that is open to the public. For a further discussion regarding online publicly available information, see DIOG 18.5.1.

(U) **Real-time communication:** A key factor to determining if an exchange is occurring in real time is whether the exchange is preserved and made available later on the site to viewers. Forums where the communications are preserved for future viewers are generally not real time. Typically, a blog or bulletin board system preserves posted comments to enable future viewers to see the information, meaning that communications posted on these forums are not real time. Further, even when several contributors to a bulletin board site are using it to rapidly engage in an exchange, it is not a real-time

UNCLASSIFIED//~~LES~~
Domestic Investigations and Operations Guide

forum, as the content enjoys some degree of permanency even though the information may only be posted online for as little as a week. In contrast, a typical chat room is designed to allow only users currently in the room to view the exchange and does not preserve the exchange for those entering the room at a later point in time. Examples of real-time communications include most chat rooms, instant messaging, and Skype. These modes of communication are still considered real-time even if they are stored and accessible at a later date, because obtaining that information at a later date would require legal process. If the information remains on the online environment, and legal process is not required to obtain the contents, is it not considered real-time communications.

(U)

b7E

(U//~~LES~~) DIOG Appendix L: Online Investigations Quick Reference Guide

This QRG is for reference only and is not a substitute for official policy. For the most updated policies, see [Appendix L of the DIOG](#).

Investigative Authority	Online Activity	
Authorized Activities Conducted Online Prior to Opening an Assessment	• Access public information (DIOG 5.1.1.1) • Access publicly available information on the Internet [redacted] • Access public chat rooms [redacted] • Obtain identifying information about users or networks • Access and search information restricted to law enforcement • [redacted] • [redacted]	b7E
Authorized Investigative Methods Conducted Online: Assessments	Everything above AND: • Access publicly available information (DIOG 18.5.1) [redacted] • [redacted] • [redacted] • [redacted] • Task a CHS or a consenting party to access a private or restricted forum or Web site when (DIOG 18.5.5.): - o Access must be authorized (i.e., consent to access) - o Consensual recording of a restricted site's communications is prohibited in an Assessment • Monitor public, real-time communications and private, real-time communications during open Assessments • Electronic recording is only permitted for public, real-time communications and when an employee or a consenting party (e.g., CHS) is present	b7E
Authorized Investigative Methods Conducted Online: Predicated Investigations	Everything above AND: • Conduct consensual recordings of communications (DIOG 18.6.1) • Monitor private, real-time, online communications • Intercept the communications of a computer trespasser (DIOG 18.6.2) • Conduct undercover activity (UCA) (DIOG 18.6.13.3) • Conduct undercover operations (DIOG 18.6.13.3) • [redacted]	b7E

M APPENDIX M: (U) THE FAIR CREDIT REPORTING ACT (FCRA)

(U) (*Note:* The policy for The Fair Credit Reporting Act was not completed by the time of the DIOG publication. It will be linked in the DIOG once approved.)

This Page is Intentionally Blank.

N APPENDIX N: (U) FEDERAL TAXPAYER INFORMATION (FTI)

N.1 (U) SUMMARY

(U//~~FOUO~~) During the course of criminal investigations, the Federal Bureau of Investigation (FBI) often requests taxpayer records from the Internal Revenue Service (IRS) via *ex parte* orders. The Internal Revenue Code (IRC) reinforces the confidentiality of the relationship between the taxpayer and the IRS by making it a crime to violate that confidence. The sanctions of the IRC are designed to protect the privacy of taxpayers. Information obtained by the FBI directly from the IRS must be protected in accordance with the provisions of the IRC and IRS Publication 1075.¹⁰¹ This appendix provides guidance on the proper procedures for obtaining, handling, and protecting the federal taxpayer information (FTI) received by the FBI directly from the IRS. As a condition of receiving FTI, the FBI is statutorily obligated to properly protect the information in accordance with the safeguarding provisions established under Title 26 United States Code (U.S.C.) Section (§) 6103(p)(4), the “Internal Revenue Code” (IRC hereafter referred to as “Code”). All FBI personnel who handle FTI must be familiar with these procedures and requirements. FBI personnel includes all FBI employees, applicants, contractors, consultants, interns, task force personnel, and other government agency (OGA) personnel detailed to the FBI in the course of their assigned duties.

(U//~~FOUO~~) The Code permits the IRS¹⁰² to disclose tax returns and return information to certain federal, state, and local agencies, but only to the extent that such disclosure is specifically authorized within § 6103 of the Code. It is the responsibility of FBI personnel who handle FTI to comply with all requirements of 26 U.S.C. § 6103. All agencies receiving such information are prohibited from unlawfully disclosing such information. The IRS commonly refers to this category of information as “Federal Taxpayer Information” or “FTI.”¹⁰³ Agencies are statutorily obligated to properly protect this information in accordance with the safeguarding provisions established under 26 U.S.C. § 6103(p)(4). The information may only be accessible to persons whose duties or responsibilities require access and to whom disclosure is available under the statute. The FBI is required to establish a system of records relating to each request and receipt of information, as well as a secure area for storage with restricted access to that area and the information stored there. Once the information is no longer needed, the IRS requires that the FTI be disposed of in accordance with the Code’s requirements.¹⁰⁴

(U//~~FOUO~~) Many FBI investigations involve “joint task forces” and may include the cooperation of state and local law enforcement authorities. Section 6103(i) of the Code does not authorize disclosure of tax information to nonfederal investigators, even if they are formally assigned to a federal task force, unless they qualify as federal employees. State and local task force officers who are deputized qualify as federal employees.

¹⁰¹ (U) *Tax Information Security Guidelines for Federal, State and Local Agencies and Entities* (August 24, 2010) (IRS Pub. 1075).

¹⁰² (U) Specifically, the statute refers to the Secretary of the United States Department of the Treasury; however, throughout this document, all references to the IRS mean the Secretary of the Treasury.

¹⁰³ (U) See § 1.1 of IRS Pub. 1075.

¹⁰⁴ (U) *Id.* at § 8. Disposal of Federal Tax Information. See also 26 U.S.C. § 6103(p)(4)(F).

(U//~~FOUO~~) The FBI can only accept FTI from the IRS or another agency when it is disclosed in accordance with an authority provided under the statute for disclosure of FTI. FTI can be received and used by several units within the FBI for the same case and purpose; however, safeguarding responsibilities must be centralized with consistent standards.

(U//~~FOUO~~) Any agency that receives FTI for an authorized use may not use that information in any manner or for any purpose not consistent with the authorized use.¹⁰⁵ If the FBI requires FTI for a different authorized use under the Code, a separate request must be made. An unauthorized secondary use of information is specifically prohibited and may result in discontinuation of disclosures by the IRS and the imposition of civil and or criminal penalties on the responsible official.

N.2 (U) APPLICATION

(U//~~FOUO~~) FTI may be acquired from the IRS during a predicated investigation for use in any judicial or administrative proceeding pertaining to the enforcement of a federal criminal statute other than tax administration to which the United States or the FBI is a party.¹⁰⁶

(U//~~FOUO~~) Tax information acquired directly from the IRS is considered FTI and is protected under the IRC's confidentiality protections. [REDACTED]

b7E

N.3 (U) DEFINITIONS

N.3.1 (U) FEDERAL TAX INFORMATION

(U//~~FOUO~~) Information that is protected under the confidentiality provisions of 26 U.S.C. § 6103 is referred to as FTI and includes all information relating to the taxpayer that is received by the Department of the Treasury (hereinafter referred to as "IRS"). It specifically includes information obtained by the IRS from third parties, including informants [confidential human sources]; information derived from those third-party submissions; and the work product of the IRS in determining, assessing, and collecting taxes or investigating taxpayer criminality.

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

b7E

[REDACTED] The IRS guidelines for confidentiality protection apply specifically to information that agencies receive directly from the IRS.

N.3.2 (U) RETURN

(U//~~FOUO~~) As defined in 26 U.S.C. § 6103(b)(1), "The term 'return' means any tax or information return, declaration of estimated tax, or claim for refund" filed with the IRS and any amendments such as "supporting tax schedules, attachments, or lists which are supplemental to, or part of, the return so filed."

N.3.3 (U) RETURN INFORMATION

(U//~~FOUO~~) Return information is defined as any information (other than the return filed by the taxpayer) that is filed with the IRS by sources other than the taxpayer [REDACTED]

b7E

¹⁰⁵ (U) IRS Publication 1075, § 2.2 ("Need and Use").

¹⁰⁶ (U) 26 U.S.C. § 6103(i)(A).

[REDACTED]
These documents become part of the individual's file and are maintained by the IRS for tax purposes.

N.3.4 **(U//~~FOUO~~) TAXPAYER RETURN INFORMATION**

(U//~~FOUO~~) Taxpayer return information is information filed with, or furnished to, the IRS by, or on behalf of, a taxpayer.¹⁰⁷ (See N.3.3. above.) [REDACTED]

[REDACTED]
(U//~~FOUO~~) "The term 'taxpayer return information' means return information as defined in paragraph (2) which is filed with, or furnished to, the Secretary by or on behalf of the taxpayer to whom such return information relates." (26 U.S.C. § 6103 (b)(3))

N.3.5 **(U//~~FOUO~~) RETURN INFORMATION (INFORMATION RETURNS) OTHER THAN TAXPAYER RETURN INFORMATION (OTRI)**

(U//~~FOUO~~) OTRI includes return information that was NOT provided to the IRS by, or on behalf of, a taxpayer. It includes information obtained from third parties who are not representatives of the taxpayer and extends to the following types of information:

1. The books and records of a named taxpayer supplied to the IRS by a third party
2. The portion of an interview between the IRS agent and a third party discussing a named taxpayer
3. Information developed by IRS agents in the course of investigating a named taxpayer's return from sources other than a taxpayer's representative acting on behalf of the taxpayer
4. The fact that a named taxpayer filed or failed to file a return

N.3.6 **(U) DERIVATIVE TAX INFORMATION**

(U//~~FOUO~~) Any information taken from records obtained directly from the IRS retains its original classification as FTI. [REDACTED]
[REDACTED]

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

¹⁰⁷ (U) See 26 U.S.C. § 6103(b)(3).

N.4 (U) DEPARTMENT OF JUSTICE (DOJ) REQUIREMENTS FOR OBTAINING AND SAFEGUARDING FTI¹⁰⁸

(U//~~FOUO~~) In order to receive tax information from the IRS, 26 U.S.C. § 6013 requires that the DOJ establish and maintain the following, to the satisfaction of the IRS:

1. (U//~~FOUO~~) A permanent system of records, with respect to any requests and any disclosures of tax information.
2. (U//~~FOUO~~) A secure area or place where the information will be stored.
3. (U//~~FOUO~~) Restricted access to the information by those individuals whose duties and responsibilities require such access and to whom disclosure may be made under the provisions in the Code.
4. (U//~~FOUO~~) Any other safeguards that the IRS determines to be necessary to protect the confidentiality of the information.
5. (U//~~FOUO~~) A report must be furnished to the IRS, containing information describing the procedures established and utilized for ensuring the confidentiality of tax information, as required by the IRS.

N.5 (U) DISCLOSURE TO FEDERAL OFFICERS OR EMPLOYEES FOR ADMINISTRATION OF FEDERAL LAWS NOT RELATING TO FEDERAL TAX ADMINISTRATION

N.5.1 (U) LEGAL PROCESS FOR OBTAINING FTI IN FBI INVESTIGATIONS

(U//~~FOUO~~) The IRS may disclose return and return information to federal officers or employees for use in criminal investigations unrelated to tax administration. FTI may be obtained from the IRS via *ex parte* order or written request from the head of the agency, either the Director of the FBI or a United States attorney (USA), for purposes of FBI investigations. It **cannot** be obtained from the IRS via grand jury subpoena or administrative subpoena. In certain circumstances, the IRS may elect to voluntarily provide the FBI with FTI in order to report possible violations of criminal law or in an emergency situation within the FBI's jurisdiction.

N.5.1.1 (U) EX PARTE ORDERS (26 U.S.C. § 6103(i)(1))

(U//~~FOUO~~) An application for an *ex parte* order may be submitted by the Attorney General, the Deputy Attorney General, the Associate Attorney General, any Assistant Attorney General, any USA, a special prosecutor appointed under 28 U.S.C. § 593, or any attorney in charge of a criminal division organized crime strike force (28 U.S.C. § 593). Prior to submitting an application for an *ex parte* order, the responsible official should notify the appropriate IRS district director that such an action is being planned.¹⁰⁹ The notice should include all relevant details so that the IRS can assemble the requested information and make

¹⁰⁸ (U) See DOJ Order 2620.5A, *Safeguarding Tax Returns and Tax Return Information* (February 23, 1981).

¹⁰⁹ (U) This responsibility would most likely rest with the United States Attorney's Office (USAO) prosecuting the case.

an appropriate determination, taking into consideration whether the disclosure would impair any civil or criminal tax investigation or reveal the identity of a confidential informant.

(U//~~FOUO~~) An *ex parte* disclosure will be granted by the court to provide information to all personnel who are personally and directly engaged in the preparation of any judicial or administrative proceeding pertaining to the enforcement of federal criminal statutes unrelated to tax administration; any investigation that may result in such a proceeding; or any federal grand jury proceeding pertaining to enforcement of criminal statutes. The information may only be used by those officers and employees.

(U//~~FOUO~~) The assistant United States attorney (AUSA) working with the FBI will prepare the order for the signature of the USA. A judge or magistrate may grant such an application for an order if there is a finding based upon the facts submitted that there is reasonable cause to believe that:¹¹⁰

1. (U//~~FOUO~~) A specific crime has been committed.
2. (U//~~FOUO~~) The return or return information is or may be relevant to a matter relating to the commission of that crime.
3. (U//~~FOUO~~) The information is sought exclusively for use in a federal investigation, and the information cannot reasonably be obtained from another source.

(U//~~FOUO~~) Language in the application and order should track the statutory language as closely as possible, listing every statutory violation for which “reasonable cause” exists to request these records. [REDACTED]

b7E

(U//~~FOUO~~) Tax return information received pursuant to an *ex parte* order is limited for use solely for the incident, threat, or activity described in the application to the court.¹¹¹ FTI obtained via *ex parte* order may only be used by the employees working on the investigation(s) described in the *ex parte* application. The information cannot be shared among case files or among FBI squads investigating separate cases. A separate *ex parte* order must be obtained if the FTI is needed for a different investigation not described in the original *ex parte* application. Due to the sensitivity of tax information and the penalties that attach to the unauthorized inspection and dissemination of this information, FBI employees should consult with their chief division counsels (CDC) and the Office of the General Counsel (OGC), as needed, prior to requesting an *ex parte* order from an AUSA.

N.5.1.2 (U) WRITTEN REQUEST (LETTERHEAD)

(U//~~FOUO~~) A letterhead request may be made to the IRS by the Director of the FBI to obtain information “other than taxpayer return information.”¹¹² The IRS may disclose this information to the Director of the FBI, in writing, if the information may constitute evidence of a violation of any federal criminal law within the investigative jurisdiction of the FBI. The request must be made in writing to the appropriate IRS district director by the Director of the FBI (see 26 U.S.C. § 6103(i)(1)). The request must be for the intended use and must set forth the taxpayer’s name and address, the taxable periods for which the information is sought, the

¹¹⁰ (U) 26 U.S.C. § 6103(i)(1)(B).

¹¹¹ (U//~~FOUO~~) This information is available in a Preliminary or Full Investigation.

¹¹² (U) 26 U.S.C. § 6103(i)(2)(A).

statutory authority under which the enforcement proceeding is being conducted, and the specific reason(s) why the information sought is relevant to the enforcement proceeding, and it must indicate that the agency is directly engaged in preparing for a judicial or administrative proceeding, an investigation which may result in such a proceeding, or a grand jury proceeding (see 26 U.S.C. § 6103(i)(1)(A)(iii)). The Secretary of the Treasury shall disclose this information to officers and employees of the FBI who are personally and directly engaged in the investigation solely for their use as needed to enforce such law.

(U//~~FOUO~~) This information is limited to the taxpayer's name, address, and SSN; whether a tax return has or has not been filed within the last three years; or the name and address of any individual who filed from a particular address for a requested period of time. If the information may constitute evidence of a violation by any taxpayer of any federal criminal law unrelated to tax administration, then the taxpayer's identity may also be disclosed (26 U.S.C. § 6103(i)(3)).

**N.5.1.3 (U) DISCLOSURE OF RETURN INFORMATION BY THE IRS
RELATED TO CRIMINAL, TERRORIST ACTIVITIES OR
EMERGENCY CIRCUMSTANCES (26 U.S.C. § 6103(i)(3))**

N.5.1.3.1 (U) POSSIBLE VIOLATIONS OF FEDERAL CRIMINAL LAW

(U//~~FOUO~~) Generally, the IRS may voluntarily disclose in writing, without a request, return information (OTRI) that may constitute evidence of a violation of any federal criminal law that does not involve tax administration in order to notify the head of the federal agency responsible for enforcement of that violation. If there is return information other than OTRI that may constitute evidence of such a crime, the taxpayer's identity may also be disclosed under that provision. Upon receipt of this information, the Director of the FBI may disclose the information to the officers and employees who are working or will be assigned to the investigation.

N.5.1.3.2 (U) EMERGENCY CIRCUMSTANCES¹¹³

(U//~~FOUO~~) In circumstances where there is an imminent danger of death or physical injury to any individual, the IRS may voluntarily disclose return information to the extent necessary to apprise appropriate officers or employees of a federal or state law enforcement agency.

(U//~~FOUO~~) In situations involving fugitives (flight from federal prosecution) a voluntary disclosure of return information may be made by the IRS to apprise the appropriate law enforcement agency.

**N.5.1.3.3 (U) DISCLOSURE BY THE IRS OF INFORMATION RELATING TO
TERRORIST ACTIVITIES (26 U.S.C. § 6103(i)(3)(C))**

(U//~~FOUO~~)

b7E

¹¹³ (U) 26 U.S.C. § 6103(i)(3)(C).

N.5.2 (U) **TERRORISM INVESTIGATIONS**

N.5.2.1 (U) **FBI APPROVAL REQUIREMENTS FOR OBTAINING FTI VIA AN
EX PARTE ORDER IN TERRORISM CASES**

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

b7E

[REDACTED]

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

[REDACTED]

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

b7E

[REDACTED]

[REDACTED]

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

[REDACTED]

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

[REDACTED]

b7E

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

[REDACTED]

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

[REDACTED]

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

N.5.2.2 (U) WRITTEN REQUEST RELATED TO TERRORIST ACTIVITIES

(U//~~FOUO~~)

b7E

(U//~~FOUO~~)

- (U)
- (U)
- (U)
- (U)
- (U)
- (U)
- (U)
- (U)
- (U)
- (U)

b7E

(U//~~FOUO~~)

¹¹⁴ (U) 26 U.S.C. § 6103(i)(7)(A).

¹¹⁵ (U//~~FOUO~~) Case ID

b7E

N.5.3 ***(U) BACKGROUND INVESTIGATION REQUESTS***

(U//~~FOUO~~) The IRS may disclose the return of any taxpayer, or return information with respect to such taxpayer, to such individuals as the taxpayer may designate in a request for, or consent to, disclosure for the purposes of background investigations for employment.

(U//~~FOUO~~) In addition, § 6103(g)(1) and (2) discuss disclosure to the President and certain other persons provided for in the statute. It provides for disclosure of return information to Presidential appointees and certain other federal government appointees. Upon written request of the President or the head of any federal agency, the IRS may disclose to an authorized representative of the Executive Office of the President, federal agency head, or the FBI, return information with respect to an individual under consideration for an appointment to a position in the executive or judicial branch of the federal government. The information shall be limited to whether the individual has filed returns for the preceding three years; has failed to pay any tax within ten days after notice and demand; has been assessed a penalty in the current year or preceding three years; has been under investigation for possible criminal offenses under the internal revenue laws and the results of such an investigation; or has been assessed any civil penalty under the internal revenue laws for fraud. Within three days of receipt of the request for this information, the Secretary of the Treasury shall notify the individual in writing that the information has been requested under the Code.

(U//~~FOUO~~) The employee who receives this information from the Secretary may not disclose such information to any other person except the President or the head of the federal agency without the written direction of the President or head of the federal agency.

N.5.4 ***(U) INFORMATION OBTAINED FROM STATE TAX ADMINISTRATION/AGENCY***

(U//~~FOUO~~) Information requested and obtained from state tax authorities is not considered FTI, and the requirements of Title 26 of the IRS Code do not apply to these types of records. However, each state may have specific requirements concerning the procedures for obtaining and maintaining these types of official records pertaining to their taxpayers. Many state tax returns are also protected by antidisclosure laws that are closely patterned after § 6103 of the Code. State returns may not be available through subpoenas, and the AUSA's access to them may not be covered by exceptions to the state disclosure laws. If the investigation demonstrates a need for these records, agents should consult with their CDC and local USAOs or state prosecutors to determine the appropriate methods for obtaining and safeguarding these records in compliance with state requirements.

N.5.5 ***(U) OTHER THAN FTI***

(U//~~FOUO~~) Tax information obtained directly from an individual or from that individual's tax preparer [REDACTED] is not covered by the statutory requirements set forth in the Code and does not require the same treatment as FTI.

b7E

N.6 (U) HANDLING, STORING, AND SAFEGUARDING FTI

(U//~~FOUO~~) The IRS requires that certain specific safeguards be employed by an agency for the protection of FTI.¹¹⁶ FTI must be protected from unauthorized disclosure to persons who do not possess the need to know. Access must be limited only to those individuals working on the specific case for which the FTI was requested, and the requested FTI may only be used for the specific reason that it was requested. If the FTI is to be used for a different purpose, a new request must be filed under a different provision of 26 U.S.C. § 6103.

(U//~~FOUO~~) The information must be protected using minimum protection standards, as defined in the Internal Revenue Code. This method establishes the minimum standards that will be applied on a case-by-case basis, considering local circumstances to determine space and containers for the basic framework of minimum security requirements [REDACTED]

b7E

[REDACTED]

(U//~~FOUO~~) All tax information must be maintained in accordance with the requirements of the *United States Attorney's Manual* (Sections 3-6.300), DOJ Order 2620.5A (February 23, 1981), and the memorandum from the Executive Office for United States Attorneys (EOUSA) Director, entitled "Maintenance of Tax Returns and Return Information" (August 23, 1996) [REDACTED]

[REDACTED]

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

b7E

N.6.1 (U) TRACKING FTI

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

[REDACTED]

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

¹¹⁶ (U) For more information, see *Tax Information Security Guidelines for Federal, State and Local Agencies* (August 24, 2010), IRS Publication 1075, available on the IRS website: www.irs.gov and on the Security Division Intranet site.

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

(U//~~FOUO~~) All original FTI received from the IRS, both electronic and hard copies, must be protected in accordance with the guidance referenced above. [REDACTED]

[REDACTED]

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

[REDACTED]

b7E

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

[REDACTED]

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

[REDACTED]

N.6.2 (U) *MARKING FTI*

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

[REDACTED]

N.6.3 (U) *HANDLING AND TRANSPORTING OF FTI*

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

[REDACTED]

b7E

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

[REDACTED]

N.7 (U) *REMOVABLE ELECTRONIC MEDIA*

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

[REDACTED]

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

[REDACTED]

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

[REDACTED]

b7E

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

[REDACTED]

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

[REDACTED]

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

[REDACTED]

N.8 (U) DISPOSAL OF MATERIAL UPON DISPOSITION OF CASE

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

b7E

[REDACTED]

(U) [REDACTED]

[REDACTED]

-
-
-

[REDACTED]

(U) [REDACTED]

b7E

(Note: [REDACTED]

[REDACTED]

N.8.1 (U) RETURN OF FTI

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

[REDACTED]

1. [REDACTED]

2. [REDACTED]

¹¹⁷ (U) See IRS Publication 1075, subsection 8.3.

3. [REDACTED]

(U) [REDACTED]

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

[REDACTED]

b7E

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

[REDACTED]

N.8.2 (U) *FINAL DISPOSITION OF FTI SERIALIZED INTO SENTINEL*

(U) Upon the closing of a case file, all records serialized utilizing the FTI caveat must be permanently charged out of Sentinel (Per current policy, only IMD has the authority to delete/permanently charge out a serialized record. Therefore, a permanent charge out (PCO) lead request must be sent to [REDACTED] See *Permanent Charge Out (Deletion) of Records From All Electronic Recordkeeping Systems Policy Directive, 0861D* for additional guidance) requesting that the serials identified be permanently charged out. Prior to submission of the PCO lead request, [REDACTED]

b7E

[REDACTED]

[REDACTED] These last steps must be accomplished to ensure the FBI is acting in accordance with National Archives and Records Administration (NARA) approved records disposition schedules established for investigative records/files.

N.9 (U) *TRAINING AND CERTIFICATION*

(U//~~FOUO~~) All FBI employees, detailees, and contractors who could potentially come in contact with FTI are required to complete annual training on the proper safeguarding of FTI.

(U//~~FOUO~~) Annually, each field office or division will certify, by EC to the SecD Strategy, Policy, and Information Security Unit that all appropriate individuals have completed the FTI training on Virtual Academy.

(U//~~FOUO~~) The training provided before the initial certification, and annually thereafter, must also cover the incident response policy and procedures for reporting unauthorized disclosures and data breaches.

¹¹⁸ (U) See Publication 1075, subsection 8.4.

This Page is Intentionally Blank.

O APPENDIX O: (U) RIGHT TO FINANCIAL PRIVACY ACT (RFPA)

O.1 (U) SUMMARY

(U//~~FOUO~~) The Right to Financial Privacy Act (RFPA), Title 12 United States Code (U.S.C.) Section (§) 3401, et seq., prohibits financial institutions from providing financial records to the government, unless access is authorized by one of the exceptions or methods that is outlined below. The RFPA applies when the government is seeking the “financial records” of a “customer” of a “financial institution.” The RFPA only applies if all three elements are met (e.g., the FBI is obtaining customer financial account records from a bank).

(U//~~FOUO~~) This appendix outlines the general responsibilities of FBI personnel to comply with the statutory requirements of the RFPA when seeking to obtain financial records from financial institutions defined under the statute.

O.2 (U) DEFINITIONS

O.2.1 (U) FINANCIAL INSTITUTION (12 U.S.C. § 3401(1))

(U//~~FOUO~~) The definition focuses on offices of institutions “located in any State or territory of the United States, the District of Columbia, Puerto Rico, Guam, American Samoa, or the Virgin Islands.” This includes all banking and banking-type institutions, as well as consumer finance companies, and companies that issue credit cards, even though such companies are often not banking-type institutions. The RFPA does not apply to records maintained by a bank in a foreign jurisdiction or a U.S. financial institution’s office located in a foreign jurisdiction. The RFPA also does not apply to bonding companies, credit bureaus, brokerage houses, government lending agencies, small business investment companies, the United States Postal Service, and money-service businesses such as Western Union.

O.2.2 (U) FINANCIAL RECORDS

(U//~~FOUO~~) A “financial record” is any original, copy of, or information “knowingly derived from” a record pertaining to a present or past customer’s relationship with a financial institution. Excluded from the RFPA are records or information not identifiable with a particular customer (12 U.S.C. § 3413(a)) or those records that reside in the account of a third party, such as a check endorsed and deposited into a third-party account or items drawn to an individual, then deposited by the individual into the account of a corporation if the item was obtained from the corporation’s financial records. It also excludes forged or counterfeit financial instruments and records relating to fictitious account names.

(U//~~FOUO~~) Requests for basic account information are also excluded from the RFPA’s protection (12 U.S.C. § 3413(g)), as are records relating to bank surveillance photographs; contents of a safe deposit box sought pursuant to a search warrant; or records pertaining to functions that do not involve an account relationship, such as the sale of stocks and other activities that do not constitute routine bank services. If the records are obtained by a formal written request, obtaining the basic account information requires the use of *Department of Justice (DOJ) Form 475*, which has a Certificate of Compliance incorporated into it. If a

subpoena or other process is used to obtain this basic account information, then the subpoena or other process is required, along with DOJ Form 461 ("Certificate of Compliance with the Right to Financial Privacy Act of 1978").

(U) Under most circumstances, financial information relating to the accounts of individuals and partnerships of five or fewer individuals is protected under the RFPA (12 U.S.C. § 3401(2)).

0.2.3 (U) CUSTOMERS COVERED (12 U.S.C. § 3401(5))

(U//~~FOUO~~) To be considered a "customer" under the RFPA, the entity must meet the definition of a "person" under the statute. A "person" is defined as any natural person or partnership of five or fewer individuals (12 U.S.C. § 3401(4)) and includes any person for whom the financial institution is acting or has acted as a fiduciary in relation to an account maintained in the person's name at the institution. Corporations, associations, larger partnerships, pension funds, special interest nonprofit organizations, trusts, or other legal entities are not covered by the RFPA.

0.2.4 (U) GOVERNMENT AUTHORITY

(U//~~FOUO~~) The RFPA applies to all federal agencies, including the FBI or any officer, employee, or agent thereof, including TFOs.

0.2.5 (U) LAW ENFORCEMENT INQUIRY

(U) Any lawful investigation or official proceeding inquiring into a violation of, or a failure to comply with, any criminal or civil statute, regulation, rule, or order issued thereunder, is considered a law enforcement inquiry.

0.3 (U) METHODS FOR OBTAINING RECORDS

(U) Only the methods listed below may be used under the RFPA to obtain information from a financial institution.

0.3.1 (U) WRITTEN REQUEST

(U//~~FOUO~~) The FBI is authorized by Title 28 Code of Federal Regulations (CFR) § 47.3 to request financial records of any customer from a financial institution pursuant to a formal, written request (see 12 U.S.C. § 3408).

(U//~~FOUO~~) The FBI may request these records from the financial institutions; however, this method of access requires the cooperation of the financial institution, as well as notification (i.e., disclosure of the request using DOJ Form 464, "Customer Notice") to the customer, unless a delay of notice order (DOJ Form 468, "Order") is obtained.

(U//~~FOUO~~) The written request (DOJ Form 463, "Formal Written Request for Financial Records") must state the purpose of the investigation, without reference to the specific title and section of the U.S.C. Generic terms, such as fraud, bribery, extortion, and the like, may be used to describe the offense, similar to the character descriptions of cases the FBI now uses. If no delay of notice order is obtained, the customer notice provision within the request must state the name and business address of the FBI supervisory official to be served with copies of customer challenge papers, should the customer decide to challenge the production of records written

request. [REDACTED]

b7E

O.3.1.1 (U) FORMS REQUIRED FOR A WRITTEN REQUEST

(U) The following forms may be required when requesting a customer's financial records from a financial institution pursuant to a formal written request:

- (a) (U) DOJ Form 461, "Certificate of Compliance with the Right to Financial Privacy Act of 1978"
- (b) (U) DOJ Form 463, "Formal Written Request for Financial Records"
- (c) (U) DOJ Form 464, "Customer Notice"
- (d) (U) DOJ Form 465, "Motion for Order Pursuant to Customer Challenge Provisions of the Right to Financial Privacy Act of 1978"
- (e) (U) DOJ Form 466, "Sworn Statement of Movant"

O.3.2 (U) JUDICIAL SUBPOENA

(U//~~FOUO~~) A judicial subpoena is any court order to produce records other than a grand jury subpoena—the most common of which is the trial subpoena directed at a party not involved in litigation. When used, a copy of the judicial subpoena, together with mandatory customer notice (i.e., DOJ Form 464, "Customer Notice"), is served or mailed to the customer. The notice provisions for the judicial subpoena are the same as for the written request above (12 U.S.C. § 3407).

O.3.3 (U) ADMINISTRATIVE SUBPOENA

(U//~~FOUO~~) The statutory requirements of the RFPA provide that a government authority may have access to, or obtain copies of, the information contained in the financial records of any customer of a financial institution when such records are disclosed in response to an administrative subpoena or a summons meeting the requirements of 12 U.S.C. § 3405. The FBI may use administrative subpoenas to obtain bank records in Title 21 (Controlled Substance), sexual exploitation or abuse of children investigations, and healthcare fraud investigations. (**Note:** Healthcare fraud administrative subpoenas are issued by the relevant United States Attorney's Office [USAO]). See DIOG subsection 18.6.4, "Investigative Method: Administrative Subpoenas." For guidance on the use of administrative subpoenas and associated financial privacy limitations, see DIOG subsection 18.6.4.3.4.

O.3.4 (U) GRAND JURY SUBPOENA

(U//~~FOUO~~) The RFPA does not require notification to the customer when records are requested using a grand jury subpoena. However, the RFPA still places restrictions on the handling and use of customer financial records obtained in this manner. The RFPA record-handling requirements are consistent with the treatment of federal grand jury documents [REDACTED]

b7E

[REDACTED]

(U) Financial records of a customer that were obtained from a financial institution by use of grand jury subpoena should be treated in accordance with guidance from the relevant USAO or DOJ component and marked as “Subject to RFPA.” (See relevant DIOG subsection in 18.6.5, “Marking, Physical Storage, and Mailing of Grand Jury Material.”)

(U//~~FOUO~~) Financial records (as defined by RFPA) obtained with a grand jury subpoena (see 12 U.S.C. § 3420) must be returned and actually presented to the grand jury unless the volume of such records makes it impractical. In that situation, the grand jury must be provided with a description of the content of the records. The records may only be used (1) for the purpose of considering whether to issue an indictment or presentment by that grand jury, (2) for prosecuting a crime for which the indictment or presentment has been issued, (3) for a purpose authorized by Rule 6(e) of the Federal Rules of Criminal Procedure (FRCP), or (4) for a purpose authorized under § 3412 of the RFPA.

(U//~~FOUO~~) Records obtained under the RFPA via a grand jury subpoena must be destroyed or returned to the financial institution if not used for one of the purposes noted above, unless such records have been used in the prosecution of a crime for which the grand jury issued an indictment or a presentment or for a purpose authorized by Rule 6(e) of the FRCP (see 12 U.S.C. § 3420). If the records have been used in the prosecution, then the records—or a description of them—may only be maintained by a government authority if they are placed in the sealed records of the grand jury, unless such records have been introduced as evidence and thus disclosed publically in the criminal proceedings.

(U//~~FOUO~~) Given the differences in how federal judicial circuits define matters occurring before the grand jury under Rule 6(e), [REDACTED]

[REDACTED]

(U//~~FOUO~~) Although grand jury subpoenas are not subject to the certification of compliance, customer notice, or the civil liability provisions of the RFPA, they are subject to the FGJ reimbursement procedures established through the USAO.

0.3.5 (U) CRIMINAL SEARCH WARRANTS

(U//~~FOUO~~) A search warrant may be used to obtain a customer’s account-related records from a financial institution under the RFPA, with notice to the customer (DOJ Form 46-L, “Customer Notice”) of the search occurring within 90 days after execution. There are no changes in the procedures to obtain a search warrant [REDACTED]

0.3.6 (U) CUSTOMER AUTHORIZATION

(U) Customers may authorize access to identified records for up to 90 days by signing a revocable statement specifying the recipient, the purpose for disclosure, and an acknowledgement that he or she is aware of his or her rights under the RFPA. A customer-signed authorization (e.g., DOJ Form 462, "Voluntary Customer Authorization for Financial Records") is required when the records are obtained from the financial institution. This method of obtaining financial records typically applies in applicant-type investigations or when the financial records of a cooperative witness are being sought. The customer may revoke such authorization at any time before the records are disclosed.

0.3.7 (U) NATIONAL SECURITY LETTERS (NSL)

(U//~~FOUO~~) Financial institutions must comply with a request for a customer's or an entity's financial records made pursuant to 12 U.S.C. § 3414 by the FBI when the Director of the FBI certifies in writing, via an NSL, to the financial institution that such records are sought for

For additional information regarding NSLs, including nondisclosure requirements (i.e., notification to customer), see DIOG subsection 18.6.6.

0.3.8 (U) EMERGENCY ACCESS

(U//~~FOUO~~) A government authority may obtain financial records from a financial institution if the government authority determines that a delay in obtaining access to the records would create imminent danger of physical injury, serious property damage, or flight from prosecution. Access may be obtained immediately by merely presenting the financial institution with DOJ Form 461, "Certificate of Compliance with the Right to Financial Privacy Act of 1978," signed by a supervisory official as described below (see subsection O.7.1 of this appendix, "FBI Supervisory Personnel"). Within five days of obtaining access to the financial records, the government authority must file a signed, sworn statement of the supervisory official with the court, setting forth the grounds for the emergency access (12 U.S.C. § 3414(b) (3)).

(U//~~FOUO~~) Since notice is delayed under this provision, notification must subsequently be provided to the customer whose records were accessed (12 U.S.C. § 3409(c)).

(U//~~FOUO~~) Pursuant to Attorney General's Order 821-79, the Director has delegated this authority to include all supervisory officials, including those individuals serving as acting supervisory special agents and relief supervisors. (See the Delegation of Authority to sign

Certificate of Compliance and File a Sworn Affidavit with the Court Authorizing Emergency Access to Financial Records under the Right to Financial Privacy Act (RFPA))

O.3.9 (U) ACCESS TO FINANCIAL RECORDS FOR CERTAIN INTELLIGENCE AND PROTECTIVE PURPOSES

(U//~~FOUO~~) Nothing in the RFPA (except for 12 U.S.C. §§ 3415, 3417, 3418, and 3421) applies to the production and disclosure of financial records pursuant to a request from a government official authorized to [REDACTED]

b7E

[REDACTED]

(U) [REDACTED]

b7E

[REDACTED]

[REDACTED] This provision does not apply to those individuals for whom disclosure is necessary to comply with the government's request or to an attorney whom the financial institution may consult with to obtain legal advice or assistance with respect to that request.

O.4 (U) CUSTOMER NOTICE REQUIREMENTS AND PROCEDURES

(U//~~FOUO~~) Required notice (i.e., disclosure of the request, using *DOJ Form 464*) advises the customer that his or her records are being sought (e.g., by administrative subpoena) and the nature of the inquiry, which may include a statement to the effect that the customer is not a subject of the investigation. If customer notification is not delayed pursuant to a court order, a supervisory request, or a notice exception, the records sought do not have to be produced, and the customer has ten days, if notice is personally served, and 14 days, if notice is mailed, to complete and file an affidavit detailing why the records are not relevant to a legitimate law enforcement inquiry. The customer must then serve a copy of the affidavit on the government authority and be prepared to present additional facts in court. If the customer does not comply with the above within the prescribed time limits, the records may be made available by the financial institution. Any FBI supervisory official (defined in subsection O.7.1) may execute a written request for financial records. Pursuant to a written request, customer notice may be delayed for period of up to 90 days (see subsection O.4.1.1. below).

(U//~~FOUO~~) The request serves as notification of the nondisclosure requirement.

O.4.1 (U) EXCEPTIONS TO CUSTOMER NOTICE

(U//~~FOUO~~) Notwithstanding the restrictions on obtaining financial records, financial institutions are permitted to notify government authorities of possible violations of law reflected in their

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

records. In these situations, neither the financial institution nor the FBI is required to give any notice to the customer; however, the information provided may only include names or other identifying information concerning the individual or entity, the account involved, and the nature of the suspected illegal activity. The purpose of this exception under the RFPA is so that the government may use this information to obtain direct access to the customer's financial records through other legal means. In addition, there are no criminal penalties under the RFPA that prevent an institution from notifying its customer in the absence of a court order; however, recourse, such as obstruction of justice charges, may be available.

(U//~~FOUO~~) When basic account information is requested, it may be obtained under the RFPA without notice to the customer; however, a DOJ Form 461 "Certificate of Compliance with the Right to Financial Privacy Act of 1978" must be filed with the financial institution (12 U.S.C. § 3403(b)) prior to receipt of the records. This information is limited to the customer's name, address, account numbers, and types of accounts. It may subsequently be disclosed to other non-DOJ federal agencies without further notice to the customer but does require that an additional transfer certification be completed (DOJ Form 474) and delivered to that agency (12 U.S.C. § 3413(g)).

O.4.1.1 (U) DELAY OF NOTICE

(U//~~FOUO~~) Delays of customer notice (i.e., disclosure of the request, 12 U.S.C. § 3409) may be obtained for access to the records sought through the use of administrative subpoenas, judicial subpoenas, formal written requests, search warrants, NSLs, emergencies, and subsequent interagency transfers [REDACTED]

b7E

Delays of up to 90 days (or 180 days in the case of a search warrant) may be requested in the application to a court where there is a reason to believe (lesser standard than probable cause) that notice would cause (1) danger to life or physical safety, (2) flight from prosecution, (3) destruction of, or tampering with, evidence, (4) intimidation of a potential witness, (5) other serious jeopardy to an investigation or an official proceeding, or (6) undue delay to a trial or an ongoing official proceeding. To obtain a delay of notice, a sworn, written statement must be presented to a judge or magistrate that one or more of above situations exist. Extensions of the delay of notice may be similarly obtained based on necessity.

(U//~~FOUO~~) In addition to delaying the timing of the government notification to the customer, the court order issued should also prohibit the financial institution from disclosing to the customer that records pertaining to that customer are being sought. [REDACTED]

b7E

O.4.2 (U) CUSTOMER CHALLENGE

(U//~~FOUO~~) In instances where notice is not delayed, a customer may challenge a judicial subpoena or a formal written request. Grand jury subpoenas, being generally excepted by the RFPA and having no notice provisions, cannot be challenged at the time of access. NSLs are governed by nondisclosure procedures outlined in DIOG subsection 18.6.6.

(U//~~FOUO~~) Within 10 or 14 days, depending on the method of notice (served or mailed), the customer may file a motion to quash a judicial subpoena in U.S. district court or an application to enjoin the FBI from pursuing a formal, written request. Close coordination should be maintained

between the field office and the United States Attorney's Office (USAO) throughout the customer challenge process.

(U//~~FOUO~~) In support of the motion or application, the customer must file a sworn statement that he or she is the person whose records are being sought, and that he or she:

- (a) (U) Has reason to believe the records sought are not relevant to the inquiry.
- (b) (U) Believes that the RFPA has not been substantially complied with.
- (c) (U) Has another legal reason for denying access.

(U//~~FOUO~~) The challenge does not shift the burden of proof to the customer, but it does require more than a mere allegation. The FBI field office, in coordination with the relevant USAO, must then convince the judge or magistrate that the records sought are relevant to a legitimate law enforcement inquiry. Relevance means anything that might be used as evidence or that might logically lead to evidence. Denial of customer challenge motions or applications is not appealable until after the trial or other proceeding.

(U//~~FOUO~~) If the FBI and USAO fail to justify attempted access to these records, the subpoena will be quashed or the formal, written request enjoined. If the government justifies access, the subpoena will be enforced, and the formal written request may be pursued with the financial institution.

(U//~~FOUO~~) If, after obtaining court access to the information, the USAO determines that no legal proceeding will be contemplated against the customer, the USAO must promptly notify the customer of his or her status related to the investigation.

(U//~~FOUO~~) Any applicable statute of limitation is suspended during the time the customer's motion or application is pending in court.

(U//~~FOUO~~) In the case of judicial subpoenas, venue for the customer challenge is restricted to the court that issued the subpoena. When a formal, written request is used, the customer may challenge in any one of three districts:

- 1. (U) The District of Columbia
- 2. (U) The site of the financial institution
- 3. (U) The site of the residence of the customer

0.4.3 (U) CERTIFICATE OF COMPLIANCE (12 U.S. C. § 3403(B))

(U//~~FOUO~~) No financial institution or officer or employee or agent of a financial institution may release the financial records of any customer to any government authority until the government authority certifies to the institution, in writing, that it has complied with the applicable provisions of the RFPA (e.g., customer notice or delay order). The government authority must provide the financial institution with a DOJ Form 461 "Certificate of Compliance with the Right to

Financial Privacy Act of 1978” and, upon receipt of the certificate, the financial institution must provide the requested records to the government.

O.4.4 (U) RECEIPT OF RECORDS

(U//~~FOUO~~) Upon receipt of a request from a government authority, the financial institution must assemble the requested records and be prepared to deliver them once they receive the Certificate of Compliance under 12 U.S.C. § 3403(b) (see 12 U.S.C. § 3411).

O.5 (U) DISSEMINATION OF INFORMATION

O.5.1 (U) TO THE DEPARTMENT OF JUSTICE (DOJ)

(U//~~FOUO~~) Generally, the FBI may transfer records freely within the DOJ [REDACTED]

b7E

[REDACTED] Transfers between and among the components of the DOJ are not restricted by the RFPA, except during an investigation of a financial institution whenever customer records are obtained through that investigation and the customer had no notice or challenge opportunity. In those circumstances, the customer records obtained may not be used for a separate inquiry on the customer. However, enough information about the separate inquiry on the customer may be given to another component so that access may be sought independently.

O.5.2 (U) TO OTHER FEDERAL DEPARTMENTS (NON-DOJ)

(U//~~FOUO~~) Financial records obtained under the RFPA may be transferred to another federal agency under 12 U.S.C. § 3412 only if an official of the transferring agency certifies, in writing (*DOJ Form 474*) to the file, that “there is reason to believe that the records are relevant to a legitimate law enforcement inquiry of the receiving agency.” This may require a statement from the receiving agency. Within 14 days of the transfer, the customer must be notified of the transfer by the transferring agency unless the government has obtained, in connection with its original access or at the time of the transfer, a court order delaying that notice under the provisions of 12 U.S.C. § 3409.

O.5.3 (U) TRANSFERS TO STATE, LOCAL, AND FOREIGN GOVERNMENTS

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

b7E

[REDACTED] because they are not subject to the RFPA.

O.6. (U) MATTERS OUTSIDE THE SCOPE OF THE RFPA

O.6.1 (U) FINANCIAL INSTITUTIONS

(U//~~FOUO~~) The RFPA does not require customer notice when the institution in possession of such records is the subject of the investigation. Nonetheless, the Certificate of Compliance is necessary. Customer records obtained under this exception may only be used or transferred in furtherance of that specific investigation. If evidence of another violation is developed, enough

information (not records) may be given the appropriate agency, including the FBI, to identify the record and violation. Thereafter, the receiving agency may proceed as if independent of the initial inquiry.

O.6.2 (U) CORPORATIONS OR OTHER LEGAL ENTITIES

(U//~~FOUO~~) Investigations directed at corporations or other legal entities not protected by the RFPA may be conducted in same fashion as subsection O.6.1 above.

O.6.3 (U) NOT IDENTIFIABLE WITH CUSTOMER

(U//~~FOUO~~) A financial institution can disclose records if the information contained therein is not identified with, or identifiable as being derived from, the records of a particular customer.

O.6.4 (U) PARTIES IN INTEREST

(U//~~FOUO~~) The RFPA does not apply when the government and the customer are litigants in a judicial or an administrative adjudicatory proceeding.

O.6.5 (U) OTHER

(U//~~FOUO~~) Other matters specifically excluded are: (1) certain designated supervisory agencies of financial institutions, (2) the Internal Revenue Service, (3) the General Accounting Office, (4) certain reports required of financial institutions, (5) the account's identifying information only, and (6) the administration of guaranty or loan insurance programs.

O.7 (U) ROLES AND RESPONSIBILITIES

O.7.1 (U) FBI SUPERVISORY PERSONNEL

(U//~~FOUO~~) Before records may be obtained under any provision of the RFPA, [REDACTED]

[REDACTED]

b7E

[REDACTED] any FBIHQ or field office supervisor [REDACTED]

[REDACTED]

[REDACTED] (See Delegation of Authority in subsection O.3.8.)

(U//~~FOUO~~) Access to financial records for certain intelligence and protective purposes requires a certification, in writing (via an NSL), to the financial institution, stating that such records are sought for foreign counterintelligence purposes to protect against international terrorism or clandestine activities. [REDACTED]

b7E

[REDACTED]

[REDACTED]

O.7.2 (U) SPECIAL AGENTS AND TASK FORCE OFFICERS (TFO)

(U//~~FOUO~~) All special agents and TFOs should obtain familiarity with the RFPA in order to ensure compliance therewith. Although the RFPA does not apply to state and local law

enforcement, deputized TFOs working on FBI-led task forces are considered federal law enforcement agents; therefore, they are bound by the RFPAs requirements when working on federal cases.

O.7.3 (U) CHIEF DIVISION COUNSEL (CDC)

(U//~~FOUO~~) The CDC provides training on the requirements of the RFA, as needed, during field office legal training.

O.7.4 (U) OFFICE OF THE GENERAL COUNSEL (OGC)

(U//~~FOUO~~) OGC ensures that any changes to the law or significant developments in the case law of the RFA are communicated to CDCs.

O.8 (U) REMEDIES AND SANCTIONS

(U//~~FOUO~~) Failure to adhere to the statutory requirements of the RFA could lead to notification by the financial institution to the customer that the FBI requested his or her records and that there is a possibility that the FBI could be held liable in a civil action brought by the customer. An FBI employee may also be subject to disciplinary action for willful or intentional violation of the RFA and may be subject to civil liability. The customer cannot, however, seek other remedies not specified in the statute such as suppression of the records (12 U.S.C. § 3417(d)).

O.9 (U) REIMBURSEMENT COST

(U//~~FOUO~~) The RFA is an exception to the general rule that federal agencies do not pay for information associated with compliance with a grand jury subpoena. The RFA specifically requires the FBI to reimburse the financial institution for specific costs as set forth in the statute (see 12 U.S.C. § 3415). Reimbursement should be accomplished through the routine commercial vouchering procedures. The schedule of authorized fees is set forth in 12 CFR § 219.3, Appendix A.

b7E

This Page is Intentionally Blank.

P APPENDIX P: (U) ACRONYMS

A/EAD	Associate Executive Assistant Director
AD	Assistant Director
ADD	Associate Deputy Director
ADIC	Assistant Director-in-Charge
AFID	Alias False Identification
AG	Attorney General
AGG	Attorney General Guidelines
AGG-CHS	Attorney General Guidelines Regarding the Use of FBI Confidential Human Sources
AGG-Dom	Attorney General's Guidelines for Domestic FBI Operations
AGG-UCO	The Attorney General's Guidelines on FBI Undercover Operations
AOR	Area of Responsibility
ASAC	Assistant Special Agent in Charge
ASC	Assistant Section Chief
ATF	Bureau of Alcohol, Tobacco, Firearms and Explosives
AUSA	Assistant United States Attorney
BOP	Bureau of Prisons
CALEA	Communications Assistance for Law Enforcement Act
CCRSB	Criminal Cyber Response and Services Branch
CD	Counterintelligence Division
CDC	Chief Division Counsel
CFR	Code of Federal Regulations
CHS	Confidential Human Source
CHSPG	Confidential Human Source Policy Guide

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

CIA	Central Intelligence Agency
CID	Criminal Investigative Division
CMS	Collection Management Section
CUORC	Criminal Undercover Operations Review Committee
CyD	Cyber Division
DAD	Deputy Assistant Director
DD	Deputy Director
DEA	Drug Enforcement Administration
DGC	Deputy General Counsel
DI	Directorate of Intelligence
DLAT	Deputy Legal Attache
DNI	Director of National Intelligence
DOD	Department of Defense
DOJ	Department of Justice
DOJ OEO	Office of Enforcement Operations, DOJ
DOS	Department of State
DPO	Division Policy Officer
EAD	Executive Assistant Director
EC	Electronic Communication
ECF	Electronic Case File
ECPA	Electronic Communication Privacy Act
ECS	Electronic Communication Service
EDA	ELSUR Data Application

b7E

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

EI	Enterprise Investigation
ELSUR	Electronic Surveillance
EO	Executive Order
EOT	ELSUR Operations Technician
ESN	Electronic Serial Number
ESU	DOJ OEO, Electronic Surveillance Unit
ETR	Electronic Technical Request
FBIHQ	FBI Headquarters
FGJ	Federal Grand Jury
FICP	Foreign Intelligence Collection Program
FIG	Field Intelligence Group
FISA	Foreign Intelligence Surveillance Act
FISC	Foreign Intelligence Surveillance Court
FPO	Field Office Policy Officer
FRCP	Federal Rules of Criminal Procedure
GC	General Counsel
HIPAA	Health Insurance Portability and Accountability Act
HSC	Homeland Security Council
ICE	Department of Homeland Security Immigration and Customs Enforcement
ICM	Investigative Case Management
IINI	Innocent Images National Initiative

b7E

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

ILB	Investigative Law Branch
ILU	Investigative Law Unit
IMD	Information Management Division
IOB	Intelligence Oversight Board
IOD	International Operations Division
IP Address	Internet Protocol Address
IPO	Internal Policy Office
ISP	Internet Service Provider
JDA	Juvenile Delinquency Act
JTTF	Joint Terrorism Task Force
LEGAT	Legal Attaché
LHM	Letterhead Memorandum
LO	Lead Office
MLAT	Mutual Legal Assistance Treaties
MOU/MOA	Memorandum of Understanding/Agreement
MSIN	Mobile Station Identification Number
NARA	National Archives and Records Administration
NCMEC	National Center for Missing and Exploited Children
NISS	National Information Sharing Strategy
NSB	National Security Branch
NSC	National Security Council
NSD	National Security Division, DOJ
NSL	National Security Letter
NSCLB	National Security and Cyber Law Branch

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

NSSE	National Special Security Events
OCA	Office of Congressional Affairs
OCRS	Organized Crime and Racketeering Section, DOJ
OGC	Office of the General Counsel
OIA	Otherwise Illegal Activity
OIC	Office of Integrity and Compliance
OLC	Office of Legal Counsel, DOJ
OO	Office of Origin
OPA	Office of Public Affairs
OTD	Operational Technology Division
PBDM	Pattern Based Data Mining
PCHS	Potential CHS
PCLU	Privacy and Civil Liberties Unit
PCTDD	Post Cut-through Dialed Digits
PFI	Positive Foreign Intelligence
PG	Policy Guide
PI	Preliminary Investigation
PIA	Privacy Impact Assessment
PIAB	President's Intelligence Advisory Board
PSA	Performance Summary Assessments
PTA	Privacy Threshold Analysis
RA	Resident Agency
RF	Radio Frequency

b7E

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

RFPA	Right to Financial Privacy Act
RICO	Racketeer Influenced and Corrupt Organizations
RIG	Regional Intelligence Group
SA	Special Agent
SAC	Special Agent-in-Charge
SC	Section Chief
SIA	Supervisory Intelligence Analyst
SIU	Strategic Initiative's Unit
SIM	Sensitive Investigative Matter
SOG	Special Operations Group
SORC	Sensitive Operations Review Committee
SSA	Supervisory Special Agent
SSG	Special Surveillance Group
SSRA	Supervisory Senior Resident Agent
TFM	Task Force Member
TFO	Task Force Officer
TFP	Task Force Participant
TMD	Technical Management Database
TTA	Technically Trained Agent
UC	Unit Chief
UCE	Undercover Employee
UCFN	Universal Case File Number
UCO	Undercover Operation
UCRC	Undercover Review Committee

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

UDP	Undisclosed Participation
UNI	Universal Index
USA	United States Attorney
USAO	United States Attorney's Office
U.S.C.	United States Code
USG	United States Government
USIC	United States Intelligence Community
USMS	United States Marshals Service
USPER	United States Person, United States Persons, US PER, USPERs, US Person, US Persons, U.S. Person, U.S. Persons
USPS	United States Postal Service
USSS	United States Secret Service
VS	Victim Specialist
WITT	Wireless Intercept Tracking Technology
WMD	Weapons of Mass Destruction
WMDD	Weapons of Mass Destruction Directorate

This Page is Intentionally Blank.

Q APPENDIX Q: (U) DEFINITIONS

(U//~~FOUO~~) Academic Nexus SIM: [REDACTED]

b7E

(U) Aggrieved Person: [REDACTED]
[REDACTED]

(U//~~FOUO~~) **Assessments:** The AGG-Dom authorizes as an investigative activity called an “Assessment” which requires an authorized purpose and articulated objective(s). The DIOG defines five types of Assessments that may be carried out to detect, obtain information about, or prevent or protect against federal crimes or threats to the national security or to collect foreign intelligence. Although “no particular factual predication” is required, the basis of an Assessment cannot be arbitrary or groundless speculation, nor can an Assessment be based solely on the exercise of First Amendment protected rights or on the race, ethnicity, gender, national origin, religion, disability, sexual orientation, or gender identity of the subject, or a combination of only those factors.

(U//~~FOUO~~) **Closed Circuit Television (CCTV):** a fixed-location video camera that is typically concealed from view or that is placed on or operated by a consenting party.

(U) **Consensual Monitoring:** Monitoring of communications for which a court order or warrant is not legally required because of the consent of a party to the communication.

(U) **Electronic Communication Service:** Any service that provides to users thereof the ability to send or receive wire or electronic communications. For example, telephone companies and electronic mail companies generally act as providers of electronic communication services.

(U) **Electronic Communications System:** Any wire, radio, electromagnetic, photo optical or photo electronic facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications.

(U) **Electronic Storage:** Any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof, or any storage of such communication by an electronic communication service for purposes of backup protection of such communication. In short, “electronic storage” refers only to temporary storage, made in the course of transmission, by a provider of an electronic communication service.

(U//~~FOUO~~) Electronic Tracking Device: [REDACTED]
[REDACTED]

b7E

(U//~~FOUO~~) **Employee:** For purposes of the AGG-Dom and DIOG, an “FBI employee” includes, but not limited to, an operational/administrative professional staff person, intelligence analyst, special agent, task force officer (TFO), task force member (TFM), task force participant (TFP), detailee, and FBI contractor. An FBI employee is bound by the AGG-Dom and DIOG. The FBI employee definition excludes a confidential human source (CHS).

(U//~~FOUO~~) **Enterprise:** The term “enterprise” includes any individual, partnership, corporation, association, or other legal entity, and any union or group of individuals associated in fact although not a legal entity.

(U//~~FOUO~~) **Enterprise Investigation:** An Enterprise Investigation (EI) examines the structure, scope, and nature of the group or organization including: its relationship, if any, to a foreign power; the identity and relationship of its members, employees, or other persons who may be acting in furtherance of its objectives; its finances and resources; its geographical dimensions; its past and future activities and goals; and its capacity for harm. (AGG-Dom, Part II.C.2)

(U//~~FOUO~~) Enterprise Investigations are a type of Full Investigation and are subject to the same requirements that apply to Full Investigations described in Section 7. Enterprise Investigations focus on groups or organizations that may be involved in the most serious criminal or national security threats to the public, as described in Section 8. Enterprise Investigations cannot be conducted as Preliminary Investigations or Assessments, nor may they be conducted for the sole purpose of collecting foreign intelligence.

b7E

(U//~~FOUO~~) **Extraterritorial Guidelines:** The guidelines for conducting investigative activities outside of the United States are currently contained in: (i) *The Attorney General’s Guidelines for Extraterritorial FBI Operations and Criminal Investigations*; (ii) *The Attorney General’s Guidelines for FBI National Security Investigations and Foreign Intelligence Collection*; and (iii) *The Attorney General Guidelines on the Development and Operation of FBI Criminal Informants and Cooperative Witnesses in Extraterritorial Jurisdictions* (collectively, the Extraterritorial Guidelines); (iv) *The Attorney General Procedure for Reporting and Use of Information Concerning Violations of Law and Authorization for Participation in Otherwise Illegal Activity in FBI Foreign Intelligence, Counterintelligence or International Terrorism Intelligence Investigations* (August 8, 1988); and (v) the *Memorandum of Understanding Concerning Overseas and Domestic Activities of the Central Intelligence Agency and the Federal Bureau of Investigation* (2005).

(U//~~FOUO~~) **FISA:** The Foreign Intelligence Surveillance Act of 1978, as amended. The law establishes a process for obtaining judicial approval of electronic surveillance, physical searches, pen register and trap and trace devices, and access to certain business records for the purpose of collecting foreign intelligence.

(U) **For or On Behalf of a Foreign Power:** The determination that activities are for or on behalf of a foreign power shall be based on consideration of the extent to which the foreign power is involved in control or policy direction; financial or material support; or leadership, assignments, or discipline.

(U) **Foreign Computer Intrusion:** The use or attempted use of any cyber-activity or other means, by, for, or on behalf of a foreign power to scan, probe, or gain unauthorized access into one or more United States-based computers.

(U) **Foreign Intelligence:** Information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations or foreign persons, or international terrorists.

(U) Foreign Intelligence Requirements:

- A) (U//~~FOUO~~) National intelligence requirements issued pursuant to authorization by the Director of National Intelligence, including the National Intelligence Priorities Framework and the National HUMINT Collection Directives, or any successor directives thereto;
- B) (U//~~FOUO~~) Requests to collect foreign intelligence by the President or by Intelligence Community officials designated by the President; and
- C) (U//~~FOUO~~) Directions to collect foreign intelligence by the Attorney General, the Deputy Attorney General, or an official designated by the Attorney General.

(U) **Foreign Power:** A foreign government or any component thereof, whether or not recognized by the United States; a faction of a foreign nation or nations, not substantially composed of United States persons (USPERs); an entity that is openly acknowledged by a foreign government or governments to be directed and controlled by such foreign government or governments; a group engaged in international terrorism or activities in preparation therefore; a foreign-based political organization, not substantially composed of USPERs; or an entity that is directed or controlled by a foreign government or governments.

(U) **Full Investigation:** A Full Investigation may be opened if there is an “articulable factual basis” for the investigation that reasonably indicates one of the following circumstances exists:

(U) An activity constituting a federal crime or a threat to the national security has or may have occurred, is or may be occurring, or will or may occur and the investigation may obtain information relating to the activity or the involvement or role of an individual, group, or organization in such activity:

- A) (U) An individual, group, organization, entity, information, property, or activity is or may be a target of attack, victimization, acquisition, infiltration, or recruitment in connection with criminal activity in violation of federal law or a threat to the national security and the investigation may obtain information that would help to protect against such activity or threat; or
- B) (U) The investigation may obtain foreign intelligence that is responsive to a PFI requirement, as defined in DIOG Section 7.4.3.

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

(U) All lawful investigative methods may be used in a Full Investigation.

(U) A Full Investigation of a group or organization may be opened as an Enterprise Investigation if there is an articulable factual basis for the investigation that reasonably indicates the group or organization may have engaged, or may be engaged in, or may have or may be engaged in planning or preparation or provision of support for:

A) (U) Racketeering Activity:

- 1) (U) A pattern of racketeering activity as defined in 18 U.S.C. § 1961(5);

B) (U) International Terrorism:

- 1) (U) International terrorism, as defined in the AGG-Dom, Part VII.J, or other threat to the national security;

C) (U) Domestic Terrorism:

- 1) (U) Domestic terrorism as defined in 18 U.S.C. § 2331(5) involving a violation of federal criminal law;
- 2) (U) Furthering political or social goals wholly or in part through activities that involve force or violence and a violation of federal criminal law; or
- 3) (U) An offense described in 18 U.S.C. § 2332b(g)(5)(B) or 18 U.S.C. § 43.

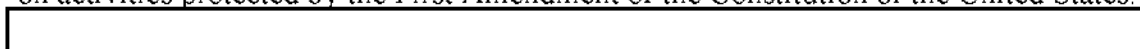
(U) Human Source: A Confidential Human Source as defined in the Attorney General's Guidelines Regarding the Use of FBI Confidential Human Sources.

(U) Intelligence Activities: Any activity conducted for intelligence purposes or to affect political or governmental processes by, for, or on behalf of a foreign power.

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

(U) Member of the Public with a Disability: a person with a disability who meets the essential eligibility requirements for participation in, or receipt of benefits from, a traditional law enforcement program or activity conducted by the FBI. See Department of Justice's *Guidance on Interactions with Members of the Public with Disabilities in Traditional Law Enforcement Programs and Activities*.

(U//FOUO) National Security Letters: an administrative demand for documents or records that can be made by the FBI during a predicated investigation relevant to a threat to national security. The standard for issuing an NSL, except under 15 U.S.C. § 1681v, is relevance to an authorized investigation to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a United States person (USPER) is not predicated solely on activities protected by the First Amendment of the Constitution of the United States.



b7E

[REDACTED]

(U//~~FOUO~~) **Operational Division or Operational Unit:** “Operational” division or operational unit as used in the DIOG means the FBIHQ division or unit responsible for management and program oversight of the file classification for the substantive investigative matter (i.e., Assessment or predicated investigation). Previously referred to as the FBIHQ “substantive” division or substantive unit.

(U//~~FOUO~~) **Pen Register Device:** Records or decodes dialing, routing addressing or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided that such information must not include the contents of any communication.

(U//~~FOUO~~) **Physical Surveillance (Not Requiring a Court Order):** The deliberate observation by an FBI employee of persons, places, or events, on either a limited or continuous basis, in areas where there is no reasonable expectation of privacy. *Note:* DIOG Section 18.5.8 makes a distinction between “casual observation” and physical surveillance, and specifies factors to be considered when determining whether a particular plan of action constitutes casual observation or physical surveillance. (See DIOG Section 18.5.8)

(U) **Predicated Investigation:** While Assessments only require an “authorized purpose” to initiate, a predicated investigation requires factual predication to open. As defined in the AGG-Dom, a predicated investigation that relates to a federal crime or national security threat may be opened as a Preliminary Investigation (based on “information or allegation”) or a Full Investigation (based on an “articulable factual basis”). See DIOG Sections 6 and 7, respectively. Enterprise Investigations (DIOG Section 8) and Positive Foreign Intelligence Investigations (DIOG Section 9) are types of Full Investigations.

(U) **Preliminary Investigation:** A Preliminary Investigation is a type of predicated investigation authorized under the AGG-Dom that may be opened (predicated) on the basis of any “allegation or information” indicative of possible criminal activity or threats to the national security. Preliminary Investigations may be opened to detect, obtain information about, or prevent or protect against federal crimes or threats to the national security. [REDACTED]

[REDACTED]

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

(U) **Provider of Electronic Communication Services:** Any service that provides the user thereof the ability to send or receive wire or electronic communications.

(U) **Publicly Available:** Information that has been published or broadcast for public consumption, is available on request to the public, is accessible on-line or otherwise to the public, is available to the public by subscription or purchase, could be seen or heard by any casual observer, is made available at a meeting open to the public, or is obtained by visiting any place or attending any event that is open to the public.

(U) **Records:** Any records, databases, files, indices, information systems, or other retained information.

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

(U) Relevance: Information is relevant if it tends to make a fact of consequence more or less probable.

(U//~~FOUO~~) Remote Computing Services:

b7E

(U//~~FOUO~~) Sensitive Investigative Matter: An investigative matter involving a domestic public official, domestic political candidate, religious or domestic political organization or individual prominent in such an organization, or news media, or an investigative matter having academic nexus, or any other matter which, in the judgment of the official authorizing an investigation, should be brought to the attention of FBIHQ and other DOJ officials.

(U) Sensitive Monitoring Circumstance: Consensual monitoring during one of the following scenarios:

- A) (U) Investigation of a member of Congress, a federal judge, a member of the executive branch at Executive Level IV or above, or a person who has served in such capacity within the previous two years. (Executive Levels I through IV are defined in 5 U.S.C. §§ 5312-5315.)
- B) (U) Investigation of the governor, lieutenant governor, or attorney general of any state or territory, or a judge or a justice of the highest court of any state or territory, concerning an offense involving bribery, conflict of interest, or extortion related to the performance of official duties.
- C) (U) A party to the communication is in the custody of the Bureau of Prisons (BOP) or the United States Marshals Service (USMS) or is being or has been afforded protection in the Witness Security Program.
- D) (U) The Attorney General, the Deputy Attorney General, or an Assistant Attorney General has requested that the FBI obtain prior approval for the use of consensual monitoring in a specific investigation.

(U) Special Agent in Charge: The Special Agent in Charge of an FBI field office (including an Acting Special Agent in Charge), except that the functions authorized for Special Agents in Charge by these Guidelines may also be exercised by the Assistant Director in Charge or by any Special Agent in Charge designated by the Assistant Director in Charge in an FBI field office headed by an Assistant Director, and by FBI Headquarters officials designated by the Director of the FBI.

(U) Special Events Management: Planning and conduct of public events or activities whose character may make them attractive targets for terrorist attack.

(U) State, Local, or Tribal: Any state or territory of the United States or political subdivision thereof, the District of Columbia, or Indian tribe.

(U//~~FOUO~~) Surveillance:

- A) (U//~~FOUO~~) **Electronic surveillance (ELSUR)** - under Title III and FISA is the non-consensual electronic collection of information (usually communications) under circumstances in which the parties have a reasonable expectation of privacy and court orders or warrants are required

b7E

[REDACTED]

B) (U//~~FOUO~~) **Consensual monitoring of communications, including consensual computer monitoring, or electronic surveillance (ELSUR)** - where there is no reasonable expectation of privacy is permitted in predicated investigations. These methods usually do not require court orders or warrants unless they involve an intrusion into an area where there is a reasonable expectation of privacy or non-consensual monitoring of communications, but legal review is generally required to ensure compliance with legal requirements. [REDACTED]

[REDACTED]

C) (U//~~FOUO~~) **Physical surveillance** - is the deliberate observation by an FBI employee of persons, places, or events, on either a limited or continuous basis, in areas where there may or may not be a reasonable expectation of privacy. (See DIOG Section 18.5.8 for physical surveillance in situations not requiring a court order and a discussion of the distinction between physical surveillance and casual observation). Factors to consider in determining whether observations are casual observation or physical surveillance include [REDACTED]

[REDACTED]

(U) **Threat to the National Security:** International terrorism; espionage and other intelligence activities, sabotage, and assassination, conducted by, for, or on behalf of foreign powers, organizations, or persons; foreign computer intrusion; and other matters determined by the Attorney General, consistent with Executive Order 12333 or a successor order.

(U//~~FOUO~~) **Trap and Trace Device:** Captures the incoming electronic or other impulses that identify the originating number or other dialing, routing, addressing or signaling information reasonably likely to identify the source of a wire or electronic communication, provided that such information does not include the contents of any communication.

(U//~~FOUO~~) **Undercover Activity (UCA):** An “undercover activity” is any investigative activity involving the use of an assumed name or cover identity by an employee of the FBI or another Federal, state, tribal or local law enforcement organization working with the FBI. An element of UCA is the conduct of investigative activity to seek information relevant to federal crimes or national security threats by means of interaction with a third party(ies).

(U//~~FOUO~~) **Undercover Employee (UCE):** An employee of the FBI, or employee of federal, state, or local law enforcement agency, USIC entity, or foreign intelligence agency working under the direction and control of the FBI during a particular investigation or operation whose relationship with the FBI is concealed from third parties in the course of an investigative or intelligence collection operation by the maintenance of a cover or alias identity.

(U//~~FOUO~~) **Undercover Operation (UCO):** An “undercover operation” is an operation that involves a series of related “undercover activities” over a period of time by an “undercover

employee.” A “series of related undercover activities” consists of more than five separate substantive contacts by an undercover employee with the individual(s) under investigation

b7E

(U) United States: When used in a geographic sense, means all areas under the territorial sovereignty of the United States.

(U) United States Person (USPER): Any of the following:

- A) (U) An individual who is a United States citizen or an alien lawfully admitted for permanent residence;
- B) (U) An unincorporated association substantially composed of individuals who are United States persons (USPERs); or
- C) (U) A corporation incorporated in the United States.

(U) An USPER does not include any association or corporation that is a foreign power, defined as an entity that is openly acknowledged by a foreign government or governments to be directed and controlled by such foreign government or governments.

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

(U) Use: When used with respect to human sources, means obtaining information from, tasking, or otherwise operating such sources.

This Page is Intentionally Blank.

R APPENDIX R: (U) SUPERSEDED DOCUMENTS AND NFIPM, MIOG, AND MAOP SECTION

(U//~~FOUO~~) This guide supersedes the following FBI policies and procedures:

Part	Section	Section Title	DIOG Supersession
MIOG Intro	Preface	Section: Preface (1)	DIOG Preamble
MIOG Intro	Preface	Preface	DIOG Preamble
MIOG Intro	Section 1	Section: S1: Investigative Authority and Responsibility (12)	DIOG Preamble
MIOG Intro	Section 1	1-1 AUTHORITY OF A SPECIAL AGENT	DIOG Preamble
MIOG Intro	Section 1	1-2 INVESTIGATIVE RESPONSIBILITY	DIOG Preamble
MIOG Intro	Section 1	1-3 THE ATTORNEY GENERALS GUIDELINES ON GENERAL CRIMES, RACKETEERING ENTERPRISE AND TERRORISM ENTERPRISE INVESTIGATIONS	DIOG Preamble
MIOG Intro	Section 1	1-3 INTRODUCTION	DIOG Preamble
MIOG Intro	Section 1	1-3I. GENERAL PRINCIPLES	DIOG Preamble
MIOG Intro	Section 1	1-3 II. GENERAL CRIMES INVESTIGATIONS	DIOG Preamble
MIOG Intro	Section 1	1-3 III. CRIMINAL INTELLIGENCE INVESTIGATIONS	DIOG Preamble
MIOG Intro	Section 1	1-3 IV. INVESTIGATIVE TECHNIQUES	DIOG Preamble
MIOG Intro	Section 1	1-3 V. DISSEMINATION AND MAINTENANCE OF INFORMATION	DIOG Preamble
MIOG Intro	Section 1	1-3 VI. COUNTERTERRORISM ACTIVITIES AND OTHER AUTHORIZATIONS	DIOG Preamble
MIOG Intro	Section 1	1-3 VII. RESERVATION	DIOG Preamble
MIOG Intro	Section 1	1-4 INVESTIGATIVE AUTHORITY AND THE FIRST AMENDMENT	DIOG Preamble
MIOG Intro	Section 2	Section : S2: Management and Allocation Programs (57)	DIOG Preamble
MIOG Intro	Section 2	2-1 NATIONAL PRIORITY PROGRAMS	DIOG Preamble

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

Part	Section	Section Title	DIOG Supersession
MIOG Intro	Section 2	2-1.1 Foreign Counterintelligence (FCI)	DIOG Preamble
MIOG Intro	Section 2	2-1.1.1 Definition	DIOG Preamble
MIOG Intro	Section 2	2-1.1.2 Objective	DIOG Preamble
MIOG Intro	Section 2	2-1.2 Organized Crime	DIOG Preamble
MIOG Intro	Section 2	2-1.2.1 Definition	DIOG Preamble
MIOG Intro	Section 2	2-1.2.2 Objective	DIOG Preamble
MIOG Intro	Section 2	2-1.2.3 Ranking of Organized Criminal Activities	DIOG Preamble
MIOG Intro	Section 2	2-1.3 Drug	DIOG Preamble
MIOG Intro	Section 2	2-1.3.1 Definition	DIOG Preamble
MIOG Intro	Section 2	2-1.3.2 Objective	DIOG Preamble
MIOG Intro	Section 2	2-1.4 Counterterrorism	DIOG Preamble
MIOG Intro	Section 2	2-1.4.1 Definition	DIOG Preamble
MIOG Intro	Section 2	2-1.4.2 Objective	DIOG Preamble
MIOG Intro	Section 2	2-1.5 White-Collar Crime	DIOG Preamble
MIOG Intro	Section 2	2-1.5.1 Definition	DIOG Preamble
MIOG Intro	Section 2	2-1.5.2 Objective	DIOG Preamble
MIOG Intro	Section 2	2-1.5.3 Ranking of Activities	DIOG Preamble
MIOG Intro	Section 2	2-1.6 Violent Crimes and Major Offenders	DIOG Preamble
MIOG Intro	Section 2	2-1.6.1 Fugitive Subprogram	DIOG Preamble
MIOG Intro	Section 2	2-1.6.2 Government Reservation Crimes Subprogram	DIOG Preamble
MIOG Intro	Section 2	2-1.6.3 Interstate Theft Subprogram	DIOG Preamble
MIOG Intro	Section 2	2-1.6.4 Violent Crimes Subprogram	DIOG Preamble
MIOG Intro	Section 2	2-1.6.5 Violent Crimes and Major Offenders-Organized Crime Drug Enforcement Task Force Subprogram	DIOG Preamble
MIOG Intro	Section 2	2-2 OTHER PROGRAMS	DIOG Preamble

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

Part	Section	Section Title	DIOG Supersession
MIOG Intro	Section 2	2-2.1 Deleted	DIOG Preamble
MIOG Intro	Section 2	2-2.1.1 Deleted	DIOG Preamble
MIOG Intro	Section 2	2-2.1.2 Deleted	DIOG Preamble
MIOG Intro	Section 2	2-2.1.3 Deleted	DIOG Preamble
MIOG Intro	Section 2	2-2.2 Applicant Investigations - Reimbursable and Nonreimbursable	DIOG Preamble
MIOG Intro	Section 2	2-2.2.1 Definition	DIOG Preamble
MIOG Intro	Section 2	2-2.2.2 Objective	DIOG Preamble
MIOG Intro	Section 2	2-2.2.3 Ranking of Activities	DIOG Preamble
MIOG Intro	Section 2	2-2.3 Civil Rights	DIOG Preamble
MIOG Intro	Section 2	2-2.3.1 Definition	DIOG Preamble
MIOG Intro	Section 2	2-2.3.2 Objective	DIOG Preamble
MIOG Intro	Section 2	2-2.3.3 Ranking of Activities	DIOG Preamble
MIOG Intro	Section 2	2-2.4 FBI Security Program	DIOG Preamble
MIOG Intro	Section 2	2-2.4.1 Definition	DIOG Preamble
MIOG Intro	Section 2	2-2.4.2 Objective	DIOG Preamble
MIOG Intro	Section 2	2-2.4.3 Ranking of Activities	DIOG Preamble
MIOG Intro	Section 2	2-2.5 Deleted	DIOG Preamble
MIOG Intro	Section 2	2-2.5.1 Deleted	DIOG Preamble
MIOG Intro	Section 2	2-2.5.2 Deleted	DIOG Preamble
MIOG Intro	Section 2	2-2.5.3 Deleted	DIOG Preamble
MIOG Intro	Section 2	2-2.6 Deleted	DIOG Preamble
MIOG Intro	Section 2	2-2.6.1 Deleted	DIOG Preamble
MIOG Intro	Section 2	2-2.6.2 Deleted	DIOG Preamble
MIOG Intro	Section 2	2-2.6.3 Deleted	DIOG Preamble
MIOG Intro	Section 2	2-2.7 Deleted	DIOG Preamble

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

Part	Section	Section Title	DIOG Supersession
MIOG Intro	Section 2	2-2.7.1 Deleted	DIOG Preamble
MIOG Intro	Section 2	2-2.7.2 Deleted	DIOG Preamble
MIOG Intro	Section 2	2-2.7.3 Deleted	DIOG Preamble
MIOG Intro	Section 2	2-2.8 Deleted	DIOG Preamble
MIOG Intro	Section 2	2-2.8.1 Deleted	DIOG Preamble
MIOG Intro	Section 2	2-2.8.2 Deleted	DIOG Preamble
MIOG Intro	Section 2	2-2.8.3 Deleted	DIOG Preamble
MIOG I.I	Section 7	7-5 CLARIFICATION REGARDING AN INVESTIGATION AS OPPOSED TO A PRELIMINARY INQUIRY	DIOG 5, 6 and 7
MIOG I.I	Section 7	7-6 DEPARTMENTAL INSTRUCTIONS REGARDING QUESTIONABLE CASES	Paragraphs #1 and 2 only. DIOG 5, 6 and 7
MIOG I.I	Section 7	7-20 ADMINISTRATIVE SUBPOENAS IN CHILD ABUSE AND CHILD SEXUAL EXPLOITATION (CSE) CASES	DIOG 18.6.4
MIOG I.I	Section 9	9-7.2 Use of Closed Circuit Television (CCTV)	Paragraphs #2 (all sub-parts); 3 (all sub-parts); and 4 only. DIOG 18.6.3
MIOG I.I	Section 62	62-3 DOMESTIC POLICE COOPERATION - STATUTE	
MIOG I.I	Section 62	62-3.3 Policy	Paragraphs # 5 and 6 only. DIOG 12
MIOG I.I	Section 62	62-3.4 Office of Origin	DIOG 14
MIOG I.I	Section 62	62-3.5 Classification	DIOG 12. See new 343 classification
MIOG I.2	Section 157	Section : S157 Civil Unrest (8)	DIOG 12
MIOG I.2	Section 157	157-1 RESPONSIBILITY OF THE BUREAU	DIOG 12
MIOG I.2	Section 157	157-1.1 Categories for Reporting	DIOG 12
MIOG I.2	Section 157	157-2 POLICY REGARDING REPORTING OF CIVIL DISORDERS	DIOG 12
MIOG I.2	Section 157	157-3 REPORTING OF DEMONSTRATIONS	DIOG 12

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

Part	Section	Section Title	DIOG Supersession
MIOG I.2	Section 157	157-4 PHOTOGRAPHIC SURVEILLANCES	DIOG 12
MIOG I.2	Section 157	157-5 DISSEMINATION OF DATA PERTAINING TO CIVIL DISORDERS AND DEMONSTRATIONS	DIOG 12
MIOG I.2	Section 157	157-6 REPORTING PROCEDURES TO BE UTILIZED IN CIVIL DISORDERS AND DEMONSTRATIONS	DIOG 12
MIOG I.2	Section 157	157-7 CHARACTER	DIOG 12
MIOG I.2	Section 161	161-10 DISSEMINATION TO THE WHITE HOUSE COMPLEX (WHC)	DIOG 14, 18
MIOG I.2	Section 163	163-1.1 Investigative Request	DIOG 12
MIOG I.2	Section 163	163-2 INVESTIGATIVE INSTRUCTIONS AND PROCEDURES	DIOG 12
MIOG I.2	Section 163	163-2.1 Opening Foreign Police Cooperation (FPC) - General Criminal Matters (GCM)	DIOG 12.2
MIOG I.2	Section 163	163-2.1.1 Letter Rogatory Process	DIOG 12
MIOG I.2	Section 163	163-3 REQUESTS FOR TERRORISM ENTERPRISE INVESTIGATIONS	DIOG 8, 12
MIOG I.2	Section 163	163-6 REPORTING	DIOG 12
MIOG I.2	Section 163	163-7 RULE 6(E) MATERIAL	DIOG 18
MIOG I.2	Section 163	163-8 PRIVACY ACT	DIOG 14
MIOG I.2	Section 163	163-9 RIGHT TO FINANCIAL PRIVACY ACT	DIOG Appendix O
MIOG I.2	Section 288	288-5.1 Accessing Computer Records - Summary of Compelled Disclosure under Title 18, USC, Section 2703	DIOG 18.6.8
MIOG I.2	Section 288	288-5.1.1 Subpoena - ECPA Requirements	DIOG 18.6.8
MIOG I.2	Section 288	288-5.1.2 Subpoena with Prior Notice to the Subscriber or Customer	DIOG 18.6.8
MIOG I.2	Section 288	288-5.1.3 Section 2703(d) Order	DIOG 18.6.8
MIOG I.2	Section 288	288-5.1.4 Section 2703(d) Order with Prior Notice to the Subscriber or Customer	DIOG 18.6.8

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

Part	Section	Section Title	DIOG Supersession
MIOG I.2	Section 288	288-5.1.5 Search Warrant	DIOG 18.7.1
MIOG I.2	Section 288	288-5.1.6 Voluntary Disclosure	DIOG 18.6.8
MIOG I.2	Section 289	289-13.3 Use of a Past or Present Prisoner-Witness in an Investigation (Formerly Part 2, 27-16.5)	DIOG 11.5, 18.6.1, 18.6.2
MIOG I.2	Section 308	308-1.1 Evidence Response Team Mission	generally, DIOG 12 for expert assistance.
MIOG I.2	Section 308	308-2 DEFINITION OF ERT CONCEPT	Paragraph # 4 only. DIOG 12
MIOG I.2	Section 308	308-3 PROPER TURNING	Paragraph # 2 only. DIOG 12
MIOG I.2	Section 308	308-4 ERT SUBCLASSIFICATIONS-ALPHA DESIGNATORS	Paragraph # 1 only. DIOG 12. See new classifications
MIOG I.2	Section 319	319-1 INTELLIGENCE PROGRAM	generally, DIOG 5
MIOG I.2	Section 319	319-2 FIELD INTELLIGENCE GROUP (FIG) STRUCTURE AND FUNCTIONS	generally, DIOG 5
MIOG I.2	Section 319	319-4 INTELLIGENCE COLLECTION	Paragraphs # 1 and 3 generally, DIOG 5
MIOG I.2	Section 319	319-5 COLLECTION MANAGEMENT	generally, DIOG 5
MIOG II	Section 2	2-5 COMPLAINTS (RULE 3)	DIOG 19
MIOG II	Section 2	2-5.1 Authorization of U.S. Attorney (USA)	DIOG 19
MIOG II	Section 2	2-5.3 State Prosecutions	DIOG 3, 12
MIOG II	Section 2	2-5.4 Authority for Issuance of Warrant	DIOG 19
MIOG II	Section 2	2-5.5 Notification to Special Agent in Charge (SAC)	DIOG 19
MIOG II	Section 2	2-6 WARRANT OF ARREST OR SUMMONS (RULE 4)	DIOG 18 and 19
MIOG II	Section 2	2-6.1 Forms of Warrant	DIOG 19
MIOG II	Section 2	2-6.2 Issuance of Warrant or Summons	DIOG 19
MIOG II	Section 2	2-6.3 Execution	DIOG 19

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

Part	Section	Section Title	DIOG Supersession
MIOG II	Section 2	2-7 PROCEEDINGS BEFORE THE MAGISTRATE (RULE 5)	DIOG 18, 19
MIOG II	Section 2	2-7.1 Initial Appearance	DIOG 19
MIOG II	Section 2	2-9 GRAND JURY (RULE 6)	DIOG 11.9, 11.9.1, 18.5.9, 18.6.5
MIOG II	Section 2	2-9.1 Purpose	DIOG 18.5.9, 18.6.5
MIOG II	Section 2	2-9.2 Persons Present	DIOG 18.5.9, 18.6.5
MIOG II	Section 2	2-9.3 Disclosure	DIOG 18.5.9, 18.6.5
MIOG II	Section 2	2-9.4 Exceptions	DIOG 11.9, 11.9.1, 18.5.9, 18.6.5
MIOG II	Section 2	2-9.5 Limitation of Use	DIOG 18.5.9, 18.6.5
MIOG II	Section 2	2-9.5.1 Matters Occurring Before the Grand Jury	DIOG 11.9, 11.9.1, 18.5.9, 18.6.5
MIOG II	Section 2	2-9.5.2 Physical Evidence and Statements	DIOG 18.5.9, 18.6.5
MIOG II	Section 2	2-9.6 Documentation of Disclosures of Grand Jury Material	DIOG 18.5.9, 18.6.5
MIOG II	Section 2	2-9.6.1 Documentation of Internal Disclosures of Grand Jury Material	DIOG 18.5.9, 18.6.5
MIOG II	Section 2	2-9.7 Storage of Grand Jury Material	DIOG 11.9, 11.9.1, 18.5.9, 18.6.5
MIOG II	Section 2	2-9.8 Requests for Subpoenas in Fugitive Investigations	DIOG 11.9, 11.9.1, 18.5.9, 18.6.5
MIOG II	Section 4	S4 Juveniles and Juvenile Delinquency Act	DIOG 19
MIOG II	Section 4	4-1 GENERAL STATEMENT	DIOG 19
MIOG II	Section 4	4-1.1 Purpose of Act	DIOG 19
MIOG II	Section 4	4-2 SPECIFIC PROVISIONS OF THE ACT	DIOG 19
MIOG II	Section 4	4-2.1 Definitions	DIOG 19
MIOG II	Section 4	4-2.2 Arrest Procedure	DIOG 19
MIOG II	Section 4	4-2.2.1 Advice of Rights	DIOG 19

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

Part	Section	Section Title	DIOG Supersession
MIOG II	Section 4	4-2.2.2 Notification of USA and Juveniles Parents	DIOG 19
MIOG II	Section 4	4-2.2.3 Fingerprinting and Photographing	DIOG 19
MIOG II	Section 4	4-2.2.4 Press Releases	DIOG 19
MIOG II	Section 4	4-2.2.5 Interviews of Juveniles	DIOG 18
MIOG II	Section 4	4-2.2.6 Initial Appearance Before Magistrate	DIOG 19
MIOG II	Section 4	4-2.3 Detention	DIOG 19
MIOG II	Section 4	4-2.4 Prosecution	DIOG 19
MIOG II	Section 4	4-2.5 Use of Juvenile Records	DIOG 19
MIOG II	Section 6	6-2.1 Statements of All Witnesses, Such as FD-302s	DIOG 18.5.6.4.15
MIOG II	Section 6	6-5.1 Statements of All Witnesses, Such as FD-302s	DIOG 18.5.6.4.15
MIOG II	Section 7	S7 Interviews	DIOG 18.5.6
MIOG II	Section 7	7-1 USE OF CREDENTIALS FOR IDENTIFICATION	DIOG 18.5.6
MIOG II	Section 7	7-2 THOROUGHNESS, PRECAUTIONS, TELEPHONIC AND USE OF INTERPRETERS	DIOG 18.5.6
MIOG II	Section 7	7-2.1 Thoroughness and Precautions During Interviews	DIOG 18.5.6
MIOG II	Section 7	7-2.2 Telephone Interviews	DIOG 18.5.6
MIOG II	Section 7	7-2.3 Use of Interpreters	DIOG 18.5.6
MIOG II	Section 7	7-3 REQUIRING FBIHQ AUTHORITY	DIOG 18.5.6
MIOG II	Section 7	7-4 ONE VS TWO AGENT INTERVIEW OF SECURITY SUBJECT	DIOG 18.5.6
MIOG II	Section 7	7-5 EVALUATION OF AN INTERVIEW	DIOG 18.5.6
MIOG II	Section 7	7-6 INTERVIEWING COMPLAINANTS AND SUBJECTS OF CRIMINAL	DIOG 18.5.6
MIOG II	Section 7	7-6.1 Interviews of Complainants	DIOG 18.5.6

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

Part	Section	Section Title	DIOG Supersession
MIOG II	Section 7	7-6.2 Subjects of Criminal Investigations	DIOG 18.5.6
MIOG II	Section 7	7-7 DEVELOPMENT OF DEROGATORY INFORMATION DURING INTERVIEWS	DIOG 18.5.6
MIOG II	Section 7	7-8 IDENTIFICATION OF SUSPECTS	DIOG 18.5.6
MIOG II	Section 7	7-9 INTERVIEWS INVOLVING OR RELATING TO COMPLAINTS	DIOG 18.5.6 and 5
MIOG II	Section 7	7-9.1 Complaints Received at the Field Office	DIOG 18.5.6 and 5
MIOG II	Section 7	7-9.2 Complaints in Person or by Telephone	DIOG 18.5.6 and 5
MIOG II	Section 7	7-9.3 Complaints By Letter	DIOG 18.5.6 and 5
MIOG II	Section 7	7-9.4 Complaints Critical of the FBI or Its Employees	DIOG 18.5.6 and 5
MIOG II	Section 7	7-9.5 Legal Requirements of the Privacy Act of 1974 (Title 5, USC, Section 552a)	DIOG 14
MIOG II	Section 9	S9 Surveillances	DIOG 18.5.8
MIOG II	Section 9	9-1 GENERAL GUIDELINES	DIOG 18.5.8
MIOG II	Section 9	9-1.1 Surveillance Restrictions	DIOG 18
MIOG II	Section 9	9-7.5 Surveillance Logs	DIOG 3
MIOG II	Section 10	S10 Records Available and Investigative Techniques	DIOG 18
MIOG II	Section 10	10-1 INTRODUCTION	DIOG 18
MIOG II	Section 10	10-2 RECORDS AVAILABLE	DIOG 18
MIOG II	Section 10	10-3 INVESTIGATIVE TECHNIQUES	in-part DIOG 18
MIOG II	Section 10	10-6 MAIL COVERS	DIOG 18.6.10
MIOG II	Section 10	10-6.1 United States Postal Service (USPS) Regulations	DIOG 18.6.10
MIOG II	Section 10	10-6.2 Policy	DIOG 11.3, 18.6.10
MIOG II	Section 10	10-6.3 Requesting Approval	DIOG 11.3, 18.6.10
MIOG II	Section 10	10-6.3.1 Fugitive or Criminal Cases	DIOG 18.6.10

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

Part	Section	Section Title	DIOG Supersession
MIOG II	Section 10	10-6.3.2 National Security Cases	DIOG 18.6.10
MIOG II	Section 10	10-7 STOP NOTICES	DIOG
MIOG II	Section 10	10-7.1 Definition	DIOG
MIOG II	Section 10	10-7.2 Placement of Stops	DIOG
MIOG II	Section 10	10-7.3 Indexing Stops	DIOG
MIOG II	Section 10	10-7.4 Removal of Stops	DIOG
MIOG II	Section 10	10-7.5 Types of Stops	DIOG
MIOG II	Section 10	10-7.5.1 Savings Bonds	DIOG
MIOG II	Section 10	10-7.5.2 Immigration and Naturalization Service (INS)	DIOG
MIOG II	Section 10	10-7.5.3 Bureau of Prisons	DIOG
MIOG II	Section 10	10-8 STORED WIRE AND ELECTRONIC COMMUNICATIONS AND TRANSACTIONAL RECORDS ACCESS	DIOG 18.6.8
MIOG II	Section 10	10-8.1 Compelled Disclosure of the Contents of Stored Wire or Electronic Communications	DIOG 11.12, 18.6.8
MIOG II	Section 10	10-8.2 Access to Transactional Information	DIOG 18.6.8
MIOG II	Section 10	10-8.3 Access to and Use of Electronic Communications Located on the Internet, E-Mail, and Bulletin Board Systems	DIOG 18.6.8
MIOG II	Section 10	10-8.3.1 Definitions	DIOG 18.6.8
MIOG II	Section 10	10-8.3.2 Interception of Electronic Communications	DIOG 11.12, 18.6.8
MIOG II	Section 10	10-8.3.3 Undercover Use of the Internet	DIOG 18.6.8
MIOG II	Section 10	10-8.4 Monitoring the Internet	DIOG 18.6.8
MIOG II	Section 10	10-9 ELECTRONIC SURVEILLANCE (ELSUR) PROCEDURES AND REQUIREMENTS	DIOG 11.12, 18.7.2
MIOG II	Section 10	10-9.1 Definitions	DIOG 11.6.4 and 5, 18.7.2

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

Part	Section	Section Title	DIOG Supersession
MIOG II	Section 10	10-9.2 Instructions for Maintaining ELSUR Indices	Appendix H
MIOG II	Section 10	10-9.3 Requests for ELSUR Checks	Appendix H
MIOG II	Section 10	10-9.4 ELSUR Searching Procedures	DIOG 11.6.6, 18.7.2, Appendix H
MIOG II	Section 10	10-9.5 Transmitting ELSUR Material to FBIHQ	
MIOG II	Section 10	10-9.6 Retention of ELSUR Files and Related Records	DIOG 3.3
MIOG II	Section 10	10-9.8 Marking File Cover "ELSUR":	DIOG 18.7.2
MIOG II	Section 10	10-9.8.2 Removable Recording Media	DIOG 18.7.2
MIOG II	Section 10	10-9.9 Recordkeeping Procedures for ELSUR Information Generated Through Joint FBI Operations	DIOG 18.7.2
MIOG II	Section 10	10-9.10 Electronic Surveillance - Title III Criminal Matters	DIOG 11.12, 18.7.2
MIOG II	Section 10	10-9.11 Emergency Provisions, Title III Criminal Matters	DIOG 18.7.2 and 05/22/2008 memo
MIOG II	Section 10	10-9.11.1 Form 2 Report	DIOG 18
MIOG II	Section 10	10-9.11.2 Completion of Form 2 Report	DIOG 18
MIOG II	Section 10	10-9.11.3 Submissions of Form 2 Report to FBIHQ	DIOG 18
MIOG II	Section 10	10-9.11.4 Supplemental Form 2 Reports	DIOG 18
MIOG II	Section 10	10-9.12 ELSUR Indexing in Title III Criminal Matters	DIOG 18
MIOG II	Section 10	10-9.13 Marking of Recordings for Identification	DIOG 18
MIOG II	Section 10	10-9.14 Loan of Electronic Surveillance Equipment to State and Local Law Enforcement Agencies	DIOG 12
MIOG II	Section 10	10-9.15 Submission of Recordings	DIOG 18

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

Part	Section	Section Title	DIOG Supersession
MIOG II	Section 10	10-9.16 Transcription of Recordings	DIOG 18
MIOG II	Section 10	10-10 CONSENSUAL MONITORING - CRIMINAL MATTERS	DIOG 18.6.1, 18.6.2
MIOG II	Section 10	10-10.1 Use of Consensual Monitoring in Criminal Matters	DIOG 11.5, 18.6.1, 18.6.2
MIOG II	Section 10	10-10.2 Monitoring Telephone Conversations in Criminal Matters	DIOG 11.5, 18.6.1, 18.6.2
MIOG II	Section 10	10-10.2.1 Access to Recordings and Information Concerning Monitored Inmate Telephone Calls in Federal Prisons	DIOG 11.5, 18.6.1, 18.6.2
MIOG II	Section 10	10-10.3 Monitoring Nontelephone Communications in Criminal Matters	DIOG 11.5, 18.6.1, 18.6.2
MIOG II	Section 10	10-10.4 Monitoring Communications with Persons Outside the United States	DIOG 11.5, 18.6.1, 18.6.2
MIOG II	Section 10	10-10.5 ELSUR Indexing in Consensual Monitoring Matters	DIOG 11.5, 18.6.1, 18.6.2
MIOG II	Section 10	10-10.5.1 Administration of ELSUR Records Regarding Informants and Assets	DIOG 11.5, 18.6.1, 18.6.2
MIOG II	Section 10	10-10.6 Use of Consensual Monitoring in National Security Matters	DIOG 11.5, 18.6.1, 18.6.2
MIOG II	Section 10	10-10.7 Pen Registers (Dialed Number Recorder)	DIOG 11.11, 18.6.9
MIOG II	Section 10	10-10.7.1 Emergency Provisions	DIOG 18.6.9
MIOG II	Section 10	10-10.8 Electronic Tracking Devices	DIOG 11.6.3, 18.7.2
MIOG II	Section 10	10-9.8.1	DIOG 18.6.3.9
MIOG II	Section 10	10-10.9 Closed Circuit Television (CCTV) (Video Only) - Criminal Matters	DIOG 18.6.3
MIOG II	Section 10	10-10.9.1 CCTV Authorization - Criminal Matters	DIOG 18.6.3.4-5
MIOG II	Section 10	10-10.9.2 CCTV - ELSUR Records - Criminal Matters	DIOG 18.6.3
MIOG II	Section 10	10-10.9.3 CCTV (Audio and Video) - ELSUR Indexing - Criminal Matters	DIOG 18.6.3

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

Part	Section	Section Title	DIOG Supersession
MIOG II	Section 10	10-10.9.4 CCTV - Preservation of the Original Tape Recording	DIOG 18.6.3.7
MIOG II	Section 10	10-10.10 Media Recorders (Formerly Tape Recorders)	DIOG 18.6.1
MIOG II	Section 10	10-10.11 Radio Monitoring	DIOG 18.6.1
MIOG II	Section 10	10-10.11.1 Paging Devices	DIOG 18.6.1
MIOG II	Section 10	10-10.11.2 Cordless Telephones and Other Types of Radio Monitoring	DIOG 18.6.1
MIOG II	Section 10	10-10.11.3 Cellular Telephones	DIOG 18.6.1
MIOG II	Section 10	10-10.17 Trap-Trace Procedures	DIOG 11.11, 18.6.1
MIOG II	Section 10	10-11 FBI UNDERCOVER ACTIVITIES - CRIMINAL MATTERS	DIOG 18.6.13
MIOG II	Section 10	10-18 FBI PRINCIPLES AND POLICIES FOR ONLINE CRIMINAL INVESTIGATIONS	DIOG Appendix L
MIOG II	Section 10	10-18.1 Online Communications	DIOG Appendix L
MIOG II	Section 10	10-18.2 Monitoring Online Communications	DIOG Appendix L
MIOG II	Section 10	10-18.3 Access to Stored Electronic Information	DIOG Appendix L
MIOG II	Section 10	10-18.4 Record Retention and Dissemination	DIOG 14, Appendix L
MIOG II	Section 10	10-18.5 Undercover Online Communications	DIOG Appendix L
MIOG II	Section 10	10-18.6 International Issues	DIOG Appendix L
MIOG II	Section 10	10-19 HANDLING AND PRESERVATION OF AIRCRAFT-MOUNTED VIDEO AND EVIDENCE	DIOG 11.6.6, DIOG 18.6.3.6
MIOG II	Section 10	10-20 MAJOR CASES	DIOG Appendix K - Major cases
MIOG II	Section 11	S11 Techniques and Mechanics of Arrest	DIOG 19
MIOG II	Section 11	11-1 ARREST TECHNIQUES	DIOG 19

b7E

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

Part	Section	Section Title	DIOG Supersession
MIOG II	Section 11	11-1.1 General	DIOG 19
MIOG II	Section 11	11-1.2 Initial Approach	DIOG 19
MIOG II	Section 11	11-1.3 Search of the Person	DIOG 19
MIOG II	Section 11	11-1.3.1 High-Risk Search-Full-Body Search-Handcuffing	DIOG 19
MIOG II	Section 11	11-1.3.2 Final Search and Collection of Evidence	DIOG 19
MIOG II	Section 11	11-1.4 Transportation of Arrested Persons	DIOG 19
MIOG II	Section 11	11-1.5 Handcuffing	DIOG 19
MIOG II	Section 11	11-2 PROCEDURES FOR ARREST	DIOG 19
MIOG II	Section 11	11-2.1 Arrests and Searches	DIOG 19
MIOG II	Section 11	11-2.1.1 Types of Arrest Warrants	DIOG 19
MIOG II	Section 11	11-2.1.2 Authority to Serve Arrest Warrants	DIOG 19
MIOG II	Section 11	11-2.1.3 Summons and Subpoenas	DIOG 18
MIOG II	Section 11	11-2.1.4 Arrests Without Warrants	DIOG 19
MIOG II	Section 11	11-2.1.5 Forcible Entry	DIOG 19
MIOG II	Section 11	11-2.1.6 Search of the Person	DIOG 19
MIOG II	Section 11	11-2.2.2 Property of Prisoner	DIOG 19
MIOG II	Section 11	11-2.2.3 Removal of Prisoner from the Custody of the U.S. Marshal	DIOG 19
MIOG II	Section 11	11-2.3.2 Medical Attention for Bureau Subjects	DIOG 19
MIOG II	Section 11	11-2.3.3 Arrest of Foreign Nationals	DIOG 19
MIOG II	Section 11	11-4.7.1 Juveniles	DIOG 19
MIOG II	Section 12	12.1.3.1	DIOG 19
MIOG II	Section 12	12-2.1 Deadly Force - Standards for Decisions	DIOG has pdf of policy in Appendix F
MIOG II	Section 13	Section 13	DIOG 18.5.6.4.15.1

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

Part	Section	Section Title	DIOG Supersession
MIOG II	Section 14	14-16.9 Fingerprinting of Juveniles by Federal Agencies under the Violent Crime Control and Law Enforcement Act of 1994 (Hereinafter, the Act)	DIOG 19
MIOG II	Section 16	16-4.1.2 Dialed Number Recorders (Pen Registers)	Paragraph #1, last two sentences only. DIOG 18.6.9
MIOG II	Section 16	16-4.1.3 Consensual Monitoring (Formerly 16-7.4.1)	Paragraphs # 3 and 4 only. DIOG 18.6.1
MIOG II	Section 16	16-4.1.4 Electronic Surveillance - Title III	DIOG 18.7.2
MIOG II	Section 16	16-4.1.5 Electronic Surveillance FISA	DIOG 18.7.3
MIOG II	Section 16	16-4.1.6 Telephone Toll Records	DIOG 18
MIOG II	Section 16	16-4.2.2 Court-Ordered Electronic Surveillance (RCU)	DIOG 18.6.9; 18.7.2; and 18.7.3
MIOG II	Section 16	16-4.2.3 Computing Time for Title III Electronic Surveillance (RCU)	DIOG 18.7.2
MIOG II	Section 16	16-4.2.4 Emergency Electronic Surveillance (RCU)	DIOG 18.6.9; 18.7.2; and 18.7.3
MIOG II	Section 16	16-4.2.5 Roving Electronic Surveillance (RCU)	DIOG 18.7.2 and 18.7.3
MIOG II	Section 16	16-4.3 Consensual Monitoring - Technical Assistance (RCU)	Paragraph # 1, first two sentences only. DIOG 18.6.1 and 18.6.2
MIOG II	Section 16	16-4.4 Electronic Surveillance (ELSUR) Interceptions (RCU)	Paragraph # 1, first sentence only. DIOG 18.7.2 and 18.7.3
MIOG II	Section 16	16-4.4.2 Telecommunications Interceptions - Reporting Requirements (TICTU)	DIOG 18.7.2 and 18.7.3
MIOG II	Section 16	16-4.4.3 Telecommunications - Use of Pen Registers and Traps-Traces (TICTU)	Paragraph # 1 only. DIOG 18.6.9
MIOG II	Section 16	16-4.4.4 Pen Registers and Traps-Traces Reporting Requirements (TICTU)	DIOG 18.6.9
MIOG II	Section 16	16-4.8.1 Authorized Use of Technical Devices in Conducting Physical Surveillances (TTU)	Paragraph # 1, second, third and forth sentences only. DIOG 18

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

Part	Section	Section Title	DIOG Supersession
MIOG II	Section 16	16-4.8.4 Technical Devices in Physical Surveillance - Technical, Practical, and Legal Considerations (TTU)	Paragraph # 1 only. DIOG 18
MIOG II	Section 16	16-4.8.9 Authorized Use of Electronic Tracking and Locating Devices and Techniques (TTU)	DIOG 18
MIOG II	Section 16	16-4.8.12 Tracking - Technical, Practical, and Legal Considerations (TTU)	Paragraph # 1; Paragraph # 2, third sentence; Paragraph # 4, second sentence only. DIOG 18
MIOG II	Section 16	16-4.9 Closed Circuit Television (CCTV) (VSU)	DIOG 18.6.3
MIOG II	Section 16	16-4.13.1 Availability and Control of Technical Equipment	Paragraphs # 2 and 3 only. DIOG 18
MIOG II	Section 16	16-4.13.4 Loan of Electronic Surveillance Equipment	DIOG 12
MIOG II	Section 21	21-12 APPREHENSION OF BUREAU FUGITIVES	Paragraph # 1 only. DIOG 19
MIOG II	Section 21	21-13.4 Policy	Paragraphs # 2 and 3 only. DIOG 19
MIOG II	Section 21	21-20 FUGITIVE INVESTIGATIONS FOR OTHER FEDERAL AGENCIES	Paragraph # 3, new classification 343 replaces 62. DIOG 12.5
MIOG II	Section 21	21-20.1 Fugitive Inquiries Abroad on Behalf of U.S. Marshals Service (USMS)	Paragraph # 4, new classification 343 replaces 62. DIOG 12.5
MIOG II	Section 23	23-2 THE FAIR CREDIT REPORTING ACT	DIOG Appendix M - FCRA
MIOG II	Section 23	23-2.1 Section 1681a. Definitions	DIOG Appendix M - FCRA
MIOG II	Section 23	23-2.2 Section 1681b. Permissible Purposes of Consumer Reports	DIOG Appendix M - FCRA
MIOG II	Section 23	23-2.3 Section 1681f. Disclosures to Government Agencies	DIOG Appendix M - FCRA
MIOG II	Section 23	23-2.4 Section 1681g. Disclosure to Consumers	DIOG Appendix M - FCRA

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

Part	Section	Section Title	DIOG Supersession
MIOG II	Section 23	23-2.5 Section 1681e. Compliance Procedures	DIOG Appendix M - FCRA
MIOG II	Section 23	23-2.6 Summary	DIOG Appendix M - FCRA
MIOG II	Section 23	23-2.7 Penalties	DIOG Appendix M - FCRA
MIOG II	Section 23	23-2.8 Section 1681n, o, q, and r. Civil and Criminal Liability for Willful or Negligent Noncompliance	DIOG Appendix M - FCRA
MIOG II	Section 23	23-3.1 Information Desired from Outside the Field Office Territory	DIOG 18.1.4, Appendix J
MIOG II	Section 23	23-4.4 Interviews in Foreign Countries	DIOG 18
MIOG II	Section 23	23-4.10 Extraterritorial Investigative Activity	DIOG 11.5, 18.6.1, 18.6.2
MIOG II	Section 23	23-6 TITLE XI, RIGHT TO FINANCIAL PRIVACY ACT OF 1978 (RFPA)	DIOG Appendix O - RFPA
MIOG II	Section 23	23-6.1 Statute	DIOG Appendix O - RFPA
MIOG II	Section 23	23-6.2 Access to Financial Records	DIOG Appendix O - RFPA
MIOG II	Section 23	23-6.2.1 Intent	DIOG Appendix O - RFPA
MIOG II	Section 23	23-6.2.2 Methods Available to FBI	DIOG Appendix O - RFPA
MIOG II	Section 23	23-6.2.3 Methods Not Available to FBI	DIOG Appendix O - RFPA
MIOG II	Section 23	23-6.3 Definitions	DIOG Appendix O - RFPA
MIOG II	Section 23	23-6.3.1 Financial Institution	DIOG Appendix O - RFPA
MIOG II	Section 23	23-6.3.2 Financial Record	DIOG Appendix O - RFPA
MIOG II	Section 23	23-6.3.3 Government Authority	DIOG Appendix O - RFPA

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

Part	Section	Section Title	DIOG Supersession
MIOG II	Section 23	23-6.3.4 Customers Covered	DIOG Appendix O - RFPA
MIOG II	Section 23	23-6.3.5 Law Enforcement Inquiry	DIOG Appendix O - RFPA
MIOG II	Section 23	23-6.4 Responsibility of Financial Institutions	DIOG Appendix O - RFPA
MIOG II	Section 23	23-6.5 Certification of Compliance	DIOG Appendix O - RFPA
MIOG II	Section 23	23-6.6 Methods of Access	DIOG Appendix O - RFPA
MIOG II	Section 23	23-6.6.1 Customer Authorization	DIOG Appendix O - RFPA
MIOG II	Section 23	23-6.6.2 Search Warrants	DIOG Appendix O - RFPA
MIOG II	Section 23	23-6.6.3 Formal Written Request	DIOG Appendix O - RFPA
MIOG II	Section 23	23-6.6.4 Judicial Subpoena	DIOG Appendix O - RFPA
MIOG II	Section 23	23-6.6.5 Grand Jury Subpoena	DIOG Appendix O - RFPA
MIOG II	Section 23	23-6.7 Customer Notice	DIOG Appendix O - RFPA
MIOG II	Section 23	23-6.7.1 Contents of Notice	DIOG Appendix O - RFPA
MIOG II	Section 23	23-6.7.2 Delay of Notice	DIOG Appendix O - RFPA
MIOG II	Section 23	23-6.8 Customer Challenges	DIOG Appendix O - RFPA
MIOG II	Section 23	23-6.9 Emergency Access	DIOG Appendix O - RFPA
MIOG II	Section 23	23-6.10 Exceptions to RFPA	DIOG Appendix O - RFPA
MIOG II	Section 23	23-6.10.1 Financial Institutions	DIOG Appendix O - RFPA

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

Part	Section	Section Title	DIOG Supersession
MIOG II	Section 23	23-6.10.2 Corporations or Other Legal Entities	DIOG Appendix O - RFPFA
MIOG II	Section 23	23-6.10.3 Not Identifiable with Customer	DIOG Appendix O - RFPFA
MIOG II	Section 23	23-6.10.4 Parties in Interest	DIOG Appendix O - RFPFA
MIOG II	Section 23	23-6.10.5 Federal Grand Jury	DIOG Appendix O - RFPFA
MIOG II	Section 23	23-6.10.6 Foreign Counterintelligence	DIOG Appendix O - RFPFA
MIOG II	Section 23	23-6.10.7 Telephone Company Toll Records	DIOG Appendix O - RFPFA
MIOG II	Section 23	23-6.10.8 Other	DIOG Appendix O - RFPFA
MIOG II	Section 23	23-6.11 Dissemination of Information	DIOG Appendix O - RFPFA
MIOG II	Section 23	23-6.11.1 To Department of Justice	DIOG Appendix O - RFPFA
MIOG II	Section 23	23-6.11.2 To Other Departments	DIOG Appendix O - RFPFA
MIOG II	Section 23	23-6.12 Penalties	DIOG Appendix O - RFPFA
MIOG II	Section 23	23-6.12.1 Civil	DIOG Appendix O - RFPFA
MIOG II	Section 23	23-6.12.2 Disciplinary Action	DIOG Appendix O - RFPFA
MIOG II	Section 23	23-6.12.3 Other	DIOG Appendix O - RFPFA
MIOG II	Section 23	23-6.13 Cost Reimbursement	DIOG Appendix O - RFPFA
MIOG II	Section 23	23-6.14 Reporting Requirements	DIOG Appendix O - RFPFA
MIOG II	Section 23	23-6.14.1 Dissemination of Information Obtained	DIOG Appendix O - RFPFA

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

Part	Section	Section Title	DIOG Supersession
MIOG II	Section 23	23-6.14.2 Statistical Reporting	DIOG Appendix O - RFPA
MIOG II	Section 28	28-1 ATTORNEY GENERAL'S GUIDELINES ON METHODS OF OBTAINING DOCUMENTARY MATERIALS HELD BY THIRD PARTIES	DIOG Appendix C
NFIPM	Section 1	01-2: (U) The National Security List	DIOG Appendix G
NFIPM	Section 1	01-3: (U) Acronyms	DIOG Appendix P
NFIPM	Section 1	01-4: (U) File Classifications and Alpha Designations for Investigative and Administrative Activities Which Uniquely Fall Within the Purview of the FBI's National Foreign Intelligence Program	CPD #0015D. See RPO web-page.
NFIPM	Section 2	02-1: (U) General Investigative and Administrative Activities	Appendix M for definitions: #2, 6, 7, 10, 12, 14, 15, 18, 19, 20, 25, 26 and 27.
NFIPM	Section 2	02-2: (U) National Security Investigations	DIOG 5, 6, 7, 8, 9
NFIPM	Section 2	02-3: (U) Summary Guidance and Applicability of Threat Assessments	DIOG 5
NFIPM	Section 2	02-4: (U) Summary Guidance and Applications for Preliminary Investigations	DIOG 6, 18
NFIPM	Section 2	02-5: (U) Summary Guidance and Application for Full Investigations (FI)	DIOG 7, 8, 9, 18
NFIPM	Section 2	02-6: (U) Collection of Foreign Intelligence	DIOG 9
NFIPM	Section 2	02-8: (U) Office of Origin	DIOG 14
NFIPM	Section 2	02-9: (U) Physical and Photographic Surveillances	DIOG 18.5.8
NFIPM	Section 2	02-10: (U) Interviews in National Security Investigations	DIOG 18.5.6
NFIPM	Section 2	02-11: (U) Education Records (Buckley Amendment)	DIOG Appendix I
NFIPM	Section 2	02-12: (U) Polygraph Examinations	DIOG 18.6.11
NFIPM	Section 2	02-14: (U) 	DIOG 19.2 and Appendix G

b7E

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

Part	Section	Section Title	DIOG Supersession
NFIPM	Section 2	02-15: (U) Physical Searches in Which a Warrant is Not Required	DIOG 11.4, 18.6.12
NFIPM	Section 2	02-16: (U) Monitoring Devices Which Do Not Impose Upon Reasonable Expectations of Privacy	DIOG 18.6.3
NFIPM	Section 2	02-17: (U) National Security Letters (NSL)	DIOG 11.9-11.9.3, 18.6.6
NFIPM	Section 2	02-19: (U) Business Records	DIOG 18.6.7
NFIPM	Section 2	02-21: (U) Mail Covers	DIOG 11.3, 18.6.10
NFIPM	Section 2	02-22: (U) Operations Conducted Outside the United States [REDACTED]	See IPO MOU Library
NFIPM	Section 2	02-23: (U) The Role of Legal Attaches in Foreign Counterintelligence, Foreign Intelligence and Counterterrorism Investigations	See CD PG
NFIPM	Section 2	02-24: (U) Otherwise Illegal Activities	DIOG 17
NFIPM	Section 2	02-25: (U) Arrests, Interdictions, Demarches and Declarations	DIOG 19 - Arrest Procedure
NFIPM	Section 2	02-29: (U) Laboratory Assistance	See Lab web-page
NFIPM	Section 2	02-32: (U) [REDACTED]	DIOG 19.3, 19.4 and appendix G -12.C
NFIPM	Section 2	02-33: (U) [REDACTED] [REDACTED]	DIOG Appendix G - 12.C
NFIPM	Section 2	02-34: (U) Special Surveillance Group (SSG) Program	DIOG 18.5.8
NFIPM	Section 2	02-35: (U) The Behavioral Analysis Program (BAP)	DIOG 19.4
NFIPM	Section 2	02-36: (U) Investigations of Current and Former Department of State Personnel, and Diplomatic Missions Personnel Abroad	DIOG 10, generally
NFIPM	Section 2	02-37: (U) Investigations of Current and Former Central Intelligence Agency Personnel	DIOG 10, generally

b7E

b7E

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

Part	Section	Section Title	DIOG Supersession
NFIPM	Section 2	02-38: (U) Investigations of Current and Former Military and Civilian Department of Defense Personnel	DIOG 10, generally
NFIPM	Section 2	02-39: (U) Investigations of Current and Former Department of Energy Personnel	DIOG 10, generally
NFIPM	Section 2	02-40: (U) Investigations of Other Government Agency Personnel	DIOG 10
NFIPM	Section 2	02-41: (U) Investigations of White House Personnel	DIOG 10
NFIPM	Section 2	02-42: (U) Investigations of Presidential Appointees	DIOG 10
NFIPM	Section 2	02-43: (U) Investigations of Members of the Judiciary	DIOG 10
NFIPM	Section 2	02-44: (U) Investigations of Members of the U.S. Congress and their Staffs	DIOG 10
NFIPM	Section 2	02-45: (U) Disseminating Information to Other Agencies in the Federal Government	DIOG 12.4/DIOG 14
NFIPM	Section 2	02-47: (U) Disseminating Information to Congressional Committees	DIOG 12.4 and 14.3(A)(4)
NFIPM	Section 2	02-48: (U) Disseminating Information to the Federal Judiciary	DIOG 12.4
NFIPM	Section 2	02-49: (U) Disseminating Information to the White House	DIOG 12.4 and 14.5
NFIPM	Section 2	02-50: (U) Disseminating Information to Foreign Governments and Investigations at their Behest	DIOG 12.4/DIOG 14.5
NFIPM	Section 2	02-51: (U) Disseminating Information to State and Local Government Agencies	DIOG 12 and 14
NFIPM	Section 2	02-52: (U) Disseminating Information to the Private Sector	DIOG 14.3 (A)(6-8)
NFIPM	Section 2	02-54: (U) [REDACTED] [REDACTED]	See IIIA web-page
NFIPM	Section 2	02-56: (U) Intelligence Oversight Board Matters	DIOG 4/DIOG 18.6.6 (Re: NSLs) and CPD 0188PG

b7E

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

Part	Section	Section Title	DIOG Supersession
NFIPM	Section 2	02-57: (U) Alpha Designations	CPD #0015D. See RPO web-page.
NFIPM	Section 3	03-1: (U) Consensual Monitoring	DIOG 11.5, 18.6.1
NFIPM	Section 3	03-2: (U) Volunteered Tape Recordings	DIOG 6.9(B)(7), 18.5.7
NFIPM	Section 3	03-4: (U) Pen Registers and Trap and Trace Devices	DIOG 11.11-11.12, 18.6.9
NFIPM	Section 3	03-5: (U) Unconsented Electronic Surveillance	DIOG 11.12, 18.7.3
NFIPM	Section 3	03-6: (U) Electronic Surveillance Minimization, Logs and Indexing	0137PG
NFIPM	Section 3	03-8: (U) Operational Support to the Intelligence Community	DIOG 12, 12.5, 14.5
NFIPM	Section 3	03-9: (U) Operational Technology Division (OTD) Technical Assistance	CPD #0170D
NFIPM	Section 3	Section 3-10 (U) Operational Technology Division (OTD) Technical Assistance Support to the Intelligence Community	DIOG 12 (generally)
NFIPM	Section 3	03-11: (U) Unconsented Physical Searches	DIOG 11.13, 18.7.1
NFIPM	Section 3	03-12: (U) Tax Return Information	Appendix N - Tax Return Info
NFIPM	Section 3	03-13: (U) Searches of Mail Without Consent	DIOG 18.7.1
NFIPM	Section 3	03-14: (U) Unconsented Physical Search Minimization, Logs and Indexing	DIOG 18.7.1 and SMP PG
NFIPM	Section 4	04-1: (U) The Domain Program	DIOG 5, type 4 assessments generally.
NFIPM	Section 5	05-2: (U) Countries on the Current National Security List	Appendix G
NFIPM	Section 5	05-23: (U) Alpha Designations	CPD #0015D. See RPO web-page.
NFIPM	Section 6	06-12: (U) Alpha Designations	CPD #0015D. See RPO web-page.
NFIPM	Section 8	08-11: (U) Alpha Designations	CPD #0015D. See RPO web-page.

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

Part	Section	Section Title	DIOG Supersession
NFIPM	Section 9	09-8: (U) Alpha Designations	CPD #0015D. See RPO web-page.
NFIPM	Section 11	11-4: (U) Alpha Designations	CPD #0015D. See RPO web-page.
NFIPM	Section 12	12-4: (U) Alpha Designations	CPD #0015D. See RPO web-page.
NFIPM	Section 13	13-4: (U) Alpha Designations	CPD #0015D. See RPO web-page.
NFIPM	Section 14	14-4: (U) Alpha Designations	CPD #0015D. See RPO web-page.
NFIPM	Section 15	15-4: (U) Alpha Designations	CPD #0015D. See RPO web-page.
NFIPM	Section 16	16-13: (U) Alpha Designations	CPD #0015D. See RPO web-page.
NFIPM	Section 18	18-3: (U) Issue Threat Preliminary Investigations	DIOG 6
NFIPM	Section 18	18-4: (U) Issue Threat Full Investigations	DIOG 7
NFIPM	Section 18	18-6: (U) Issue Threat File Numbers	CPD #0015D. See RPO web-page.
NFIPM	Section 19	19-3: (U) Procedural Requirements in International Terrorism Investigations	DIOG 5, 6, 7, 8
NFIPM	Section 19	19-4: (U) Closing International Terrorism Investigations	DIOG 5, 6, 7, 8
NFIPM	Section 19	19-11: (U) The Behavioral Analysis Program	DIOG 19.4
NFIPM	Section 19	19-13: (U) Alpha Designations	CPD #0015D. See RPO web-page.
NFIPM	Section 20	20-9 (U) The Behavioral Analysis Program	DIOG 19.4
NFIPM	Section 20	20-10 (U) Alpha Designations	CPD #0015D. See RPO web-page.
NFIPM	Section 21	21-6: (U) Alpha Designations	CPD #0015D. See RPO web-page.
NFIPM	Section 22	22-2: (U) Alpha Designations	CPD #0015D. See RPO web-page.

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

Part	Section	Section Title	DIOG Supersession
NFIPM	Section 27	Confidential Human Sources Manual	CHSPM
NFIPM	Section 27	Confidential Human Source Validation Standards Manual	CSHVSM
NFIPM	Section 28	Section : 28 (U) Undercover Operations (4)	DIOG and NSUCOPG
NFIPM	Section 28	28-1: (U) UC Operations	DIOG 11.12, 18.6.3, and NSUCOPG
NFIPM	Section 28	28-2: (U) Group I	DIOG 11.12, 18.6.3, and NSUCOPG
NFIPM	Section 28	28-3: (U) Group II	DIOG 11.12, 18.6.3, and NSUCOPG
NFIPM	Section 28	28-4: (U) UC Administrative Matters	DIOG 11.12, 18.6.3, and NSUCOPG
NFIPM	Section 30	30-11: (U) The Behavioral Analysis Program	DIOG 19.4
MAOP I	0-1	Authority of the Director	DIOG 3.2.1
MAOP I	21-7 (6)	Monitoring, documenting and reviewing	DIOG 3.4.D
MAOP II	1-1	SAC and ASAC Supervisory Responsibility	Paragraphs # 2 and # 5. DIOG 3.4.C and Succession and delegation policy
MAOP II	1-1.4 (# 1)	Supervision of Cases	Paragraph # 1 - DIOG 14
MAOP II	1-1.4 (# 2 and # 3 a-f)	Supervisory File Reviews	Paragraph # 2 and # 3 (a-f) - # 2 Supervisory File reviews and # 3 PSAs. DIOG 3.4.D
MAOP II	1-1.5.1	Official Channels	Paragraph (5) b only - superseded by CPD 0152D - FBI Policy Cycle Directive.
MAOP II	1-3.5	Designation of Senior Resident Agent and Alternate	Second and third sentences only - DIOG 3.4.C and succession and delegation policy ____?

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

Part	Section	Section Title	DIOG Supersession
MAOP II	1-3.6	Reporting to HQ City	First and second sentence - file reviews every 90 days: DIOG 3.4.D
MAOP II	1-3.13..2 (1)	Supervision of Investigations	Paragraph (1) - DIOG 3.4.C and succession and delegation policy ____?
MAOP II	1-3.13.3 (all)	Case Reviews	All (paragraphs 1-6) - DIOG 3.4.D
MAOP II	2-3	Indexing	DIOG 14
MAOP II	2-3.1	Purpose	DIOG Appendix J
MAOP II	2-4	Management of Files	DIOG 14
MAOP II	2-4.1	Investigative Files	DIOG 14
MAOP II	2-4.1.1	Serializing	DIOG 14
MAOP II	2-4.1.2	Zero Files	Paragraph (2) only. DIOG 14
MAOP II	2-4.1.3	Double Zero Files	DIOG 14
MAOP II	2-4.1.4	Dead Files - No Pending Investigation	DIOG 14
MAOP II	2-4.1.5	Control Files	Paragraph (1) first four sentences only. DIOG 14
MAOP II	2-4.2	Administrative Files	DIOG 14
MAOP II	2-4.2.1	Noninvestigative Files	DIOG 14
MAOP II	2-4.3.6	Consolidation of Files	DIOG 14
MAOP II	2-4.3.7	Reclassification of Files	DIOG 14
MAOP II	2-5	Case Management - Field Offices	DIOG 14
MAOP II	2-5.1	Opening Cases	Paragraphs 1, 2, 3, 4 (initial paragraph only before sub-letters), 4d, 4e, 4f, and 5 (first sentence only). DIOG various sections

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

Part	Section	Section Title	DIOG Supersession
MAOP II	2-5.1.1	Leads	Paragraph (2), delete "Discretionary Action" leads in first sentence only; and delete 2b. DIOG 14
MAOP II	2-5.2	Status of Cases	DIOG 14
MAOP II	2-5.2.1	Pending Case	DIOG 14
MAOP II	2-5.2.2	Pending Inactive	Paragraphs 2, 2a-c, and 3 only. DIOG 14
MAOP II	2-5.2.3	Referred Upon Completion to the Office of Origin (RUC)	DIOG 14
MAOP II	2-5.2.4	Closed	DIOG 6.11, 7.11, 8.8, 9.12
MAOP II	2-5.2.5	Unaddressed Work	DIOG 14
MAOP II	3-1	FBI Classifications/Sub-classifications and Program Groupings	CPD 0015D. RPO/RAU is now responsible for this area by EC 66F-HQ-1079817 serial 705. Link to RPO web-site. Supersede section 3.1 and all subparts.
MAOP II	3-1.1	FBI Classifications and Subdivided Classifications	only 62D; 62E replaced with new 343 classification. 163 M-U classification added. DIOG 12
MAOP II	3-3 (3c)	Task Force Officers (defined)	DIOG 3.3.2
MAOP II	3-3.2 (1)	Special TURK Recording Procedures (1) Major Cases	#1a-g. DIOG Appendix J-Major Cases
MAOP II	3-4.5 (9 a-g)	Case Count Information (# 9 re: closings)	Paragraph # 9 a-g was supersede by DIOG 6.11; 7.11; 8.8; and 9.12.
MAOP II	3-4.6	Reclassifying Cases and Error Correction	DIOG 6.11.C; 7.11.C; 8.8.C; and 9.12.C

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

Part	Section	Section Title	DIOG Supersession
MAOP II	3-4.8	Criminal Preliminary Inquires	Paragraph #1 only. DIOG Section 6.7 - PIS are authorized for 6 months; extension authorized for 6 additional months by SAC; and FBIHQ SC.
MAOP II	3-4.10 (1)	Spin-off Cases (paragraph #1 - defined)	DIOG 14
MAOP II	3-4.10 (2)	Spin-off Cases (paragraph #2 - who can authorize)	DIOG 5, 6, 7, 8, and 9.
MAOP II	3-4.11(1)	Control Files (Paragraph #1 - defined)	superseded paragraph #1, defined in DIOG 14
MAOP II	3-4.11 (2)	Control Files (Paragraph #2 - leads)	superseded paragraph # 2, DIOG 14
MAOP II	3-4.11 (3)	Control Files (paragraph #3, third sentence only)	delete third sentence only, DIOG 14
MAOP II	9	Dissemination of Information	DIOG 14.3 (generally)
MAOP II	9-3	Information to Be Disseminated	DIOG 14.3, 14.4, 14.5 and 14.6
MAOP II	9-3 (paragraph 1)		DIOG 14.3.A and B
MAOP II	9-3 (paragraph 2)	AG Memo 9/21/2001 - "Disseminating Information to Enhance Public Safety and National Security."	DIOG 14
MAOP II	9-3 (paragraph 3)		DIOG 14.3.A.5
MAOP II	9-3.1	Dissemination to State and Local Criminal Justice and Noncriminal Justice Agencies	DIOG 14.3.A.3
MAOP II	9-3.1.1	Dissemination to State and Local Criminal Justice Agencies	DIOG 14.3
MAOP II	9-3.2	Information Totally Within Jurisdiction of Other Federal Agencies	DIOG 14.4.B
MAOP II	9-3.3	Information within FBI Jurisdiction and of interest to another Federal Agency	DIOG 3.4.E
MAOP II	9-3.4.2	Interested Agency Outside a Field Office Territory	DIOG 12.4

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

Part	Section	Section Title	DIOG Supersession
MAOP II	9-3.4.3	Interested Agency Within a Field Office's Territory	DIOG 12.4
MAOP II	9-3.4.4	Reporting Information Furnished	DIOG 12.4 and 12.5
MAOP II	9-3.5	Method of Dissemination to Outside Agencies	DIOG 12.4 and 12.5
MAOP II	9-3.5.3	Oral Dissemination to Outside Agencies	DIOG 12 and 14, generally
MAOP II	9-3.5.4	Accounting of Dissemination	DIOG 12.4 and 12.5
MAOP II	9-4.2.6	Investigative Activity in Congressional Offices	Interview or CHS - DIOG 18.5.6 and CHSPM
MAOP II	9-4.2.9	Dissemination to the White House Complex	Interview or CHS - DIOG 18.5.6. Paragraph (2) Superseded by AGG-Dom, DIOG and AG Memo WH Contacts
MAOP II	9-6	Major Cases - Dissemination of Information	DIOG Appendix K - Major Cases
MAOP II	9-7	Threat to Life - Dissemination of Information	DIOG 14
MAOP II	9-7.1	Information Concerning Threats Against the President and Other Designated Officials	DIOG 14
MAOP II	9-7.2	Information Concerning Threats, Possible Violence or Demonstrations Against Foreign Establishments or Officials in the US	DIOG 14
MAOP II	9-7.2.1	Information Received Through other Than Technical Surveillance	DIOG 14
MAOP II	9-7.2.2	Information Received Through Technical Surveillance	DIOG 14
MAOP II	9-7.2.3	Miscellaneous	DIOG 14
MAOP II	9-8	Replies to Foreign Police and Intelligence Contacts	DIOG 14
MAOP II	9-8.1	Letterhead Memoranda Prepared by Bureau's Foreign Offices	DIOG 14
MAOP II	9-8.2	Dissemination of Classified Information	DIOG 12, 14

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

Part	Section	Section Title	DIOG Supersession
MAOP II	9-9	Dissemination of Grand Jury Material	DIOG 18.6.5
MAOP II	9-10	Dissemination of Title XI, Right to Financial Privacy Act of 1978	DIOG Appendix O - RFPA
MAOP II	9-13	Dissemination By Field Intelligence Groups	DIOG 14
MAOP II	10-9	General Rules Regarding Recording and Notification of Investigations	Supersede Paragraphs # 1a-c; 2a-c; 5; 6; 7; 9; 10a-c; 11-16; and 23-24. DIOG, various sections.
MAOP II	10-10.9.1	Approval by individuals Delegated to Act on Behalf of Higher Bureau Officials	DIOG 3.4.C
MAOP II	10-12	Notes made During Investigations - Interviews	DIOG 3, 14
MAOP II	10-13, 10-13.1, 10-13.2, 10-13.3, 10-13.4	FD-302	DIOG subsection 18.5.6.4.15.1
MAOP II	1-1.4 (3)	File Review	DIOG 3.4.4.1
MAOP II	2-5.1.4 (a) and (b)	Sub-file	Appendix J 1.5
MAOP II	2-4.1.5 (4)		Appendix J 1.4.4
MAOP II	10-16.2	Office of Origin	DIOG 14
MAOP II	13	FD-302	DIOG subsection 18.5.6.4.15.1
MAOP P1	21-7 (6)	Monitoring, Documenting and Reviewing	Remove second to last and last sentence only. Remove citation to MAOP at the end of Paragraph # 6 and add citation "See DIOG 3.4.4"
N/A	EC		34.D
N/A	EC	Legal Advice and Opinions, Tax Return Information, and Return information Relevant to Terrorism Cases, Ex Parte Orders	Appendix N

b7E

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

Part	Section	Section Title	DIOG Supersession
N/A	EC	[redacted] Tax Return Information Other than Taxpayer Return Information to Terrorism-related Cases; delegation of Authority	Appendix N
N/A	EC	To Provide Guidance on Least Intrusive Techniques in National Security and Criminal Investigations - OGC EC [redacted] 12/20/2007	DIOG 4, 4.1, 4.4, 11.1.1, 18.1.1-2
N/A	EC	Mail Cover Cites - EC dated 12/22/2004	DIOG 11.3, 18.6.10
MIOG II	10-10.17.1, and form	FD-670, Consensual Monitoring - Telephone Checklist	DIOG 11.5, 18.6.1
N/A	form	FD-671, Consensual Monitoring - Non-telephone Checklist	DIOG 11.5, 18.6.1
N/A	EC	Electronic Surveillance - EC dated 12/20/2007	DIOG 11.12, 18.7.2-3
N/A	EC	Civil Liberties and Privacy EC issued by OGC dated 3/19/2004	DIOG 4.1, 6.3, 8.3, 9.3, 15.3
N/A	EC	Civil Liberties and Privacy EC issued by OGC dated 9/8/2005	DIOG 4.1, 7.3
N/A	EC	Least Intrusive Techniques in National Security and Criminal Investigations - EC issued by OGC on 12/20/2007, file number [redacted]	DIOG 4, 4.4, 18.1.1-2
N/A	EC	Protection of First Amendment Rights EC issued by OGC dated 3/19/2004 EC issued by CTD dated 09/01/2004 EC issued by OGC dated 12/05/2003	DIOG 4.2
N/A	EC	FBI National Collection Requirements EC issued by DO dated 01/30/2003	DIOG 5.11
N/A	EC	Retention and Dissemination of Privacy Act Records EC issued by OGC dated 03/19/2004	DIOG 5.13
N/A	EC	Authorized Investigative Methods in Assessments ECs issued by OGC dated 03/19/2004 and 9/18/2005	DIOG 18.3, 18.5
N/A	EC	Authorized Investigative Methods in Full Investigations EC issued by OGC dated 10/29/2003	DIOG 18.3, 18.7

b7E

b7E

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

Part	Section	Section Title	DIOG Supersession
N/A	EC	Federal Grand Jury Subpoena EC issued by OGC dated 06/01/2007	DIOG 18.5.9, 18.6.5
N/A	EC	Administrative Subpoena EC issued by CID dated 06/06/2001	DIOG 18.6.4
N/A	EC	Voluntary Disclosure of Non-Content Customer Records	DIOG 18.6.8
N/A	EC	Definition of Investigative Method EC issued by OGC dated 10/14/2003	DIOG 18.6.9.3
N/A	EC	FISA Review Board for RISA Renewals EC issued by Director's Office dated 02/06/2006	DIOG 18.7.3.1.5.3
N/A	EC	Assistance to Other Agencies EC issued by OGC dated 12/5/2003	DIOG 12
N/A	EC	Emergency Disclosure Provision for Information from Service Providers Under 18 U.S.C. Section 2702(b) - EC issued by OGC 08/25/2005, file number [REDACTED] [REDACTED] and [REDACTED]	DIOG 18
LHSA	7-4.1(7)	Consolidated Legal Handbook for Special Agents Section 7-4.1(7) into Interview Section of DIOG	DIOG 18
N/A	EC	Electronic Recording of Confessions and Witness Interviews -EC issued by OGC on 03/23/2006, file number [REDACTED] and [REDACTED] and EC dated 7/16/11, file [REDACTED]	DIOG 18
N/A	EC	FBI Mandated File Review Process - EC issued by INSD on 07/07/2010, file number [REDACTED]	DIOG 3
N/A	EC	Procedural and Operational Issuance - Guidance for Legislative Corruption - EC issued by CID on 08/08/2006, file number [REDACTED]	DIOG 18
N/A	CPD 0227	Designation of an Acting Official to Issue National Security Letters	DIOG 18.6.6.3
N/A	PD 0242D	Requirement for Written Operations Order- Field Operations	DIOG 19.2.3
N/A	CPN 0382N	Notice, National Security Mail Cover Request Approval Authority	DIOG 18.6.10.5

b7E

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

Part	Section	Section Title	DIOG Supersession
N/A	CPN 00541N	Recordkeeping Policy for ELSUR Administrative Information Resulting from Joint Criminal Investigative Operations	DIOG 18.7.2.13
NA	EC/SAC Memo	March 5, 2003 Director's Memorandum to All Special Agents in Charge Re: Pre-Title III Electronic Surveillance (ELSUR) Search Policy, and the April 14, 2008, All Field Offices EC from IMD, Case ID# [REDACTED] [REDACTED]	Appendix H
N/A	RAP Tool User Guide v1.1	Resource Allocation Planning (RAP) Tool, User Guide v1.1 - delete definition of task force officer and task force member on page 1	DIOG 3

b7E

This Page is Intentionally Blank.

S APPENDIX S: (U) LISTS OF INVESTIGATIVE METHODS

S.1 INVESTIGATIVE METHODS LISTED BY NAME (ALPHABETIZED)

- (U) Administrative subpoenas. (Section 18.6.4)
- (U) CHS use and recruitment. (Section 18.5.5)
- (U) Closed-circuit television/video surveillance, direction finders, and other monitoring devices. (Section 18.6.3)
- (U) Consensual monitoring of communications, including electronic communications. (Section 18.6.1)
- (U) Closed-circuit television/video surveillance, direction finders, and other monitoring devices. (Section 18.6.3)
- (U) Electronic surveillance – FISA and FISA Title VII (acquisition of foreign intelligence information). 18.7.3)
- (U) Electronic surveillance – Title III. (Section 18.7.2)
- (U) FISA Order for business records. (Section 18.6.7)
- (U) Grand jury subpoenas. (Section 18.6.5)
- (U) Grand jury subpoenas – to providers of electronic communication services or remote computing services for subscriber or customer information only in Type 1 & 2 Assessments. (Section 18.5.9)
- (U) Information voluntarily provided by governmental or private entities. (Section 18.5.7)
- (U) Intercepting the communications of a computer trespasser. (Section 18.6.2)
- (U) Interview or request information from the public or private entities. (Section 18.5.6)
- (U) Mail covers. (Section 18.6.10)
- (U) National Security Letters. (Section 18.6.6)
- (U) On-line services and resources. (Section 18.5.4)
- (U) Pen registers and trap/trace devices. (Section 18.6.9)
- (U) Physical Surveillance (not requiring a court order). (Section 18.5.8)
- (U) Polygraph examinations. (Section 18.6.11)
- (U) Public information. (Section 18.5.1)
- (U) Records or information - FBI and DOJ. (Section 18.5.2)
- (U) Records or information - Other federal, state, local, tribal, or foreign government agency. (Section 18.5.3.1)
- (U) Searches that Do Not Require a Warrant or Court Order (Trash Cover, Abandoned Property from a Public Receptacle, Administrative Inventory Search of a Lost/Misplaced Item) and Inventory Searches Generally. (Section 18.6.12)

- (U) Searches – with a warrant or court order. (Section 18.7.1)
- (U) Stored wire and electronic communications and transactional records. (Section 18.6.8)
- (U) Undercover Operations (Section 18.6.13)

S.2 INVESTIGATIVE METHODS LISTED BY ORDER IN DIOG SECTION 18

- 18.5.1 (U) Public information
- 18.5.2 (U) Records or information - FBI and DOJ.
- 18.5.3.1 (U) Records or information - Other federal, state, local, tribal, or foreign government agency.
- 18.5.4 (U) On-line services and resources.
- 18.5.5 (U) CHS use and recruitment.
- 18.5.6 (U) Interview or request information from the public or private entities.
- 18.5.7 (U) Information voluntarily provided by governmental or private entities.
- 18.5.8 (U) Physical Surveillance (not requiring a court order).
- 18.5.9 (U) Grand jury subpoenas – to providers of electronic communication services or remote computing services for subscriber or customer information only in Type 1 & 2 Assessments.
- 18.6.1 (U) Consensual monitoring of communications, including electronic communications.
- 18.6.2 (U) Intercepting the communications of a computer trespasser.
- 18.6.3 (U) Closed-circuit television/video surveillance, direction finders, and other monitoring devices.
- 18.6.4 (U) Administrative subpoenas.
- 18.6.5 (U) Grand jury subpoenas.
- 18.6.6 (U) National Security Letters.
- 18.6.7 (U) FISA Order for business records.
- 18.6.8 (U) Stored wire and electronic communications and transactional records.
- 18.6.9 (U) Pen registers and trap/trace devices.
- 18.6.10 (U) Mail covers.
- 18.6.11 (U) Polygraph examinations.
- 18.6.12 (U) Searches that Do Not Require a Warrant or Court Order (Trash Cover, Abandoned Property from a Public Receptacle, Administrative Inventory Search of a Lost/Misplaced Item) and Inventory Searches Generally.
- 18.6.13 (U) Undercover operations.
- 18.7.1 (U) Searches – with a warrant or court order.

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

18.7.2 (U) Electronic surveillance – Title III

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