Counterintelligence Division
Policy Implementation Guide

Federal Bureau of Investigation

0309PG

August 9, 2010
GENERAL INFORMATION: Questions or comments pertaining to this policy implementation guide can be directed to:

FBIHQ/Counterintelligence Division (CD)
Division Point of Contact: IIC Counterintelligence Program

NOTE: All investigative activity authorized in this document will be carried out in accordance with the DIOG, in particular Section 4 (privacy, civil liberties and least intrusive methods) and Section 3.9 (Operational Program Manager Roles and Responsibilities).

SUPERSESSION INFORMATION: This document supersedes sections of the National Foreign Intelligence Program Manual applicable to counterintelligence. See Appendix B for an extensive list of supersessions.

This document and its contents are the property of the FBI. If the document or its contents are provided to an outside agency, it and its contents are not to be distributed outside of that agency without the written permission of the FBI.
## Table of Contents

1. (U) Scope ................................................................. 1
   1.1. (U) Purpose .......................................................... 1
   1.2. (U) Background .................................................... 1
   1.3. (U) Intended Audience ........................................... 1
   1.4. (U) Investigative Classifications ............................... 1

2. (U) Counterintelligence Division Mission Statement ....... 2
   2.1. (U) Counterintelligence Division Mission .................. 2
   2.2. (U) Counterintelligence Division National Strategy .... 2
   2.3. (U) Counterintelligence Division Counterintelligence Program Operations Plan 3
   2.4. (U) Counterintelligence Division Legal Authorities .... 3
   2.5. (U) Counterintelligence Division Reference and Procedure Guide ................. 3

3. (U) Threat Country and Issue Threat Investigations .......... 4
   3.1. (U) Counterintelligence Investigations in General ........ 4
      3.1.1. (U) Reporting Requirements ............................. 4
      3.1.2. (U) Office of Origin ....................................... 5
   3.2. (U) Issue Threats ............................................... 5
      3.3. (U) Counterintelligence Investigations - Goals and Objectives .......... 8
         3.3.1. (U) Neutralization ..................................... 8
         3.3.2. (U) Recruitments or Penetrations of Foreign Intelligence Services 9
      3.4. (U) Counterintelligence Investigations - Goals and Objectives .......... 9
         3.4.1. (U) Neutralization ..................................... 9
         3.4.2. (U) Recruitments or Penetrations of Foreign Intelligence Services 9
         3.4.3. (U) Neutralization of a Counterintelligence Target ............. 9
         3.4.4. (U) Gathering and Analysis of Data on Targets ............ 9
         3.4.5. (U) Analysis of Collected Information ................. 10
   3.5. (U) Issue Threat Investigations ................................ 10
      3.5.1. (U) Espionage & Economic Espionage .................. 10
         3.5.1.1. (U) Espionage ....................................... 10
         3.5.1.2. (U) Economic Espionage ............................ 10
      3.5.2. (U) Targeting National Information Infrastructure Investigations 10
      3.5.3. (U) Targeting the United States Government ............ 10
   3.6. (U) Country Based Investigations .......................... 10
      3.6.1. (U) Counterintelligence Investigations ................. 10
      3.6.2. (U) Targeting National Information Infrastructure Investigations 10
      3.6.3. (U) Targeting the United States Government ............ 10
      3.6.4. (U) Neutralization ....................................... 10
Counterintelligence Division Policy Implementation Guide

5. (U) Directorate of Intelligence Matters
   5.1. (U) Counterintelligence Division - Directorate of Intelligence (DI) Integration
   5.2. 
   5.3. (U) Other Dissemination Methods
   5.4. 

6. (U) Intelligence Partners
   6.1. (U) Operations
   6.2. (U) The Office of the National Counterintelligence Executive
   6.3. 
   6.4. (U) Immigration and Customs Enforcement/Custums and Border Patrol
   6.5. 
   6.6. 
   6.7. 
   6.8. 

7. (U) CI Strategic Partnership Program
   7.1. (U) CI Strategic Partnership Program
   7.1.1. (U) Implementation of National Counterintelligence Strategy
   7.1.2. (U) Strategic Guidance
   7.1.3. (U) Strategic Partnership Activities
Counterintelligence Division Policy Implementation Guide

7.1.4. (U) Critical National Asset Initiative ................................................................. 182
7.1.5. (U) Counterintelligence Working Groups .......................................................... 182
7.1.6. (U) FBI Support to the Committee on Foreign Investment in the United States 182

List of Appendices

Appendix A: (U) Sources of Additional Information .................................................. A-1
Appendix B: (U) Supersessions ................................................................................. B-1
Appendix C: (U) Glossary ....................................................................................... C-1
Appendix D: (U) Acronyms ..................................................................................... D-1
Appendix E: (U) Types of Investigations ................................................................. E-1
1. (U) Scope

1.1. (U) Purpose

(U) The Counterintelligence Division Policy Implementation Guide (CDPG) establishes the Federal Bureau of Investigation's (FBI) policy for conducting counterintelligence (CI) investigations, and the various methods utilized in investigating those cases. CI investigations address threats related to national security, specifically defined in the Attorney General's Guidelines for Domestic FBI Operations (AGG-Dom) as espionage and other related intelligence activities conducted by, for, or on behalf of foreign powers, organizations, or persons, and other matters determined by the Attorney General (AG), consistent with Executive Order (EO) 12333, or any successor order. (See Corporate Policy Directive 0309D.)

1.2. (U) Background

(U) The AG signed the AGG-Dom on September 29, 2008. The AGG-Dom became effective on December 1, 2008. The formulation of the FBI's general policy implementing these new guidelines required each FBI investigative division to replace existing policy manuals to reflect new policy. As a result, the CDPG supersedes the National Foreign Intelligence Policy Manual (NFIPM) and provides policy guidance and authorized methods specific to CI investigations. The CDPG was validated by the Counterintelligence Division's (CD) policy office through a review of existing CI policies contained within the NFIPM, and in consultation with both CD and field office subject matter experts.

(U) The CDPG is organized into three major sections: 1) CD Mission Statement, Roles and Functional Responsibilities; 2) Country and Issue Threat Investigations Authorized to Execute the CI Mission; and 3) Operational Methods for Use in CI Investigations.

1.3. (U) Intended Audience

(U) This policy implementation guide (PG) is applicable to all FBI personnel, in both field offices and at FBI Headquarters (FBIHQ), engaged in or supporting CI investigations related to threats to national security.

1.4. (U) Investigative Classifications

(U) Current investigative classifications within the CI Program are located on the Intranet site for FBI Classifications.
2. (U) Counterintelligence Division Mission Statement

2.1. (U) Counterintelligence Division Mission

(U) Protecting America from national security threats is the FBI's top priority. The CI program is a critical component of the FBI's overall strategy towards this goal. Accordingly, the CD's mission is to protect the national security of the United States from intelligence threats originating from foreign powers, organizations, or persons. (See AGG-Dom A.2)

(U) The FBI is vested by law and Presidential directive with the primary role in the United States to investigate national security threats, including, but not limited to, CI operations, and to collect foreign intelligence. Pursuant to EO 12333, as amended, the FBI coordinates the U.S. Government's (USG) collection of foreign intelligence through human sources and CI operations within the United States. The FBI is responsible for the integration of U.S. law enforcement and U.S. intelligence community (USIC) efforts to deploy all available means to identify, neutralize, and mitigate national security threats, consistent with U.S. law and Department of Justice (DOJ) policy. (EO 12333 Sect 1.3(b)(20)(A))

(U) The United States faces foreign intelligence threats from both state and non-state actors. The threat from foreign intelligence services is grave, and is increasingly complex and asymmetrical in nature. Foreign intelligence services are dedicated to using all means to obtain information which would enhance their countries' strategic positions and harm U.S. national security. In an effort to effectively address threats to national security, the following policies are in place:

- (U) Domestic Investigations and Operations Guide (DIOG): The DIOG emanates from the guidance established in the AGG-Dom and establishes the fundamental policy for the FBI's operations which are common to all FBI investigative programs: CI, Counterterrorism (CT), Intelligence, Cyber, and Criminal Investigative;
- (U) Counterintelligence Policy Implementation Guide: The CDPG applies operational policy common to all CI programs; and
- (U) CD's Reference and Procedure Guides: Within the CD, and under the direction of the Assistant Director (AD), individual sections and units provide country and program specific guidance. Each individual section and unit will use FBI Intranet sites as repositories for country and program specific reference and informational matters, and procedural and operational guidance.

(U) The CD will execute its mission with the full utilization of the authority available under the AGG-Dom, consistent with the Constitution and laws of the United States.

2.2. (U) Counterintelligence Division National Strategy
(U) The National Security Branch (NSB), FBIHQ, is responsible for oversight of the FBI elements involved in national security investigations and foreign intelligence collection. The Executive Assistant Director (EAD), NSB oversees the activities of the CD, the Counterterrorism Division (CTD), the Directorate of Intelligence (DI), the Weapons of Mass Destruction Directorate (WMDD), and the national security investigative activities of the Cyber Division (CyD). The Director of the Terrorist Screening Center reports directly to the EAD, NSB.

2.3. (U) Counterintelligence Division Counterintelligence Program Operations Plan

2.4. (U) Counterintelligence Division Legal Authorities

(U) Federal statutes, executive orders, treaties and other legal authorities relevant to the CI Program are located on the National Security Law Branch (NSLB) Library on the Office of the General Counsel (OGC), NSLB Intranet site.

2.5. (U) Counterintelligence Division Reference and Procedure Guide

(U) Effective CI operations require substantive knowledge of a wide spectrum of matters concerning several countries and issues which pose a national security threat to the United States.

(U) Each FBI CD unit is responsible for maintaining an FBI Intranet site. While each unit has the authority to design its site for its purposes, each site is required, at a minimum, to contain a link to a Reference and Procedure Guide (R&PG). The R&PG will contain pages detailing the: a) each unit's country and issue specific reference material following a common, standard format; b) each unit's country and issue specific procedural guidance; and c) any other relevant matters the unit deems necessary for effective operations against its target(s) and issue(s).

(U) All CD units are responsible for managing sub-programs and classifications for which they issue guidance to the field. This guidance is typically approved at the CD AD level and disseminated by electronic communication (EC). Each CD unit is responsible for uploading an EC or other appropriate documentation, outlining the elements of the matter and its approval to the R&PG within [blank]. Field agents should review the RP&G of the appropriate unit for current procedures and guidance while working CI matters.

(U) The RP&G shall constitute the authoritative repository for all CD country program and issue specific procedure and guidance.
3. (U) Threat Country and Issue Threat Investigations

3.1. (U) Counterintelligence Investigations in General

The DIOG sets forth the levels of authority required to investigate and neutralize these threats and the required purpose or predication for each level of investigation, whether it is an assessment, preliminary investigation or full investigation. While the authority and predication requirements are discussed below, consult the DIOG and the classified provisions (Part VIII) of the AGG-Dom for a more thorough examination of all relevant issues and policies. All CI investigations must conform to such purposes and predications. The DIOG also lists the investigative methods which may be used at each investigative level. The CDPG lists operational methods particular to the CI program, as well as operational methods which require additional articulation in a classified document.

3.1.1. (U) Reporting Requirements

Assessments have been divided by the DIOG into six distinct types. Requirements regarding initiation, oversight and reporting are unique for each type. (See DIOG Section 5.4.) Compliance with these requirements is mandated and will be subject to periodic scrutiny both internally and outside the FBI.

require a notice to of initiation unless otherwise indicated. The submission of an uploaded EC to the appropriate CD operational unit will constitute compliance with this requirement. notification must be provided to the relevant CD operational unit, in accordance with relevant requirements for the (See DIOG for specific requirements.)

Opening communications shall fully articulate the predication. If activity protected by the First Amendment is relevant to the predication, it shall be discussed, but investigations cannot be predicated solely on First Amendment activity. If protected activity is included, the communication must explain how such activity is related to a threat to the national security. The communication shall also include the status of the target (i.e., a U.S. person [USPER], non-USPER, or unknown). Predication sufficient to justify opening an investigation should be kept at the secret level. If information predating the investigation is classified top secret (TS) or sensitive compartmented information (SCI), the communication should, nevertheless, be written at the secret level and include a sentence indicating that there is TS or SCI material that provides additional predication.

For the initiation of any CD shall provide notice to the (See DIOG for specific requirements.) Should a until the requisite review and authorization has been obtained and notifications are made.
(U/FOUO) The EAD for the NSB must notify the Deputy AG if CD disapproves a field office’s initiation of a relating to a threat to the national security because the predication for the investigation is insufficient, per AGG-Dom and DIOG.

(U) The annual reporting requirement for any (USPER or non-USPER) is an annual comprehensive summary EC prepared and submitted to the CD operational unit with oversight responsibility for the investigation. Failure to submit timely investigation openings or annual reports are not potential Intelligence Oversight Board matters.

3.1.2. (U) Office of Origin

(U) The office of origin (OO) in any given investigation is usually determined by the residence, location, or destination of the subject of the investigation. When special circumstances exist, however, the origin may be assumed by the field office which has the most compelling interest.

Uncertainties are resolved by FBIHQ.

(U) No office should conduct any investigation that could reasonably be expected to impact the OO without prior coordination.

(U) In extremely rare instances may be run by separate OOs, with FBIHQ approval. Each individual office is responsible for adhering to the requirements as outlined in the DIOG and this PG.

(U) With the concurrence of the OO, a field office with current investigative interest in a subject may initiate investigative methods, as deemed appropriate, without opening a separate investigation.

3.2. (U) Issue Threats

A. Issue Threats Defined

(U) Issue threats are activities which pose such threats to U.S. national security interests that CI investigations and/or intelligence gathering activities concerning them are warranted, regardless of the actor’s country affiliation.

(U) The overarching issue threats include:

1. (U) Espionage - encompasses foreign power sponsored or coordinated intelligence activities directed at the U.S. Government (USG), U.S. corporations, U.S. establishments, or USPERs, which involve the identification, targeting, and collection, of U.S. national defense information;
2. (U) Proliferation - foreign power sponsored or coordinated intelligence activities directed at the USG, U.S. corporations, U.S. establishments, or USPERs, which involve the proliferation of weapons of mass destruction including chemical, biological, and/or nuclear weapons, missiles and other delivery systems of those weapons; or the proliferation of sensitive technologies, including advanced conventional weapons;

3. (U) Economic Espionage - foreign power sponsored or coordinated intelligence activities directed at the USG, U.S. corporations, U.S. establishments, or USPERs, which involve the unlawful or clandestine targeting or acquisition of sensitive financial, trade, or economic policy information; proprietary economic information or critical technologies; or the unlawful or clandestine targeting or influencing of sensitive economic policy decisions;

4. (U) Targeting the National Information Infrastructure - foreign power sponsored or coordinated intelligence activities directed at the USG, U.S. corporations, U.S. establishments, or USPERs, which involve the targeting of facilities, personnel, information, or computer, cable, satellite or telecommunications systems, which comprise or are associated with the National Information Infrastructure;

5. (U) Targeting the USG - foreign power sponsored or coordinated intelligence activities directed at the USG, U.S. corporations, U.S. establishments, or USPERs, which involve the targeting of government programs, information, or facilities; the targeting of personnel of the USIC, U.S. foreign affairs, U.S. economic, U.S. financial community or U.S. defense establishment; and related activities of national preparedness;

6. (U) Foreign Intelligence Activities - foreign power sponsored or coordinated intelligence activities conducted in the United States or directed against the USG, U.S. corporations, U.S. establishments, or USPERs, which are not described by or included in any other issue threat.

B. (U) Issue Threat Administration

1. (U) The caption of a communication concerning issue threat investigations shall conform to the following:
   a. (Subject) FCI (foreign counterintelligence) - Espionage (Foreign Power);
   b. (Subject) FCI - Proliferation (Foreign Power);
   c. (Subject) FCI - Economic Espionage (Foreign Power);
2. (U) Issue threat cases are to be characterized, by classification, as follows:

a. Proliferation cases concerning country threats carry the file classifications which specifically pertain to those countries.

b. Economic espionage cases carry both the 284 classification and the corresponding 285 classification.

c. Foreign intelligence activities cases carry the 203 classification.

d. Targeting the National Information Infrastructure cases carry the 203 classification.

e. Targeting the USG cases carry the 203 classification.

3.3. (U) Country Threats

d. (Subject) FCI - Targeting the National Information Infrastructure (Foreign Power);

e. (Subject) FCI - Targeting the USG (Foreign Power);

f. (Subject) FCI - Foreign Intelligence Activities (Foreign Power); and/or

g. (Subject) FCI - (Issue Threat) X (when the foreign power is unknown).
Nevertheless, with prior consultation with the appropriate CD unit and the field office Assistant Special Agent in Charge (ASAC) with program responsibility, a field office supervisory special agent (SSA) may open such an investigation if the following standards have been met:

A. There must be prior consultation between the appropriate CD unit and the field office ASAC with program oversight;

B. The SSA authorizing the opening of the investigation and the ASAC with program responsibility must determine that the investigation is an appropriate use of the division’s resources; and

C. After consultation (e-mail or telephonic consultation is adequate) with the relevant CD unit, the approving SSA may open the investigation, via a summary opening electronic communication (EC) with notification to the CD unit. The EC must memorialize the above consultation with the ASAC and CD unit overseeing the program, and set forth the justification standards, as described in B and C above, for opening the investigation.
3.4. (U) Gathering and Analysis of Data on Targets

(U) Consultation with the ASAC and CD unit means a substantive interactive discussion, oral or written, on the scope, purpose, and justification for the investigation.

3.4. (U) Counterintelligence Investigations - Goals and Objectives

3.4.1. (U) Neutralization

(U) All CI investigations are conducted with the ultimate goal of neutralizing the threat posed.

3.4.2. (U) Recruitments or Penetrations of Foreign Intelligence Services

3.4.3. (U) Neutralization of a Counterintelligence Target

(U) Neutralization of a CI target could involve:

- (S) Criminal prosecution;

3.4.4. (U) Gathering and Analysis of Data on Targets
(U) Espionage Investigations

3.4.5. (U) Analysis of Collected Information

(x/NF) Analyses of collected information provide the basis for investigative decisions. Constructive analyses are the result of continual teamwork among case agents, field supervisors, the CD substantive unit, and other analytical elements at FBIHQ, with the overall investigative goal of neutralizing targets and collecting and disseminating relevant intelligence.

3.5. (U) Issue Threat Investigations

3.5.1. (U) Espionage & Economic Espionage

For the most current and tailored guidance relative to specific countries and programs, consult the R&PG located on the CD substantive unit’s Intranet site.

3.5.1.1. (U) Espionage

A. (U) Espionage Investigations

(U) Espionage and unauthorized disclosures are the two general categories of investigations that fall under espionage investigations. Espionage is defined as “intelligence activity directed toward the acquisition of intelligence through clandestine means.”

(U) Espionage investigations cover a range of conduct and activity generally associated with the clandestine collection and transmittal of national security or national defense information by individuals with access to such information, acting on behalf of or to aid a foreign power. Unauthorized disclosure investigations cover a range of conduct and activity generally associated with the misuse or mishandling of national security or national defense information, which may rise to the level of criminal conduct. (See Title 18 Section 793, 794, 798.)

(U) The term “espionage investigation” is sometimes used in reference to matters in both of these categories. The term “espionage-related investigation” is sometimes used in reference to unauthorized disclosure matters. The espionage classification is administratively covers both categories of investigation.

(U) As part of the FBI’s strategic objective to protect U.S. national security, investigations falling within the espionage classification are among the most important matters for which the FBI has jurisdictional responsibilities. Espionage investigations involve the development of facts; the collection of foreign intelligence and CI information; the acquisition of evidence; and the assessment of threat, risk or damage associated with compromises of classified and/or sensitive U.S. national security or national defense information. Compromise of such information can seriously degrade U.S. military, diplomatic, intelligence, economic, and technological capabilities. Compromise of such information may also endanger the lives of individuals.

(U) The complexities, consequences, and national impact of espionage investigations require priority resource dedication for these matters both in the field and within CD. Because of the serious consequences of compromised classified and/or sensitive USG information, and the direct impact on the personnel and capabilities of the USG, the FBI considers it to be of

SECRET/NOFORN

Counterintelligence Division Policy Implementation Guide
paramount importance that all matters initiated within the espionage classification receive timely and thorough investigation.

(U) These investigations also require close management, oversight, and control. Legal and policy requirements pertaining to espionage matters necessitate CD having an increased level of situational awareness and a greater oversight role compared to other CI and criminal investigations. These requirements necessitate a greater level of reporting from the field to CD. CD provides national-level support and assistance to the field in these investigations. Espionage investigations require close and regular dialogue between CD, the field, and other federal agencies, which are almost always involved in some way. These investigations will always be given high priority in terms of resources and investigative attention. As a matter of FBI policy, no espionage matter can go unaddressed.

(U) Espionage and unauthorized disclosure investigations are conducted under the policies, procedures and requirements of the DIOG and this PG. Espionage and unauthorized disclosure investigations have some unique requirements, which are set forth throughout this section of the PG.

(U) If an espionage case involves as defined by the DIOG additional notification and approval requirements apply.

B. (U) Espionage Investigation Goals and Objectives

1. (U) The general goals for espionage and espionage-related investigations include the following:
   a. (U) Prevent the loss or compromise of classified or sensitive information related to national security, national defense, or critical infrastructure;
   b. (U) Detect espionage at the earliest possible stage, and develop relevant facts and obtain evidence pertaining to such activity;
   c. (U) Neutralize or mitigate espionage and espionage-related activity through criminal prosecutions, administrative actions, and other means;
   d. (U) Identify espionage tradecraft for applying and/or adapting defensive measures, training, and awareness throughout the government, to its contractors, and to scientific research facilities; and
   e. (U) Effectively and expeditiously resolve allegations of espionage and espionage-related activity.

2. (U) Specific investigative objectives will depend on the allegations and facts of each case. There are certain general objectives which should be considered in espionage and espionage-related investigations. The following objectives are furnished for general reference and are not intended to be all-inclusive or equally applicable in all investigations:
   a. (U) Identify the information compromised or placed at risk. This must be done with as much haste and specificity as possible, and shall include the classification

SECRET/NOFORN

Counterintelligence Division Policy Implementation Guide

ACLURM006908
SECRET/NOFORN
Counterintelligence Division Policy Implementation Guide

To determine whether any information compromised, and/or any relevant investigative information which was developed, can be used for prosecution, either in a declassified manner or protected under the Classified Information Procedures Act (CIPA). The field office must consult with FBIHQ to obtain appropriate authority prior to using of any classified or sensitive information in a prosecution. Additionally, all declassification must be handled at FBIHQ.

3. (U) Assessing damage:
C. (U) Initiating Espionage Investigations - Classification

(U) Investigations involving allegations of espionage or unauthorized disclosures, losses or compromises of national defense, national security or classified information, are initiated and conducted within the espionage (65) classification. National defense information does not necessarily have to be classified to establish predication in all cases, but the classification level and specific nature of the information is always an important factor in these investigations.

(U) Questions arise whether an espionage investigation can or should be initiated under another classification. While each case must be evaluated on its own facts and circumstances, it is the FBI's policy that if the investigation involves espionage or unauthorized disclosures; losses or compromises of national defense, national security or classified USG information; or the potential violation of any of the statutes related to espionage, especially when the subject of the investigation is an USPER, the investigation shall be initiated and conducted within the espionage classification and not under another classification.

(U) If an investigation being conducted under another classification subsequently develops information indicative of or alleging espionage, that investigation shall be reclassified as an espionage matter and the Counterespionage Section within CD shall be immediately notified. This policy facilitates consistent program management for espionage investigations and provides for optimal support to the field by those elements of the CD's Counterespionage Section which manage these matters on a regular basis.

D. (U) Espionage Investigation Guidelines
Espionage investigations differ from many other investigations conducted by the FBI since criminal prosecution is not the only goal. The benefits to prosecution must always be weighed.

Conducting an investigation under the authorities and procedures of the AGG-Dom and the DIOG will not preclude the possibility of eventual prosecution.

The requisite balancing of the CI and criminal aspects of these investigations adds to the complexity of the cases. Additionally, there are certain policy and procedural rules which specifically apply to espionage investigations. As a result, collaboration and coordination in these investigations between the field, CI, and the field office should telephonically contact and/or e-mail an EC requesting authorization by CD.

E. (U) Espionage Case Predication and Referrals

Espionage and unauthorized disclosure investigations will normally be initiated and conducted under the DIOG as either:

1. 
2. 
3. 

If an investigation is predicated on a referral from another agency indicating classified information is being, or may have been, disclosed in an unauthorized manner to a foreign power or an agent of a foreign power, the referral and coordination requirements of Section 811 of the Intelligence Authorization Act of 1995 apply. Section 811 requires agencies to immediately report to the FBI if classified information is being, or may have been, disclosed in an unauthorized manner to a foreign power or an agent of a foreign power. Section 811 does not require the FBI to investigate all matters reported pursuant to the statute. It remains the decision of the FBI whether to initiate an investigation based upon a referral. The decision will be based on the totality of the facts and circumstances in each situation.
Specific allegations of espionage or espionage-related activity will be investigated. Referrals from other agencies, however, may not always provide specific allegations of espionage, but instead may furnish a set of facts and circumstances, or indicators, suggesting the possibility of espionage. In those situations, an espionage investigation shall be initiated when information or circumstances indicate espionage activity or unauthorized disclosure, or compromise of classified or national defense information may have occurred.

Absent a specific allegation of espionage or espionage-related activity, a reasonable determination of the same may be based on several factors. Although the following list is not meant to be all-inclusive or limiting in terms of such a determination, such factors may include:

1. 
2. 
3. 
4. 
5. 
6. 
7. 
8. 

A decision whether to initiate an espionage or espionage-related investigation will not be made solely on the basis of the availability of resources within a field office. Due to the high national priority of all matters within this classification, it is FBI policy that espionage matters warranting investigation will not be placed in an unaddressed work status. Field offices requiring additional resources to address espionage matters shall coordinate with CD.
(U) Referrals from other government agencies may come directly to CD or a field office, and must be in writing. If a referral is made directly to a field office, the field office must immediately advise CD of the referral. If the facts in a referral are not sufficient to allow the FBI to make a decision regarding case initiation, additional information should be sought from the referring agency. The decision to initiate an investigation will be made on a case-by-case basis given the known facts. A formal decision on FBI case initiation will normally be made based on a written referral, unless exigent circumstances require an immediate action or response. CD must be immediately notified of any such exigent or emergency circumstances.

(U) Pending a decision on initiating an FBI investigation, any actions contemplated by the referring agency must be coordinated with the FBI prior to implementation, in accordance with Section 811. After a referral is made, CD will formally request the referring agency hold in abeyance any further investigation or action by that agency in order not to prejudice a potential FBI investigation and/or criminal prosecution. The local FBI field office will make the same request of the local branch of the referring agency. The referring agency should also be requested to provide the FBI with the results of any investigation already conducted in the matter. Once a decision is made to initiate an FBI investigation based on a referral, the referring agency will be advised to discontinue any ongoing internal security or administrative inquiries and consult with the FBI regarding courses of action. The FBI and the referring agency will coordinate activities in compliance with the requirements of Section 811.

(U) If a field office decides not to initiate an investigation on a...

(U) If an FBI investigation is not initiated...

The referring agency will also be advised if any additional information is developed which would affect the FBI’s determination, those facts should also be promptly communicated to the FBI within the 65 classification.

F. (U)
(U) Case predication standards, authorized techniques, and reporting requirements for espionage-related investigations and are addressed in the DIOG. Authorization levels for opening as those set forth in DIOG ——— apply to espionage and within the espionage classification are the same.

1. (U) Case Code Words
   a.
   b.

G. (U) Case Code Words
   X
   X
   X

H. (U) and Non-Disclosure Agreements
   the code word of the investigation is usually not classified

ACLURM006914
(U) Field offices are encouraged to create and maintain...

I. (U) Reporting Requirements for Espionage Investigations

(U) Because of interagency coordination and notification requirements imposed on the FBI by statute and interagency agreements, and CD's need for timely information about ongoing espionage investigations, there are certain reporting requirements within this classification, set forth below, which exceed the basic reporting and notifications required by the DIOG.

1. (U) Notification of Investigation
   a. (U) Within _______ of the initiation of an investigation, the field office is required to provide a cover EC, with an enclosed Letterhead Memorandum (LHM), to the pertinent unit in the Counterespionage Section of CD. Field offices shall refer to separate guidance or instruction from the Counterespionage Section regarding any prescribed format for an initial case-opening notification LHM.
   b. (U) The Counterespionage Section will provide the opening LHM if necessary under the AGG-Dom and within _______ of receipt of the LHM.

2. (U) Status Report
   a. (U) A _______ in an LHM format, shall be submitted to CD every _______ after the date of the initiation of any espionage investigation. This is a CD requirement unique to espionage cases. The purpose of the _______ is to provide CD with regular updates on investigative activities, and the means to appropriately disseminate information to other agencies as required by statute.
ii. (U) CD will disseminate the information normally be disseminated to the headquarters of the affected agency or agencies. CD will advise the O0, upon dissemination of a lead shall be set by the field office to the respective counterespionage unit, to distribute the information to the

iii. (U) As with any disseminable LHM, containing third-agency information cannot be disseminated to another agency without the authorization of the originating agency. CD will obtain third agency consent for dissemination of information and/or other disseminated documents or reports. The O0 shall note in the administrative section of its cover EC if there is third-agency information contained in the EC. The administrative section of the cover EC will identify those agencies authorized to receive the information by the third agency. CD shall be made aware of any objections to dissemination by a third agency.

iv. (U) Deviations from these general reporting and dissemination procedures must be approved at the AD level in CD.

3. (U) Status Report Format

(U) Field offices shall send in LHM format to the appropriate unit within the Counterespionage Section in CD. Formats may change from time to time, and field offices are to be familiar with the most current format as prescribed by CD's Counterespionage Section.

(U) The shall provide information of the following nature:

- (U) Date Investigation was Initiated:
  *(U*?) Indicate the type of case, and the date the case was initiated. The date should not be provided in a
  *(U*?) Note: When the date of initiation of the is the not the date that date was initiated.

- (U) Office of Origin:
  *(U)* Provide the name of the field office directing the investigation.

- (U) Basis for the Investigation:
  *(U)* Provide a brief (one paragraph) summary of the case predication. If the paragraph contains TS, CHS, or SCI, it shall be classified appropriately, or an approved summary at a lower classification level must be obtained.

- (U) Investigation During this Reporting Period:
Counterintelligence Division Policy Implementation Guide

(U) Provide details of the investigation conducted over the previous period. Details should include the outcome of the investigation.

(U) Anticipated Investigation in the Next Period

(U) Provide a summary of the planned investigation for the next period. It is understood the investigation will evolve and plans may change, but this summary should articulate the anticipated direction and objectives for the next period. Long-term objectives should also be considered and noted.

CD must be aware of the investigative direction of the case and be prepared to support it.

(U) Great care and attention should be given to the preparation of materials as they are requested, identity protection, shall be designated by a T-symbol in the material with the T-symbol.

(U) Field offices should consider including a closing paragraph in the cover EC, which contains contact information for the case within the field office. This may include the case agent's and/or the supervisor's name and contact information.

(U) Field offices will prepare a summary of the lead shall be set by the field office in the cover EC, to the respective counterespionage unit.

4. (U) Closing Espionage

(U) Due to the need for heightened control over the closing of espionage matters, consultation between the appropriate CD unit, the field office Assistant Special Agent in Charge (ASAC) with program responsibility, and the field office supervisory special agent (SSA) is required prior to closing all espionage investigations and

Moreover, the proposed field office closing LHM for

will be sent to CD for review by the appropriate Unit Chief to determine whether all logical and appropriate investigative steps have been taken prior to closing a case. This LHM review will form the basis for the CD and field office consultation. As warranted by prior consultation, the closing cover EC, with LHM attachment, will advise that all logical investigation has been conducted and will reference the above-mentioned prior consultation with CD upon closing the case.
(U) The LHM will provide a detailed summary of the entire investigation. The closing LHM shall contain sufficient information about the investigation conducted and the results obtained. In particular, it shall address whether there was a resolution of the pertinent issues which predicated the investigation.

(U) Closing LHMs will be routinely

Usually this will be the same agency or agencies which have been in receipt of during the course of the investigation. It is important to note that recipient agencies, especially those who employ or contract with the subjects of these investigations, will often use and rely on this product to take any appropriate action they deem necessary. Such actions may include personnel actions or administrative sanctions, changes in work assignments, security clearance actions, and terminations. These cases are often briefed at high levels within other agencies after the FBI has concluded its investigation and reported its findings.

An FBI investigation of a government employee or contractor based on a referral or some type of espionage allegation is given a high degree of scrutiny within other government agencies. This is due to the overall significance of espionage and espionage-related allegations, the impact of such activity on these agencies, and the fact that the FBI is the primary agency within the USG that has expertise and responsibility for these types of investigations.

(U) Closure of investigations will be reviewed by the section chief or a designee. Closure of will be reviewed by the unit chief or a designee. If specific agencies request a notification of closing, field offices can set leads in the cover EC for dissemination by CD. CD will

CD will apprise the OO of

J. (U) FBI Internal Investigations

(U)
(U) Authorities for these actions will be obtained through the AD, CD, by the Counterespionage Section. CD will advise the OIC immediately upon notice that the authorizations for the actions noted above have been granted.
(U) When conducting subject interviews and/or subject polygraphs of FBI employees or contractors, it is critical that the attorneys for the field office's chief division counsel (CDC) office, FBIHQ NSLB and Garrity implications. (Note: Garrity vs. New Jersey is a U.S. Supreme Court decision that ruled that when an employer gives an employee the choice of answering questions or losing his/her job, any statements the employee makes are compelled and, therefore, inadmissible in a court of law during a criminal prosecution. As a result, it is imperative that the interviewer consult with the CDC and/or NSLB. Under most circumstances, such statements may be used to take administrative action against the employee.)
L. (U) Unknown Subject and "Umbrella" Espionage Investigations

M. (U) Uploading & Case Restriction Policy for Espionage Cases

(U) All 65 cases will be uploaded according to the policy set forth by the Records Management Division (RMD). Internal 65 investigations have been exempted and are not to be uploaded unless the field is instructed to do so by CD. In cases considered too sensitive to be uploaded, CD has the option of authorizing, in writing, that the case not be uploaded. Field offices may request CD authority to not upload a case, but any case not uploaded must have written authorization by CD's AD documented in the substantive file.
(U) When a case file is closed, restrictions must be manually removed, therefore, justification for the need to continue restrictions shall be submitted by EC to FBIHO and approved by CD’s AD before the case is closed in ACS. (See EC Case 1D Serial 4, “Procedural and Operational Issuances: Automatic and Manual Case Restrictions of Files in ACS - Policy Matter,” dated 5/17/06.)

N. (U) Interviews

(U) There are additional requirements for interviews conducted in espionage and espionage-related matters which are described below.

1. (U) Subject Interviews
   a. (U) CD approval is required for all interviews of the subjects of espionage and espionage-related investigations. In certain instances, CD may have to notify and coordinate issues with DOJ and other agencies.
   b. (U) To obtain CD approval for a subject interview, the field office will send an EC to the Counterespionage Section setting forth the request to interview and providing pertinent details concerning the planned interview. Details about the interview shall include information about whether or not the interview will be custodial. Garrity issues may arise and should be reviewed with the field office’s CDC prior to a subject interview.
   c. (U) CD approvals for subject interviews will be granted for a ___________ If the interview is not conducted during the authorized ___________ another EC must be sent by the field office advising of the reasons the interview was not conducted and requesting another approval and authorization period.
   d. (U) Subject interviews will always be documented on the Form for Reporting Information That May Become the Subject of Testimony (FD-302). Consideration should also be given to obtaining signed statements from subjects, when feasible, necessary, and beneficial.

(a)
(U) Under most circumstances
Counterintelligence Division Policy Implementation Guide

h. (U) After a subject interview is conducted, the field office will send a cover EC to CD’s Counterespionage Section, with a copy of the completed FD-302 form(s) from the interview enclosed. CD will consider the issue of further dissemination of the FD-302 form outside of the FBI and

2. (U) Interviews of non-subjects in espionage investigations will be documented on an FD-302 form, if substantive information is reported

a. (U)

b. (U) In situations where classified information is to be divulged to an interviewee as a result of the interview

3. (U) In all cases, the interview of a journalist or reporter requires AD and

4. (U) If classification of an FD-302 form, insert, or signed statement is necessary, the document shall be properly classified and portion-marked with the classification by paragraph. This will clearly indicate what portions of an interview report are classified and what portions may be unclassified. The inclusion of the subject’s name in a paragraph is not reason alone to classify the paragraph.
(U) National security interests may require the detention or arrest of individuals in order to prevent the transmission or loss of national security information, or the escape of a subject. CD must be apprised, as soon as possible, of any detention and/or arrest of any espionage subject, in particular CD will make the appropriate notifications.

S. (U) Extraterritorial Espionage Investigations, Liaison and Coordination Issues

1. (U) Espionage and espionage-related investigations may require FBI personnel to travel outside the United States for investigative, operational and/or foreign liaison purposes. Pursuant to Public Law 101-193 (Section 603 of the Intelligence Authorization Act of 1990), the FBI has jurisdiction to supervise the conduct of all investigations of violations of the espionage laws of the United States by persons employed by or assigned to U.S. diplomatic missions abroad, including allegations involving foreign service nationals (FSN) employed at U.S. diplomatic missions abroad. In espionage investigations, there may also be occasions when a subject resides or travels outside the United States, and these situations may also necessitate foreign travel by FBI personnel.

2. (U) The International Operations Division (IOD) has established the general policies, approval procedures and coordination requirements for international travel by FBI employees, which must be complied with whenever authority for such travel is requested. These policies and procedures are located on the IOD Intranet site.
4. (U) If international travel is anticipated, it is strongly recommended that the field office discuss this as early as possible with CD's Counterespionage Section before sending a formal request.

5. (U) Formal requests shall reach CD with sufficient time for the necessary authorizations to be obtained. Routine requests shall reach CD a minimum of before the anticipated travel dates. Emergency requests, based only on exigent operational circumstances, will be handled as expeditiously as possible, given the requirements of the authorization process.

6. 

7. 

8. 
Espionage Matters

1. (U) Missing Documents, Computers and Other Classified Data or Storage Media

(U) Other USG agencies occasionally report that items, such as documents, computers, or other data storage media containing classified information, are missing. If such a report is received, a field office should initially conduct an investigation.
pursuant to the DIOG____ in order to determine whether a____ investigation by the FBI is warranted. The initial steps undertaken should include the following:

1. CD must be immediately notified if a field office receives a report of this nature.
2. These situations may require an FBI investigation, if there is reason to believe that the items were taken in an unauthorized manner, may have been compromised, or may have been lost through gross negligence. The nature and classification level of the information may be a factor in determining whether an FBI investigation is warranted.
3. It is important to note that the FBI is not responsible for locating the missing items, especially if the facts suggest the likelihood the items were merely misplaced. The reporting agency should continue its efforts to locate the missing items, and the field office should maintain close contact with the agency to monitor the search activities for any indications of possible criminal or CI interests to the FBI.

V. Reports of Improper Storage or Possession of Classified Information and Other Related Security Issues

1. In addition to reports of missing classified documents or data, other government agencies may report an employee has stored, transmitted or currently possesses classified information in an unauthorized manner. The most common scenario is one in which the employee has classified information at home or has placed it on an unclassified computer or network, although there is no information which suggests the classified information has been otherwise compromised.
2. As with reports of missing items, if such a report is received, a field office should initially conduct a____ pursuant to the DIOG____ in order to...
Counterintelligence Division Policy Implementation Guide

determine whether an investigation by the FBI is warranted. The initial steps undertaken should include the following:

a. (U) Obtain full details from the reporting agency concerning the nature of the classified information;

b. (U) Obtain the identity of any known or suspected employee(s) involved;

c. (U) Ascertain how the reporting agency learned of the situation and the details regarding any ongoing or prior security investigation conducted by the reporting agency; and

d. (U) Determine if the reporting agency contacted or anticipated contacting the FBI in advance with the FBI. The overriding goal should be protection of the classified information and to conduct related internal security investigations. In most cases, however, investigations or inquiries by other agencies are not conducted pursuant to any criminal law enforcement or CI investigative authority, but instead are conducted by agencies pursuant to their security or other administrative authorities.

3. (U) FBIHQ must be immediately notified if a field office receives a report of this nature.

4. (U) As with missing classified documents or storage media, reports of improper storage or possession of classified information or other related security issues may require an FBI investigation in order to determine if classified information has been compromised, is being unlawfully retained, has been or is being communicated in an unauthorized manner, or has been lost through gross negligence.

5. (U) In many of these situations, the reporting agency may have already conducted some level of investigation under its personnel and information security authorities and procedures. USG agencies have the authority, as well as a duty, to protect classified information and to conduct related internal security investigations. In most cases, however, investigations or inquiries by other agencies are not conducted pursuant to any criminal law enforcement or CI investigative authority, but instead are conducted by agencies pursuant to their security or other administrative authorities.

6. (U) When an agency reports such a situation, the FBI may initiate its own investigation, and any further actions by the reporting agency should be coordinated in advance with the FBI. The overriding goal should be protection of the classified information, although in some cases the conduct of the subject may rise to the level of criminal conduct.

7. (U) In these situations the field should be cognizant of any investigative activity that the reporting agency has already conducted or plans to conduct since actions undertaken by the subject's employer may preclude or hinder future prosecution of the subject. Once advised of the facts, CD will

W. (U)
Such determinations are not considered to be

(U) Any documents prepared by any agency which reflect evaluation or commentary ... may be discoverable in litigation. Such documents could adversely affect a prosecution, when done prematurely, if they incorrectly state or characterize the damage done.

(U) Agencies affected by espionage or unauthorized disclosures should be cautioned not to prematurely conduct or document of damage caused by compromises or disclosures under investigation.

3.5.1.2. (U) Economic Espionage

For the most current and tailored guidance relative to specific countries and programs, the reader should also consult the R&PG located on the relevant CD unit's Intranet site.

(U) Economic Espionage Investigations

A. (U) Definition:

(U) Economic espionage is defined by the FBI as intelligence activity coordinated or sponsored by a foreign power directed at the USG, U.S. corporations, U.S. establishments, or USPERs, designed to unlawfully or clandestinely obtain sensitive financial, trade, or economic policy information; proprietary economic information; or critical technologies; or to unlawfully or clandestinely influence sensitive economic policy decisions. The information and/or technologies must be considered trade secrets, in order for a successful case development and prosecution.

B. (U) Objectives of the Economic Counterintelligence and Economic Espionage Program
The National Security Review (NSR) 29, signed by President George H. W. Bush in 1991, specifically tasks the USIC in respect to international economic trends and developments. Its requirements include developing information about what foreign governments are doing to harm the United States (e.g., violating international and/or bilateral agreements; predatory and/or subversive foreign targeting of U.S. industries). The objectives of the include:

1. 
2. 
3. 
4. 
5. 
6. 
7. 
8. Collecting evidence of violations of federal law.

C. Significance

The international environment has changed dramatically since the end of the Cold War and after the terrorist attacks against the United States on September 11, 2001. In this new era, many countries have realized that the key to security and advancement, whether scientific, economic, or military, are in large part, research and development, whether done legitimately or stolen from other states.

Due to its tremendous research and development investments, the United States has been, and will continue to be, a target of economic espionage operations conducted by both adversarial and friendly nations. Think tanks have estimated that the damage to the U.S. economy resulting from these operations is in the hundreds of billions of dollars each year.
D. (U) Background on the Economic Espionage Act of 1996

1. (U) With an ongoing economic threat in mind, Congress held hearings in February and May of 1996. During a joint hearing of the Senate Select Committee on Intelligence and the Senate Committee on the Judiciary in February 1996, former FBI Director Louis Freeh testified that the FBI lacked federal statutes which directly addressed the economic espionage threat. Instead, the FBI primarily relied on several federal statutes to prosecute economic espionage cases, such as the Interstate Transportation of Stolen Property Act, the Mail Fraud Statute, the Fraud by Wire Statute, as well as existing patent laws. Each of these federal laws has significant limitations.

2. (U) On October 11, 1996, President Clinton signed into law the Economic Espionage Act (EEA). The nine sections of this act were inserted into Title 18 of the U.S. Code (USC) to help protect the trade secrets of U.S. companies. Refer to the following sections of Title 18 for information on economic espionage:
   a. (U) Title 18 USC, Section 1831 economic espionage;
   b. (U) Title 18 USC, Section 1832 theft of trade secrets; and
   c. (U) Definitions from the EEA (Section 1839).

E. (U) Jurisdiction

(U) The EEA is not limited to acts within the United States. It protects against acts in furtherance of the offense committed both inside and outside the United States, if there are sufficient links to the United States for federal jurisdiction.

F. (U) Opening

1. (U) All investigations conducted in conjunction with Title 18 USC Section 1831 will be conducted through CD's Counterespionage Section.

2. (U) If during the initial stage of an investigation it is determined no threats exist, then the field office should refer the investigation to the Cyber Division or the field office's cyber program manager, to determine whether it meets the criteria for a 295 investigation.

3. (U) For the use of CD and reporting requirements in 284 refer to DIOG

G. (U) Reporting Requirements for 284

1. (U) The requirements for an opening notification for a 284 are as follows:
   i. (U) Within of the opening of an investigation, a notification LHM must be forwarded to the appropriate CD unit to advise of a case opening, and
the field office is required to set a lead to the same CD unit requesting CD distribution of the accompanying LHM.

ii. (U) A cover EC shall be attached to the notification LHM.

iii. (U) Include an administrative section in the cover EC to identify T symbols, if used, and/or if third agency approval is needed prior to release of sensitive source information to another agency.

b. (U) The requirements for a 284 extension are as follows:

i. (U) The first extension shall be from the opening date of the investigation.

(U) 

ii.

iii. (U) The second extension (one year from the opening date of the investigation) for a 284 are as follows:

b7E

iv. (U) The requirements for additional extensions for a 284 are as follows:

b7E

v. (U) No work may be conducted after an expiration date, until an extension is approved.

iii. (U) The field office must advise, with an EC, any office with outstanding leads of the extension date.
The requirements for a closing notification for a 284 are as follows:

1. The EC shall note all logical leads completed and advise that the case is being closed. If the subject has not been interviewed, reason(s) for not doing so shall be stated.

The requirements for an opening notification for a 284 are as follows:

1. Within of the opening of an investigation, a notification LHM must be forwarded to the appropriate unit in CD's Counterespionage Section to advise of the case opening.

2. A cover EC shall be attached to the notification LHM and its lead shall be set to the same CD unit, requesting CD distribution of the accompanying LHM or USPER).

3. Include an administrative section in the cover EC to identify T symbols if used, and/or if third agency approval is needed prior to release of sensitive source information to another agency.

The requirements to convert a 284 are as follows:

1. Within of converting an investigation, a notification LHM must be forwarded to the appropriate unit in the CD's Counterespionage Section to advise of the case conversion.

2. A cover EC shall be attached to the notification LHM and its lead shall be set to the same CD unit, requesting CD distribution of the accompanying LHM or an USPER).

3. Note: All deadlines are set according to the conversion date, NOT the date of the opening of the

The requirements for a closing notification for a 284 are as follows:
Counterintelligence Division Policy Implementation Guide

i. (U) Within [missing text] of closing the investigation, an LHM must be forwarded to the appropriate unit in the CD's Counterespionage Section summarizing the investigation and case closure. If applicable, consider noting that if new information is obtained, the case will be reviewed and reopened, if deemed appropriate.

ii. (U) A cover EC must be attached to the LHM. The EC will note all logical leads completed and advise the case is being closed. If the subject has not been interviewed, state the reason(s) for not doing so. A lead shall be set to the same CD unit, requesting CD distribution of the accompanying LHM to if appropriate.

H. (U) Subject Interviews

(U) Interviews of economic espionage subjects and non-subjects shall follow the preceding guidelines for interviews in espionage cases, as established in Section 3.5.1.1.N.

I. (U) Field Office Contact with the

(U) Prior to a field office contacting regarding a 284

the field office shall contact the CD

J. (U) General Considerations

K. (U) Investigative Techniques

1. [missing text]
6. (U) In many instances -

2. (U) If the information has already been stolen.

3. (U) In many cases, this may allow the FBI the advantage of -

4. (U) In cases where -

5. (U) The investigating agent should establish whether -

6. (U) In many instances -

7. (U) A significant number of FBI economic espionage investigations progress quickly to

8. (U) The strongly recommends field offices enter their subjects’ names into

9. (U) Prior to a field office of Economic Espionage investigation, the field office shall contact the
   Section requirement is consistent with

L. (U) Protection of Trade Secret Information

(U) During all phases of the investigation, agents should exercise extreme care to protect trade secret information from unauthorized or inadvertent disclosure. The FBI, in conjunction with the DOJ, will make all attempts to protect the victim company’s trade secret information throughout the course of the investigation and subsequent prosecution.

(U) Title 18, USC, Section 1835 states: “In any prosecution or other proceeding under this chapter, the court shall enter such orders and take such other action as may be necessary and appropriate to preserve the confidentiality of trade secrets, consistent with the requirements of the Federal Rules of Criminal and Civil Procedure, the Federal Rules of Evidence, and all other applicable laws. An interlocutory appeal by the United States shall lie from a decision or order of a district court authorizing or directing the disclosure of any trade secret.”

M. (U) Other Statutes

(U) Other criminal statutes may be applicable to the economic espionage cases depending on the facts of the case. These include:
Counterintelligence Division Policy Implementation Guide

1. (U) Title 18, USC, Section 1343 - Wire Fraud;
2. (U) Title 18, USC, Section 1341 - Mail Fraud;
3. (U) Title 18, USC, Section 2314 - Interstate Transportation of Stolen Property;
4. (U) Title 18, USC, Section 1030 - Computer Fraud;
5. (U) Title 17, USC, Section 506 - Copyright Infringement;
6. (U) Title 18, USC, Section 951 - Agents of Foreign Governments;
7. (U) Title 22, USC, Section 2778 - Arms Export Control Act; and

3.5.2. (U)

For the most current and tailored guidance relative to specific countries and programs, the reader should also consult the R&PG located on the relevant CD unit’s Intranet site.

A. (U) CD - Matters - General

5

43
3.5.4. (U) Targeting National Information Infrastructure Investigations

(U) Targeting National Information Infrastructure (TNII) investigations may evolve from the use of any...

(U) Investigations involving the TNII must be coordinated between CD and CyD. A partnership between programs in the field office is highly recommended throughout any TNII investigation, and will likely maximize the operational potential.
(U) Due to the potential for overlap regarding investigations targeting state-sponsored computer intrusions, the CD and CyD have implemented the following procedures:

- (U) Upon initiation of an [redacted] the field office CI squad shall notify the field office cyber squad;
- (U) Upon initiation of either a CI [redacted] a corresponding [redacted] shall be opened by the field office cyber squad; and
- (S) CI [redacted] shall be dual captioned with the case identification numbers and titles of the corresponding [redacted].

3.5.5.
3.5.6. (U) Targeting the United States Government

3.6. (U) Country Based Investigations

(S)

3.6.1. X

(S)
Counterintelligence Division Policy Implementation Guide

(1) Investigating agents should note there are

Employees of Attorney General

ACLURM006944
Counterintelligence Division Policy Implementation Guide

C. (U) Operational Guidance
For the most current and tailored guidance relative to specific countries and programs, the reader should also consult the R&PG located on the relevant CD unit's Intranet site.
Counterintelligence Division Policy Implementation Guide

B. Goals and Objectives

1. 

2. 

3. 

4. 

ACLURM006948
For the most current and tailored guidance relative to specific countries and programs, the reader should also consult the R&PG located on the relevant CD unit's Intranet site.
For the most current and tailored guidance relative to specific countries and programs, the reader should also consult the R&PG located on the relevant CD unit's Intranet site.
Counterintelligence Division Policy Implementation Guide

For the most current and tailored guidance relative to specific countries and programs, the reader should also consult the R&PG located on the relevant CD unit's Intranet site.
A. (U) CD will designate the office of origin (OO);
B. 
C. 

SECRET/NODORNI
Counterintelligence Division Policy Implementation Guide
All non-USPER visa applications after 1995 are available by [redacted]. Many of these visa applications contain accompanying documents which provide additional information regarding the applicant including the applicant's picture, educational and employment history, and letters of invitation/sponsorship that include itineraries, purpose of the visit, and additional sponsor contact information.

A. (U) Students

For the most current and tailored guidance relative to specific countries and programs, the reader should also consult the R&PG located on the relevant CD unit's Intranet site.
A Visitor "student" is a scholar, researcher, or instructor who has entered the United States on an F or J visa. Though many such persons switch to H visas during their stay, if they continue to be enrolled as students, or involved in research, teaching or related activities at institutions of higher learning, they are still considered students. When dealing with students and educational facilities, SAs will familiarize themselves with the provisions of the Buckley Amendment (Title 20, U.S. Code, Section 1232g), which governs the acquisition of records from educational agencies and institutions.
For the most current and tailored guidance relative to specific countries and programs, the reader should also consult the R&PG located on the relevant CD unit's Intranet site.

A nonofficial/non-immigrant Visitor to the United States is a foreign citizen carrying a nonofficial passport, bearing one of the following U.S. visa types: B, C, D, E, F, H, I, K, L, M, O, P, Q, or R. If such
C. (U) Émigrés, Immigrants, Refugees, and Repatriates

For the most current and tailored guidance relative to specific countries and programs, the reader should also consult the R&PG located on the relevant CD unit's Intranet site.

1. (U) Émigrés
For the most current and tailored guidance relative to specific countries and programs, the reader should also consult the R&PG located on the relevant CD unit’s Intranet site.
3. (U) Immigrants and Refugees

For the most current and tailored guidance relative to specific countries and programs, the reader should also consult the R&PG located on the relevant CD unit's Intranet site.

4. (U) Repatriates

For the most current and tailored guidance relative to specific countries and programs, the reader should also consult the R&PG located on the relevant CD unit's Intranet site.

A repatriate is a person whose entry into the United States is based upon a claim of U.S. citizenship.
Counterintelligence Division Policy Implementation Guide

(U) Repatriate Interviews

1. (S) ...
2. (S) ...
3. (S) ...
4. (S) ...
5. (S) ...
6. (S) ...
7. (S) ...
8. (S) ...
9. (S) ...
10. (S) ...

ACLURM006959
3.6.8. (U) Foreign Agents Registration Act/Agents of Foreign Governments Investigations

(U) The Agents of Foreign Governments Statute, 18 USC § 951 (referred to hereafter as Section 951) has been used in successful FBI prosecutions. Section 951 focuses on the fulfillment of tasking at the direction of a foreign government, where such tasking is not a legal commercial transaction. These investigations are opened as 97 classifications.

(U) Often investigations and prosecutions concerning foreign agents have been mistakenly referred to as Foreign Agents Registration Act (FARA) violations. The term “FARA” properly refers to 22 USC §§ 611 et seq., the focus of which is political or quasi-political activities conducted within the United States, at the request or under the influence of a foreign principal. Both FARA and Section 951 have registration requirements.

A. (U) Procedures and Processes

1. (U) Reporting Requirements

(U) Section 951 investigations will be investigated and administered, in accordance with the AGG-Dom and the regulations set forth in DIOG.

(U) The primary objective of a Section 951 investigation is to protect the United States against foreign intelligence operations. Consequently, prosecution may not
ultimately serve as the optimal vehicle by which to neutralize the threat to U.S. national security.

(U) All Section 951 cases shall be uploaded in a timely manner, unless they contain TS, CHS, or SCI material. These communications shall be handled in accordance to the rules regulating those classifications.

a. (U) Opening Communication
   (U) The 00 shall notify CD in writing within of the opening of an investigation. CD will disseminate the opening communication to the (on an USPER).

b. (U) Closing Communication
   (U) Closing documentation will be submitted to CD via EC and LHM, summarizing the predication for opening the case, the investigation conducted, and the reason the case is being closed.

2. (U) General Administrative Requirements
   a. (U) Coordination with CD. The field office must contact the CD substantive unit immediately upon consideration of, and always prior to, any of the following circumstances:
      • (U)
d. (U) Subject Interview Authorization. The field office must notify CD prior to a subject interview. Unless advised to the contrary by the Bureau (UACB), within the subject interview can be conducted. The will allow CD to determine if there are special circumstances necessitating delay of the interview.

e. (U) Evidence and Documentation. All interviews and collection of evidence will be documented on the FD-302 form or by investigative insert. FD-302 forms shall not be classified unless they contain classified information. If classified, FD-302 forms shall be appropriately marked, including paragraph portion markings. Classified FD-302 forms can later be declassified for trial purposes by a classifying authority. Note: The inclusion of the subject's name in a paragraph does not necessarily require classification of the paragraph.

B. (U) Issues to Consider

(U) During a Section 951 investigation, as well as in any investigation that may lead to a prosecution, some, if not all, of the following issues may present themselves. The
Counterintelligence Division Policy Implementation Guide

following list is intended to provide general guidance to the field office. The list is not intended to be all inclusive.

1. X

(U) By their very nature, Section 951 investigations present delicate legal and policy issues. Prior to sharing information about a subject of a Section 951 investigation, a field office shall coordinate with the CD substantive unit to discuss the positive and negative strategic, legal, and policy implications of sharing information.

(T) In addition, determining whether to

- 
- 
- 

(S)
2. (U) **Handling grand jury information (6(e) material).** Federal Rule of Criminal Procedure 6(e) imposes strict limits on the dissemination of information developed during the course of a grand jury proceeding, and imposes penalties for grand jury leaks. The field office shall:

3. (U) **Presenting classified information to the grand jury.** Grand jurors do not have security clearances required for access to classified information. Accordingly, disclosure of such information to a grand jury may only be done with the approval of the agency responsible for classifying the information sought to be disclosed. Information classified by the FBI must be declassified prior to presentation to a grand jury. Requests for declassification must be made to the CD substantive unit.

4. (U) **Defense Counsel and Security Clearances.** Close coordination between the field office and the defense should also include consideration of who else may need clearances for handling classified material. Consideration should be given to whether the use of classified material can be avoided; where the defense will review copies of any classified material; and where the classified material will be stored.

5. (U) **Discovery.** A criminal indictment triggers the government’s discovery obligations to provide certain materials to a defendant. (F.R. Crim. P. 16.)

6. (U) **Brady/Giglio Issues.** Under Supreme Court decisions in *Brady, Giglio,* and their progeny, the USG has an obligation to disclose evidence that is favorable to the defendant relative to guilt or punishment. The failure to disclose *Brady/Giglio* material may violate due process and the rules of professional conduct, and therefore effect the prosecution. In addition, it may constitute professional misconduct and result in a referral to the Office of Professional Responsibility and disciplinary action.

7. 

---

**SECRET/NOFORN**

Counterintelligence Division Policy Implementation Guide
9. (U) Declassification

The field office may also desire to seek declassification of other classified information for use at trial. The field office will need to determine whether the entire document must be declassified or whether classified portions may be redacted. The CD substantive unit and NSLB can provide guidance in this process.

(U) During the declassification process, the following standards should guide a field office:

(U) The redaction and declassification process is an involved and time-consuming process, therefore, requests shall be made to the CD substantive unit as soon as material is identified. Consideration should be given to the broader strategy of the investigation and potential for prosecution when seeking declassification.

b. (U) Classified Information Procedures Act (CIPA). The CIPA was enacted to provide for the introduction of national security information in federal criminal proceedings, to prevent claims of inability to present a defense because of lack of access, and to defeat so-called graymail (i.e., a situation where the prosecution must choose to disclose classified information publicly or forego prosecution for fear of the potential harm caused by the disclosure). CIPA sets forth procedures designed to protect classified material from disclosure and to protect defendants'
10. **Witnesses and Sources.** A field office should discuss with the whether undercover agents, CHSs, or confidential or cooperating witnesses will be used at trial or in pretrial hearings. If so, the prosecution team will need to determine whether their identities will need to be protected and how.

Protecting witness identities is not assured. Consideration should be given to motions for protective orders to shield a witness’s identity. Field offices shall not promise anonymity to any witness.

(U) If overseas witnesses require Significant Public Benefit Parole (SPBP) to enter the United States, the process is lengthy and should begin several months before they are needed to be in the country. A visa to enter the United States may be required. Field offices shall closely and actively monitor the entire procedure to ensure the parole will actually be issued and available at the correct U.S. embassy overseas.

(U) Although SAC authority and CD authority (per CHSPM, Section 15) is required to disclose the identity of a CHS to a prosecutor, doing so should be considered when it will facilitate open discussions about investigative objectives.

(U) The FBI and the

C. (U) Statutes and Resources

1. (U) Statute

2. (U) Notifications to the Attorney General by Agents of Foreign Governments (28 C.F.R. Parts 73.1-73.6)

3. (U) Miscellaneous Resources

(U) Field offices may desire to refer to a DOJ publicly accessible website that explains Agents of Foreign Governments and activities that require registration and notification as a Foreign Agent pursuant to Section 951.

(U) OGC maintains an Intranet site which contains links to various legal issues. For example, it provides guidance regarding the following issues:

a. (U) Classified Information Procedures Act, 18 U.S.C. Appendix §§ 1-16;

b. (U) The Attorney General’s Guidelines for Prosecutions Involving Classified Information; and
For the most current and tailored guidance relative to specific countries and programs, the reader should also consult the R&PG located on the relevant CD unit's Intranet site.
(U) In developing approaches to persons who have come to the FBI's attention through extraordinary or sensitive techniques, the following should be considered:

A. 

B. 

C. 

3.6.9.1. 

For the most current and tailored guidance relative to specific countries and programs, the reader should also consult the R&PG located on the relevant CD unit's Intranet site.
3.6.11. (U) Foreign Government Currency Use

For the most current and tailored guidance relative to specific countries and programs, the reader should also consult the R&PG located on the relevant CD unit's Intranet site.
(U) If an export law violation has a CI nexus, the FBI has primary jurisdiction to investigate and neutralize the national security threat (28 CFR 0.85 (d)). In cases without such a nexus, the FBI shares concurrent jurisdiction with ICE, Commerce, or other designated government agencies.

B. (U) Applicable Statutes

(U) The two primary USG agencies that regulate and license the export of controlled items are the USDS and Commerce. The USDS regulates the export of defense articles, defense services and brokering activities covered in the International Traffic in Arms Regulations (ITAR), under the Arms Export Control Act (AECA). Commerce regulates the export of dual-use items in the Export Administration Regulations (EAR) under the Export Administration Act (EAA). Additionally, the Treasury Department, Office of Foreign Assets Control (OFAC), controls exports to specific embargoed countries. Under these export laws, the USG must establish that the subject acted willfully to violate the statutes or associated regulations. Generally, the USG must show:
1. (U) The subject exported, or caused to be exported, a controlled item or data, or acted as a broker of defense articles;
2. (U) The subject failed to obtain the necessary export license; and
3. (U) The subject acted willfully.

C. (U) FBIHQ's Role

D. (U) Field Office Responsibilities

E. (U) Coordination with the
Counterintelligence Division Policy Implementation Guide

(U) Field offices are to advise CD via an EC and LHM after identifying a potential non-WMD Directorate export violation (as defined 3.5.2.A). CD is required to

(U) Upon receiving CD

Although converted to a criminal matter, the case will retain its original universal case file number (UCFN) and investigative classification.

(U) Field offices must not attempt to obtain

3.6.13. (U) Terrorism

(U) Given CT’s position as the top FBI investigative and operational priority, both field office and CD personnel are obliged to identify all operational opportunities which can be exploited for the benefit of the CT program. CT matters may also impact CI operations.

(U) While these issues are likely to arise in the context of foreign powers which are also state-sponsors of terrorism, FBI personnel must be vigilant for cross-program issues to arise at any time, and be prepared to collaborate with CT or other appropriate personnel. Cross-program collaboration, in turn, is maximized by regular contact and communication between both agents and analysts from respective divisions.

(U) Policy matters pertaining to CT investigations are found in the Counterterrorism Policy Implementation Guide.

3.6.14. (U) Statistics

(U) Data collection and statistical analysis of data is essential to understanding the quality and quantity of program activities and initiatives in which the FBI engages, as well as the accomplishments realized as a result of those activities. Accurate statistics could make the difference between retaining or eliminating a program activity or initiative. While collecting more data than appears to be needed will rarely cause a problem, other than the time and resources it takes to collect them, failing to collect enough statistics can result in less than ideal analysis. Questions often arise as to the right time or frequency to gather data. This depends on several factors, including the demand for systematic, data-based evaluations for budget, resource, inspection, transition, or review purposes. After collection and data analysis, statistics can be used to summarize what individuals, squads, offices, and programs have done on each case or program and, across the board, on all cases and programs. Statistical reports can be analyzed by supervisors, program managers, and executives to determine the contribution of each activity and

SECRET/NOFORN

ACLURM006972
initiative to a specific mission or strategy. Once the contributions are identified, the FBI can optimize its efforts to successfully reach and maintain its goals by maximizing what works and minimizing what does not work. (See the Investigative Accomplishment Report, FD-542.)

3.7. (U) Media Leak Investigations

For the most current and tailored guidance relative to specific countries and programs, the reader should also consult the R&PG located on the relevant CD unit's Intranet site.

A. (U) Introduction

(U) While handled by CD's media leak investigations are not CI investigations. This is because there is rarely a foreign nexus involved in the violation. Media leak investigations are conducted as criminal investigations and thus employ criminal techniques. Media leak matters are opened as 332 classifications.

(U) Media leak investigations can be extremely complex, time consuming, and labor intensive. Due to these factors, and the inherent sensitivity of these investigations, media leak cases are closely scrutinized by as well as FBI executives. The implemented the following procedures to more effectively manage media leak investigations:

1. (U) A system has been developed by CD, which will be used to track FBI requests to

2. (U) meetings chaired by the will be held with FBI case agents and supervisors assigned to media leak cases, and

3. 

(U) Media leaks occur when national defense information, typically information which is classified, is revealed in the media. With the advance of technology, the types of media that can expose classified material have grown from paper publications, to radio broadcasts, to television shows, to Internet websites. Leaks of information can also be verbal, from one person to another. (See DIOG, Section 10.2.)

B. (U) The Referral Process

(U) The media leak investigative referral process begins with the victim agency, the agency that controls or "owns" the classified information that was leaked in the media. Media exposure of the information is a requirement for a 332 classification to be opened.
Otherwise, the release of classified information is treated as an unauthorized disclosure of classified material.

(U) The victim agency conducts an internal investigation which are the threshold questions used to evaluate the initiation of a media leak investigation.

(U) Upon receipt of the victim agency’s request, the investigation be referred to the FBI for an investigation. CD’s Section Chief authorizing an investigation, attached to which are the very time sensitive or high profile matters for the FBI to initiate an investigation. It is important to note only.

C. (U) Standards to Initiate an Investigation

(U) CD uses a variety of factors as a guide in its case-by-case review of which media leak referrals it will open. While one factor alone could be used to make a decision, determinations will generally be guided by a combination of factors. The main factors include:
(U) While the factors listed above will be the primary determinants in whether to open or not open a case, they are not necessarily inclusive of all factors that could be considered. If an investigation is warranted and all attachments are sent to the field.

(U) Upon assignment, the responsible field office must provide an EC to CD advising that the case has been assigned, the name of the case agent, the squad handling the case and those individuals who require access to the case.

E. (U) Conducting Interviews
H. (U) Media

(U) No media personnel will be interviewed without the approval of the CD AD and the AG. CD will prepare an EC, which will outline the purpose of the investigation, the purpose of the interview, investigative measures to date, and what the field office expects to gain from conducting the interview of the journalist. This EC shall be accompanied by a disseminable memorandum, addressed to the Deputy AG and signed by the CD AD, which explains the requested interview. If the EC and memorandum are approved, ...

I. (U) Subpoenas to the Media

(U) The issuance of a subpoena to a member of the news media is subject to DOJ regulations set out in 28 C.F.R. § 50.10. These regulations require the AG's approval.
before a subpoena can be sought for either testimony regarding news materials or the news material itself. All reasonable attempts should be made to obtain information from an alternative source before considering the issuance of a subpoena to a member of the media. Reasonable attempts are defined very strictly by the DOJ in 28 C.F.R. 50.10.

(U) Except in cases involving exigent circumstances, the express approval of the AG is necessary prior to the interrogation, indictment, or arrest of a member of the news media for an offense which the member of the news media is suspected of having committed during the course of, or arising out of, the coverage or investigation of a news story, or while engaged in the performance of the individual's official duties as a member of the news media. The request should include the considerations set out in 28 C.F.R. § 50.10(k). When an arrest or questioning is necessary before prior authorization can be obtained, notification must be communicated immediately thereafter to the AG and the

through FBIHQ and


J. (U) Reporting Requirements

(U) Field offices were informed of the requirement for espionage investigations on and this requirement has not changed under the new 332 classification for media leaks. The responsible field office shall provide a which shall be submitted in the form of an LHM, shall reflect the case title, briefly explain the case predication, give a summary of the

103

SECRET/NOFORN
investigative activity conducted over the previous and list the case
objectives for the next.

K. (U) Interaction with the

L. (U) Closing a Media Leak Investigation

(U) The field office shall conduct a logical investigation to identify who leaked classified
information. Should the field reach a point in its investigation where it cannot proceed
further, it may request closure of the investigation by sending an LHM to CD. If CD
agrees with the field office assessment to close the case, it will forward the LHM to

(S) 38. x
(S) x
(S) x

(U) In order to maximize CD operations

(U) To bring enhanced CD capabilities
Another major resource to enhance field office operations

3.9.

Any doubts as to whether such activity may constitute pattern-based data mining should be addressed to OGC.
4. (U) Counterintelligence Operational Methods

4.1. (U) General Investigative Operations (Domestic Investigative and Operations Guide)

(U) The DIOG establishes policy regarding all investigative activities and intelligence collection activities conducted by the FBI within the United States or outside the territories of all countries. Compliance with the DIOG is required for all counterintelligence (CI) operations, unless indicated otherwise. Of particular importance are the methods authorized for use in each type of investigation. Authoritative guidance is found in DIOG.

Investigative methods set forth in the DIOG are to be used in CI investigations to achieve the goals and objectives for CI investigations described in the CI Mission Statement.
4.2. (U) Counterintelligence Operational Methods
4.3. (U) CHS Development

(U) CHS development is the cornerstone of CI operations. CHSs are the means to accomplish the following goals, in furtherance of CI goals:

- X
- X
- X
- X
- X
(U) Administration of CHS operations is governed by the Confidential Human Source Policy Manual (CHSPM), and the Human Intelligence Management Unit (HIMU), DI.

For the most current and tailored guidance relative to specific countries and programs, the reader should also consult the R&PG located on the relevant CD unit's Intranet site.

(U) Goals and Objectives:
Counterintelligence Division Policy Implementation Guide

4.4.1. (U) X

4.4.2. (U) Field Office/FBI Coordination

4.4.3. (U)
Counterintelligence Division Policy Implementation Guide

(U) When determining and/or negotiating the arrangements with respect to the collection and dissemination of intelligence in a joint FBI/USIC operation...
Counterintelligence Division Policy Implementation Guide

4.4.6. X

4.4.7. (I) Policy Considerations

A (S/NB) The FBI should be used as a means of providing...
Counterintelligence Division Policy Implementation Guide

Analysis is conducted by a team of FBI SAs.
Counterintelligence Division Policy Implementation Guide
b. (U) Basic information must be obtained, including, as applicable:
   i. (U) Name;
   ii. (U) Date of birth;
   iii. (U) Place of birth;
   iv. (U) Nationality;
   v. (U) Physical description;
   vi. (U)
   vii. (U)
   viii. (U)
   ix. (U)
   x. (U)
   xi. (U)
   xii. (U)

5. (U) When

H. (X) Asylum Seekers

The FBI channels asylum seekers to

a.

b. (U) Basic information must be obtained, including, as applicable:
   i. (U) Name;
   ii. (U) Date of birth;
   iii. (U) Place of birth;
   iv. (U) Nationality;
   v. (U) Physical description;
   vi. (U)
   vii. (U)
   viii. (U)
   ix. (U)
   x. (U)
   xi. (U)
   xii. (U)
In addition, the person should not be provided with any information.
3. (U) Asylum status is granted by the District Director for ICE's district office, after consultation with the USDS, on the basis of whether the alien, if forced to return to the country of origin, will be faced with circumstances which will threaten the alien's life or freedom on account of race, religious beliefs, nationality, memberships in social groups, or held political opinions. (Title 8, U.S. Code, Section 1158(a)(2)(A))
Where applicable facts and circumstances present themselves, the CD shall orchestrate

Field office communications to the CD substantive unit about a prospective
must include:

4.6.1 (FBI)
Counterintelligence Division Policy Implementation Guide

B. (U) FBI responsibilities:

1. X
2. X
3. X
4. X
5. X
6. X
7. X

ACLURM006995
This notice requires the field office to complete a communication to CD containing the following information:
relieve FBI field offices of the responsibility to obtain proper SAC, CD, or AG approval, as noted above.

(See Section 4.12.).

4.6.4. (U) Discontinuance of Source Relationships

The reason for terminating must be expressed as falling within one of the following five categories:

A
B
C
D
E

(See Section 4.12.).
These communications will be sent to the CD substantive unit, which is responsible for providing guidance to the field, maintaining program statistics, recommending administrative actions, and forwarding copies to other offices, as necessary.

Standardized questionnaires which may be used for this purpose are available from the substantive unit.

All such items shall be submitted to this unit by registered mail, with cover communications, and packaged in an appropriate manner.

- Packages shall be addressed as follows:

  Operational Technology Division
The will provide reports on all submitted items to the field office and to the Counterintelligence Division Policy Implementation Guide.

Cover communications shall include: a list of the enclosed items and their descriptions.

Copies of communications to the substantive unit shall also be directed to the appropriate substantive unit.

The will provide reports on all submitted items to the field office and to the substantive unit.

If the field office should require the use out, as needed, for use with lectures, training and other purposes.

Field offices are encouraged to ensure submission of items and information into the

4.6.7. (U)

4.7. (U) Classified Information Procedures Act (CIPA)

The CIPA is a carefully balanced framework which is designed to ensure the fairness and reliability of a criminal trial, while permitting the government to protect its national security equities. CIPA provides for pretrial procedures to resolve questions of admissibility of classified information in advance of its use in open court, and was enacted primarily to defeat so-called graymail tactics by a defendant (i.e.)
CIPA also governs a defendant's access to classified information sought from the government in discovery, and imposes notice burdens on a defendant who intends to utilize classified information in mounting a defense. In practice, CIPA contemplates ex parte, in camera review by federal courts in which the United States presents its national security equities and, in certain situations, may authorize deletions, substitutions, or stipulations regarding classified information implicated by criminal discovery and trial procedures. If criminal prosecution is contemplated in a CD investigation or with a CD subject, in which classified information might be implicated, contact the NSLB immediately. Litigation involving classified information, including CIPA litigation, is very complex and requires substantial coordination among the field division, the CD, NSLB. Early coordination among these entities, well in advance of charges being presented to a grand jury, is essential to resolve classified litigation issues prior to overt prosecutorial action against a defendant.

4.8. (U) Undercover Operations

For the most current and tailored guidance relative to specific countries and programs, the reader should also consult the R&PG located on the relevant CD unit's Intranet site.

4.9. (U)

For the most current and tailored guidance relative to specific countries and programs, the reader should also consult the R&PG located on the relevant CD unit's Intranet site.

A. (U) General Information

1. 

2. 

3. 

(§)

134

SECRET/NOFORN
Counterintelligence Division Policy Implementation Guide

5. (U) Under extraordinary circumstances

6. X

7. X

8. X

9. X

B. (U) Administration

1. X
B. (U) Baseline goals and objectives:
C. (U) Coordination:

(U) Operations frequently have a coordination component. Such coordination responsibilities, based on EO 12333, must be complied with by Per EO 12333, noncompliance must be documented to FBIHQ.
C. (U) Requests for name searches shall be submitted via the appropriate FBIHQ unit.

1. (U) Requests shall contain enough information about the subjects to fully identify them, since names alone are not enough.

2. (U) If requests do not address the specific types of information desired, only derogatory information will be furnished.
(S)

C. FBI Field Responsibilities

(S)

(S)
4.10.3. (U) Persona Non Grata and Demarche

For the most current and tailored guidance relative to specific countries and programs, the reader should also consult the R&PG located on the relevant CD unit's Intranet site.

(U) Use of PNG and Diplomatic Demarche for Expulsion
For the most current and tailored guidance relative to specific countries and programs, the reader should also consult the R&PG located on the relevant CD unit's Intranet site.
D. (U) In addition to the databases described above, the also maintains the...
For the most current and tailored guidance relative to specific countries and programs, the reader should also consult the R&PG located on the relevant CD unit’s Intranet site.
4.12. (U) For the most current and tailored guidance relative to specific countries and programs, the reader should also consult the R&PG located on the relevant CD unit's Intranet site.
For the most current and tailored guidance relative to specific countries and programs, the reader should also consult the R&PG located on the relevant CD unit's Intranet site.
Accordingly, they may be used in connection with CI and appropriate CT investigations, as authorized by the SAC. When such authorizations are granted, the Program Manager addresses matters including selection, hiring, training, placement, temporary duty assignments, promotional criteria, productivity, staffing levels, program budget, and off-premises leases.

and oversee the coordination of personnel, training, equipment, and the
(U) Incidents which may adversely affect operations shall be promptly reported to appropriate field office supervisory personnel and to the SAC. The SAC, in turn, shall promptly report such incidents to CD.

For the most current and tailored guidance relative to specific countries and programs, the reader should also consult the R&PG located on the relevant CD unit's Intranet site.
Counterintelligence Division Policy Implementation Guide

(U) Assistance in impacting operations and investigations:
1. 
2. 
3. 
4. 

(U) Assistance in generating statistical accomplishments in accordance with the National CI Strategy:
1. 
2. 
3. 
4.15. (U) Language Specialists

Language specialists (LS) constitute a valuable resource for a field office's CI program. LSs complement the value in CD investigations.

4.16. (U) Joint Field Office Operations

Case agents, field office management, and CD personnel should
4.17. (U) Overseas Operations

Pursuant to EO 12333, whenever possible, field offices should work towards complementing each others' operations.

In addition, AG concurrence for SA travel must be obtained. This has been delegated to the AD. In the request for AG concurrence, the fact that the operation has been coordinated with and approved.

(U) Overseas travel also requires the submission of appropriate forms, a pre-travel briefing, and post-travel debriefing. Consult the Security Division Intranet site for pertinent requirements. Personnel traveling overseas must always remain aware of their environment, and
(U) Unless otherwise specified, CD operations must conform with the extraterritorial provisions of the Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection (NSIG), Section II.E.

4.18. (U)

A. (U)

1. 

(B) 

2. (B) 

a. 

b. 

c. 

d. 

e. 

3. (B) 

4. (B) 

5. (B) 

6. (U)
(U) When conducting authorized activities, there are special approval levels for certain operations. Once the FBI is authorized, the FBI may seek •

Counterintelligence Division Policy Implementation Guide
5. (U) Should the field office or substantive SSA responsible...
Counterintelligence Division Policy Implementation Guide

E. (U) As a practical matter

1. 

2. 

3. 

4. (U) As a practical matter

5. (U)
   a. (U) ACS checks to determine whether the
   b. 

6. (U) Scrutiny of the

F. (U) 

162
4.19. (U) National Security Letters

A. (U) For general information regarding NSL procedures see DIOG, Section 11.9.3.

B. (U) NSLs are administrative demands for documents or records which can be made by the FBI in support of a preliminary or full investigation. NSLs may not be issued in assessments. Every NSL must be accompanied by an EC documenting the relevance of the information sought to a national security investigation. (See NSL Intranet site.)

C. (U) There are presently three statutory categories (financial institution records, consumer credit agency records, and electronic communication service provider records) with eight variations of these three NSL types, which are:

1. (U) A subscriber's name, address, and length of service (18 USC § 2709);
2. (U) Toll billing records (18 USC § 2709);
3. (U) Electronic subscriber information (18 USC § 2709);
4. (U) Electronic communication transactional records (18 USC § 2709);
5. (U) Financial records (12 USC § 3414);
6. (U) Identity of financial institutions (15 USC § 1681u);
7. (U) Consumer identifying information (15 USC § 1681u); and
8. (U) Additional information (18 USC § 2709).
8. (U) Full credit reports (15 USC § 1681v). Note

E. (U) NSLs are drafted, approved, and issued via

A premium on accuracy must be placed on all information submitted in the process. Note that

F. (U) Other types of records are also protected by statute. For instance, tax return information in the possession of the Internal Revenue Service (26 USC § 6103), video tape rental or sale records (18 USC § 2710(b)), and educational records in the possession of educational institutions (26 USC §1232g(j)), which are subject to special statutory procedures for disclosure. If there is no statutory protection for the third party record, businesses may produce records voluntarily upon request. However, if a business is unwilling to provide such records, production may be compelled through a grand jury subpoena, if there is a criminal nexus.

G. 

4.20. (U) Interviews

A. (U) An interview is a planned and structured conversation with an individual, which is designed to gather information so evidence can be collected or intelligence can be elicited, which can be used to structure an investigation. A well conducted interview and its report
permits an agent to document and communicate the findings clearly and concisely in an organized and logical fashion. Analysis of information derived from interviews can effectively be used to focus the direction of authorized investigations.

B. (U) Interviews as authorized investigative methods:

C.

D. (U) Approvals:

(U) Subjects:

(U) The subjects of all CI predicated investigations require CD substantive unit approval. This approval insures field offices are not acting inadvertently or at cross-purposes, i.e., when one field office's interview will potentially compromise another field office's operation(s).

(U) Protection of sources/methods:

(S)
4.21. (U) Legats

A. (S) Absent specific operational security requirements, Legats are advised of all FBI CI issues which are pertinent to the countries for which they are responsible.

B. (U) In the absence of specific reasons to the contrary, Legats are always utilized as liaison officers in FBI investigations abroad.

C. (S) 

D. (U) In connection with the FBI's espionage responsibilities abroad, see the Espionage Section, 3.5.1, of this PG. In order to facilitate proactive action, Legats establish formal relationships and procedures in the embassies to which they are attached. Legats ensure all affected persons are fully aware of the FBI's responsibilities. Legats immediately advise CD of possible espionage violations, and immediately advise CD if it appears FBI interests conflict.
(S) For current and specific information concerning Legats, as well as links to additional policy manuals, please see the IOD Intranet site.
4.23. (U) Forensic Financial Examinations

For the most current and tailored guidance relative to specific countries and programs, the reader should also consult the R&PG located on the relevant CD unit’s Intranet site.

(U) An FFE may be conducted in either a

The AGG-Dom authorizes investigative techniques in

that are essential for obtaining financial information to support the FFE.

4.23.1. (U) Levels of Forensic Financial Examination

(U) Depending upon the factual predication of the case, an FFE will be done at

4.23.2. (U) FFE Should Be Considered In All

(U) An FFE may be of value in

should be consulted to arrange for an FFE to be performed outside of the investigating field office.
5. (U) Directorate of Intelligence Matters

5.1. (U) Counterintelligence Division - Directorate of Intelligence (DI) Integration

(U) Effective CI operations and dissemination of CI and foreign intelligence work-product are based on integration of CD and DI personnel working for common goals. CD personnel must cultivate and develop relationships with DI elements in order to maximize operational performance.

(U) DI analysts provide CI personnel with

(U) Case agents should rely on the DI, either in their field office or at FBIHQ, for strategic and tactical guidance on targeting priorities, the generation of source debriefing packages, the evaluation of source reporting, preparation of various raw intelligence dissemination products, and the identification of intelligence gaps (i.e.,

5.2. (U)

A. (U)

(U) are widely distributed throughout the USIC, and operational information identifying sources and/or the specifics of investigations should never be included in them.

B. (U) The following criteria shall be adhered to in deciding whether to disseminate information utilizing the format:

1. (U) Intelligence should be new;
2. (U) Intelligence should be detailed;
3. (U) Intelligence should be authoritative;
4. (U) Intelligence should be and
5. (U) Intelligence should respect the rights of USPERs.

(U) Information which does not meet the criteria may, of course, be disseminated by other means, e.g., LHM.

C. (U) FBI-originated must be issued by the DI Collection Management Section or, in the case of

169
However, operational taskings and leads will continue to be issued from an operational component to an operational component (e.g., from CD to field office CI squads).

D. (U) CD is responsible for:

1. (U) Providing operational taskings to the field; and
2. (U) Ensuring submissions will not jeopardize on-going cases.

E. DIDO approval, but also the Director's approval, prior to the dissemination. The Director has delegated this approval to the ADs.
(U) FBIHQ prepares other finished intelligence products reporting and evaluating CI information wholly, or in part, that are intended for use by FBI executive leadership and senior national policymakers.
Counterintelligence Division Policy Implementation Guide

Director and senior FBIHQ executives,

articles prepared by FBI authors addressing intelligence or CI issues from any of the FBI's operational program areas.

(U) Disseminations to

(X)

(U) In either situation, any dissemination of information from a CD investigation, especially especially must comply with the FBI's may require either senior FBI executive authority, or AG authority, depending on the source of the information to be disseminated.

5.4. (X)

(X)

SECRET/NOFORN

ACLURM007035
6. (U) Intelligence Partners

6.1. (U) Operations

(U) These meetings and interactions can transpire for many different reasons, including the following:
6.2. (U) The Office of the National Counterintelligence Executive

(U) The National Counterintelligence Center (NACIC), which was established pursuant to Presidential Decision Directive PDD-24, has been replaced by the ONCIX. PDD-75, establishing the ONCIX was signed in late 2000.
6.3. (U) For the most current and tailored guidance relative to specific countries and programs, the reader should also consult the R&PG located on the relevant CD unit's Intranet site.

A. (U) EO 12333 mandates agencies of the [redacted] consistent with applicable federal law shall, under the leadership of the [redacted] conduct administrative, technical and other support activities within the United States necessary for the performance of authorized activities; and shall protect the security of intelligence related activities, installations, property and employees, by appropriate means.

B. (U) The approval of the AG, the Deputy AG, or an official designated by the AG, is required prior to providing any type of [redacted].

D
E. (U) In addition to [Blank], which are described below.

2. (U)
   a. [Blank]
   b. [Blank]

F. [Blank]

G. [Blank]

6.4. (U) Immigration and Customs Enforcement/Customs and Border Patrol

A. [Blank]
2. (U) FBI SAs may be present at the time

B.

C. 

7. (U) CI Strategic Partnership Program

7.1. (U) CI Strategic Partnership Program

(U) The CI Strategic Partnership Program is responsible for determining and safeguarding those technologies that if compromised would result in catastrophic losses to national security. Through partnerships with businesses, academia, and the FBI and USG. This provides the first line of defense inside facilities where research and development occurs, and where intelligence services are focused.

(U) The Strategic Partnership Program concept

7.1.1. (U) Implementation of National Counterintelligence Strategy

For the most current and tailored guidance relative to specific countries and programs, the reader should also consult the R&PG located on the relevant CD unit's Intranet site.

A. (U) Strategy Implementation

(U) The successful implementation of the FBI's National CI Strategy will protect the information and technologies critical to the U.S. national and economic security, by doing the following:

B. (U) Strategy Implementation

(U) The successful implementation of the FBI's National CI Strategy will protect the information and technologies critical to the U.S. national and economic security, by doing the following:
7.1.2. (U) Strategic Guidance

For the most current and tailored guidance relative to specific countries and programs, the reader should also consult the R&PG located on the relevant CD unit’s Intranet site.

(U) Program Reviews

(U) The CI Strategic Partnership Program implements the National CI Strategy by providing field divisions with guidance and direction through CI Program Reviews.

7.1.3. (U) Strategic Partnership Activities

For the most current and tailored guidance relative to specific countries and programs, the reader should also consult the R&PG located on the relevant CD unit’s Intranet site.

A. (U) Strategic Partnership Coordinators

(U) Each field office has been asked to designate a strategic partnership coordinator (SPC) (a CI SA or a former CI SA under Personal Services Contract) who will become the expert as to what facilities and/or technologies must be protected.

B. (U) Academic Outreach
7.1.4. (U) Critical National Asset Initiative

(U) See Section 3.5.3.

7.1.5. (U) Counterintelligence Working Groups

For the most current and tailored guidance relative to specific countries and programs, the reader should also consult the R&PG located on the relevant CD unit's Intranet site.
(U) Appendix A: Sources of Additional Information

For country specific information, please view the CD sections listed below. Additional sources listed below include MOUs, directives and other reference materials.

(U) Weapons Of Mass Destruction Terms Handbook

(U) Worldwide WMD Threats

(U) Biological and Chemical Agent Quick Reference

(U) Executive Order 12333

(U) Attorney General Guidelines for Domestic FBI Investigations

(U) U.S. Patriot Act Renewal

(U) The Buckley Amendment

(U) Espionage Violations

(U) Espionage/Counterintelligence Authorities

ALL INFORMATION CONTAINED HEREBIN IS UNCLASSIFIED

DATE 05-03-2011 BY 65179/DIV/BAU/STP/bis

b7E

ACLURM007044
(U) Appendix B: Supersessions

(U//FOUO) This table identifies National Foreign Intelligence Program Manual (NFIPM) sections, that have been superseded by this PG, the DIOG, or other policy manuals and guidance.

<table>
<thead>
<tr>
<th>NFIP Manual</th>
<th>DIOG or other Manual</th>
<th>CDPG Section</th>
</tr>
</thead>
<tbody>
<tr>
<td>Section: 01 (U) Mission Statement</td>
<td></td>
<td>b7E</td>
</tr>
<tr>
<td>Acronyms, and File Classifications (4)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>01-1: (U) Mission Statement</td>
<td></td>
<td>2.1</td>
</tr>
<tr>
<td>01-2: (I)</td>
<td></td>
<td>not attached</td>
</tr>
<tr>
<td>01-3: (U) Acronyms</td>
<td></td>
<td>Appendix C</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RPO site</td>
</tr>
<tr>
<td>Section: 02 (U) General Investigative and Administrative Activities and Requirements (57)</td>
<td></td>
<td>b7E</td>
</tr>
<tr>
<td>02-1: (U) General Investigative and Administrative Activities</td>
<td></td>
<td>3.1</td>
</tr>
<tr>
<td>02-2: (U) National Security Investigations</td>
<td></td>
<td>3.1</td>
</tr>
<tr>
<td>02-3: (U) Summary Guidance and Applicability of</td>
<td></td>
<td>NA</td>
</tr>
<tr>
<td></td>
<td></td>
<td>b7E</td>
</tr>
<tr>
<td>02-4: (U) Summary Guidance and Applications for</td>
<td></td>
<td>NA</td>
</tr>
<tr>
<td></td>
<td></td>
<td>b7E</td>
</tr>
<tr>
<td>02-5: (U) Summary Guidance and Application for</td>
<td></td>
<td>NA</td>
</tr>
<tr>
<td>02-6: (U) Collection of Foreign Intelligence</td>
<td></td>
<td>3.6.5</td>
</tr>
<tr>
<td>Number</td>
<td>Description</td>
<td>Section</td>
</tr>
<tr>
<td>--------</td>
<td>------------------------------------------------------------------------------</td>
<td>---------</td>
</tr>
<tr>
<td>02-1</td>
<td>(S)</td>
<td></td>
</tr>
<tr>
<td>02-2</td>
<td>(S)</td>
<td>3.6.7</td>
</tr>
<tr>
<td>02-3</td>
<td>(U) Office of Origin</td>
<td>3.1.7</td>
</tr>
<tr>
<td>02-4</td>
<td>(U)</td>
<td>4.13</td>
</tr>
<tr>
<td>02-5</td>
<td>(U)</td>
<td>4.2</td>
</tr>
<tr>
<td>02-6</td>
<td>(U)</td>
<td>3.6.6</td>
</tr>
<tr>
<td>02-7</td>
<td>(U)</td>
<td>3.5.1.10</td>
</tr>
<tr>
<td>02-8</td>
<td>(U)</td>
<td></td>
</tr>
<tr>
<td>02-9</td>
<td>(U)</td>
<td></td>
</tr>
<tr>
<td>02-10</td>
<td>(U)</td>
<td></td>
</tr>
<tr>
<td>02-11</td>
<td>(U)</td>
<td></td>
</tr>
<tr>
<td>02-12</td>
<td>(U)</td>
<td></td>
</tr>
<tr>
<td>02-13</td>
<td>(U)</td>
<td></td>
</tr>
<tr>
<td>02-14</td>
<td>(U)</td>
<td>4.10.1</td>
</tr>
<tr>
<td>02-15</td>
<td>(U)</td>
<td></td>
</tr>
<tr>
<td>02-16</td>
<td>(U)</td>
<td>DIOG 11.4</td>
</tr>
<tr>
<td>02-17</td>
<td>(U)</td>
<td>DIOG 11.6</td>
</tr>
<tr>
<td>02-18</td>
<td>(U)</td>
<td>DIOG 11.9 and 11.9.3</td>
</tr>
<tr>
<td>02-19</td>
<td>(U)</td>
<td>4.18</td>
</tr>
<tr>
<td>02-20</td>
<td>(U)</td>
<td></td>
</tr>
<tr>
<td>02-21</td>
<td>(U)</td>
<td>DIOG 11.3</td>
</tr>
<tr>
<td>02-22</td>
<td>(S)</td>
<td>4.4.4, 4.4.5, 4.10.1</td>
</tr>
<tr>
<td>02-23</td>
<td>(S)</td>
<td>4.21</td>
</tr>
<tr>
<td>02-24</td>
<td>(U)</td>
<td>DIOG 17</td>
</tr>
<tr>
<td>02-25</td>
<td>(U)</td>
<td>4.10.3</td>
</tr>
<tr>
<td>02-26</td>
<td>(U)</td>
<td>4.10.4</td>
</tr>
</tbody>
</table>

(S) Secret
(U) Unclassified
ACLURM007047
<table>
<thead>
<tr>
<th>02-28: (U) National Counterintelligence Executive</th>
<th>4.10.5</th>
</tr>
</thead>
<tbody>
<tr>
<td>02-29: (U) Laboratory Assistance</td>
<td>6.2</td>
</tr>
<tr>
<td>02-30: (S)</td>
<td>not covered</td>
</tr>
<tr>
<td>02-31: (U)</td>
<td>not covered</td>
</tr>
<tr>
<td>02-32: (U)</td>
<td>not covered</td>
</tr>
<tr>
<td>02-33: (S)</td>
<td>4.9</td>
</tr>
<tr>
<td>02-34: (U)</td>
<td>4.14</td>
</tr>
<tr>
<td>02-35: (U)</td>
<td>4.13</td>
</tr>
<tr>
<td>02-36: (U) Investigations of Current and Former Department of State Personnel, and Diplomatic Missions Personnel Abroad</td>
<td>3.6.9</td>
</tr>
<tr>
<td>02-37: (S)</td>
<td>3.5.1.1 K, 3.6.9</td>
</tr>
<tr>
<td>02-38: (U) Investigations of Current and Former Military and Civilian Department of Defense Personnel</td>
<td>3.5.1.1 K, 3.6.9</td>
</tr>
</tbody>
</table>

ACLURM007048
### Counterintelligence Division Policy Implementation Guide

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
<th>Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>02-45</td>
<td>(U) Disseminating Information to Other Agencies in the Federal Government</td>
<td>DIOG 12.4</td>
</tr>
<tr>
<td>02-46</td>
<td>(U)</td>
<td>5.2</td>
</tr>
<tr>
<td>02-47</td>
<td>(U) Disseminating Information to Congressional Committees</td>
<td>DIOG</td>
</tr>
<tr>
<td>02-48</td>
<td>(U) Disseminating Information to the Federal Judiciary</td>
<td>DIOG</td>
</tr>
<tr>
<td>02-49</td>
<td>(U) Disseminating Information to the White House</td>
<td>DIOG</td>
</tr>
<tr>
<td>02-51</td>
<td>(U) Disseminating Information to State and Local Government Agencies</td>
<td>DIOG</td>
</tr>
<tr>
<td>02-52</td>
<td>(U) Disseminating Information to the Private Sector</td>
<td>7.1.3</td>
</tr>
<tr>
<td>02-53</td>
<td>(U) Data Collection Method for Foreign Counterintelligence, Foreign Intelligence and International Terrorism Statistics</td>
<td>3.6.14</td>
</tr>
<tr>
<td>02-54</td>
<td>(U) IIIA (Integrated Intelligence Information Application)</td>
<td>Not covered</td>
</tr>
<tr>
<td>02-55</td>
<td>(U) President’s Foreign Intelligence Advisory Board Matters</td>
<td>NA</td>
</tr>
<tr>
<td>02-56</td>
<td>(U) Intelligence Oversight Board Matters</td>
<td>NA</td>
</tr>
<tr>
<td>02-57</td>
<td>(U) Alpha Designations</td>
<td>NA</td>
</tr>
</tbody>
</table>

### Section: 03 (U) Electronic Surveillances and Unconsented Physical Searches (16)

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
<th>Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>03-1</td>
<td>(U) Consensual Monitoring</td>
<td>DIOG 11.5</td>
</tr>
<tr>
<td>03-2</td>
<td>(U) Volunteered Tape Recordings</td>
<td>DIOG 6.9</td>
</tr>
</tbody>
</table>

**B-4**
<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>03-3</td>
<td>(U) Deleted</td>
</tr>
<tr>
<td>03-4</td>
<td>(U) Pen Registers and Trap and Trace Devices</td>
</tr>
<tr>
<td>03-5</td>
<td>(U) Unconsented Electronic Surveillance</td>
</tr>
<tr>
<td>03-6</td>
<td>(U) Electronic Surveillance Minimization, Logs and Indexing</td>
</tr>
<tr>
<td>03-7</td>
<td>(U) Destruction of Electronic Surveillance Tape Recordings</td>
</tr>
<tr>
<td>03-11</td>
<td>(U) Unconsented Physical Searches</td>
</tr>
<tr>
<td>03-12</td>
<td>(U) Tax Return Information</td>
</tr>
<tr>
<td>03-13</td>
<td>(U) Searches of Mail Without Consent</td>
</tr>
<tr>
<td>03-14</td>
<td>(U) Unconsented Physical Search Minimization, Logs and Indexing</td>
</tr>
</tbody>
</table>

Section: 04 (U) The ANSIR Program and Certain Statute and Treaty Based Investigations (7)

| 04-1 | (U) The Domain Program |

DIOG 11.11, 11.11.1 thru 11.11.10  DIOG 11.12  DIOG 11.12  SMP PG  SMP PG  6.3  4.6.6  4.18  4.19  4.22  6.4  4.9  7.1
<table>
<thead>
<tr>
<th>04-2: (U) Foreign Agents Registration Act (FARA) Investigations</th>
<th>3.6.8</th>
</tr>
</thead>
<tbody>
<tr>
<td>04-3: (U) Agents of Foreign Governments Investigations</td>
<td>3.6.8</td>
</tr>
<tr>
<td>04-4: (U) Internal Security Act of 1950 Investigations</td>
<td>Not covered; most repealed</td>
</tr>
<tr>
<td>04-5: (U) Intelligence Identities Protection Act Investigations</td>
<td>not covered</td>
</tr>
<tr>
<td>04-6: (U) Registration of Persons Trained in Foreign Espionage Systems Investigations</td>
<td>not covered</td>
</tr>
<tr>
<td>04-7: (U) Arms Control Treaty Matter Investigations</td>
<td></td>
</tr>
</tbody>
</table>

05-3: (U) Goals and Objectives

<table>
<thead>
<tr>
<th>05-3: (U) Goals and Objectives</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.3.1</td>
</tr>
<tr>
<td>3.3.1</td>
</tr>
<tr>
<td>3.3.1</td>
</tr>
<tr>
<td>3.6.6</td>
</tr>
</tbody>
</table>

B-6
Counterintelligence Division Policy Implementation Guide

Section: 06 (X) Investigations
Reference and procedure guide

Section: 07 (X) Investigation
Reference and procedure guide

Section: 08 (X) Investigations
Reference and procedure guide

Section: 09 (X) Investigation
Reference and procedure guide

NA

not covered

3.6.6

3.6.6

3.6.6

3.6.6

3.6.6

3.6.6

3.6.6

3.6.9

3.6.9.1

3.6.10

3.6.13

3.6.11

3.6.12

05-10

05-11

05-12

05-13

05-14

05-15

05-16

05-17

05-18

05-19: (U)

05-20: (U)

05-21: (U)

05-22

05-23

ACLURM007052
<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
<th>Reference and procedure guide</th>
</tr>
</thead>
<tbody>
<tr>
<td>11 (U)</td>
<td>Investigation</td>
<td></td>
</tr>
<tr>
<td>12 (U)</td>
<td>Investigation</td>
<td></td>
</tr>
<tr>
<td>13 (U)</td>
<td>Investigation</td>
<td></td>
</tr>
<tr>
<td>14 (U)</td>
<td>Investigation</td>
<td></td>
</tr>
<tr>
<td>15 (U)</td>
<td>Investigation</td>
<td></td>
</tr>
<tr>
<td>16 (U)</td>
<td>Investigation</td>
<td></td>
</tr>
<tr>
<td>18 (U)</td>
<td>Issue Threat Investigations (6)</td>
<td>3.5</td>
</tr>
<tr>
<td>18-1:  (U) Issue Threat Investigations</td>
<td></td>
<td>3.5</td>
</tr>
<tr>
<td>18-2:  (U) Issue Threats</td>
<td></td>
<td>3.2</td>
</tr>
<tr>
<td>18-3:  (U) Issue Threat</td>
<td></td>
<td>NA</td>
</tr>
<tr>
<td>18-4:  (U) Issue Threat</td>
<td></td>
<td>NA</td>
</tr>
<tr>
<td>18-5:  (U) Issue Threat Case Characters</td>
<td></td>
<td>NA</td>
</tr>
<tr>
<td>18-6:  (U) Issue Threat File Numbers</td>
<td></td>
<td>NA</td>
</tr>
<tr>
<td>19 (U)</td>
<td>International Terrorism Investigations (13)</td>
<td>CTDMPG</td>
</tr>
<tr>
<td>20: (U) Espionage</td>
<td></td>
<td>3.5.1</td>
</tr>
<tr>
<td>21 (U)</td>
<td>Investigations (6)</td>
<td>3.5.2</td>
</tr>
<tr>
<td>21-1:  (U)</td>
<td></td>
<td>3.5.2</td>
</tr>
<tr>
<td>21-2:  (U) FBI Headquarters Oversight</td>
<td></td>
<td>NA</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3.5.2 D</td>
</tr>
<tr>
<td>Section</td>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
<td></td>
</tr>
<tr>
<td>21-5</td>
<td>(U) (see NFIPM)</td>
<td></td>
</tr>
<tr>
<td>21-6</td>
<td>(U) Alpha Designations</td>
<td></td>
</tr>
<tr>
<td>22-1</td>
<td>(U) Economic Counterintelligence and Economic Espionage Investigations (2)</td>
<td></td>
</tr>
<tr>
<td>22-2</td>
<td>(U) Alpha Designations</td>
<td></td>
</tr>
<tr>
<td>23-1</td>
<td>(U) Threats to the National Information Infrastructure (15)</td>
<td></td>
</tr>
<tr>
<td>23-2</td>
<td>(U) Lead Agencies</td>
<td></td>
</tr>
<tr>
<td>23-3</td>
<td>(U) The National Coordinator for Security, Infrastructure Protection and Counterterrorism</td>
<td></td>
</tr>
<tr>
<td>23-4</td>
<td>(U) Interagency Groups</td>
<td></td>
</tr>
<tr>
<td>23-5</td>
<td>(U) Cyber Division - Mission</td>
<td></td>
</tr>
<tr>
<td>23-6</td>
<td>(U) TNII Matters - Investigative Guidance</td>
<td></td>
</tr>
<tr>
<td>23-7</td>
<td>(U) The 288 Subclassification</td>
<td></td>
</tr>
<tr>
<td>23-8</td>
<td>(U) 288A</td>
<td></td>
</tr>
<tr>
<td>23-9</td>
<td>(U) 288B</td>
<td></td>
</tr>
<tr>
<td>23-10</td>
<td>(U) 288C-H</td>
<td></td>
</tr>
</tbody>
</table>

NA: Not Applicable
B-9
<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>23-13:</td>
<td>(U) Authorities, Procedures, and Requirements in Computer Intrusion IT Matters</td>
</tr>
<tr>
<td>23-14:</td>
<td>(U) 288L</td>
</tr>
<tr>
<td>23-15:</td>
<td>(U) Relevant Statutes</td>
</tr>
<tr>
<td>Section: 24</td>
<td>(U) Targeting the U.S. Government Investigations (1)</td>
</tr>
<tr>
<td>24-1:</td>
<td>(U) Targeting the U.S. Government Investigations</td>
</tr>
<tr>
<td>Section: 25</td>
<td>(U) Investigations</td>
</tr>
<tr>
<td>25-1:</td>
<td>(U) Investigations</td>
</tr>
<tr>
<td>Section: 26</td>
<td>(U) Foreign Intelligence Activities Investigations (1)</td>
</tr>
<tr>
<td>26-1:</td>
<td>(U) Foreign Intelligence Activities Investigations</td>
</tr>
<tr>
<td>Section: 27</td>
<td>(U) Confidential Human Sources Manual</td>
</tr>
<tr>
<td></td>
<td>CHSM</td>
</tr>
<tr>
<td></td>
<td>(U) Confidential Human Source Validation Standards Manual</td>
</tr>
<tr>
<td></td>
<td>CHSVSM</td>
</tr>
<tr>
<td>Section: 28</td>
<td>(U) Undercover Operations (4)</td>
</tr>
<tr>
<td>28-1:</td>
<td>(U) UC Operations</td>
</tr>
</tbody>
</table>

B-10
### Counterintelligence Division Policy Implementation Guide

#### Section 29 (U)

- 29-1: (U)

#### Section 30

- 30-1: (U) Initial Communications

- 30-4: (U) Deferred Payments

- 30-5: Among Field Offices

- 30-10: (U)

- 30-11: (U)

- 30-12: (U) Discontinuance of

- 30-13

- 30-14

- 30-15

---

**B-11**
(U) Appendix C: Glossary

(U) Agent: (a) A person who engages in clandestine intelligence or international terrorism activities under the direction of an intelligence or terrorist organization, but who is not an officer, employee or co-optee of that organization; (b) an individual who acts under the direction of an intelligence agency or security service to obtain, or assist in obtaining, information for intelligence, CI or CT purposes; (c) a person who is authorized or instructed to obtain, or assist in obtaining, information for intelligence or CI purposes.

(U) Analysis: The process in which intelligence information is subjected to systematic examination in order to identify significant facts, and derive conclusions from these facts.

(U) Asylum: An immigration status which is sought by one who seeks to remain in the United States because of persecution or anticipated persecution in the individual's country of origin.

(U) Authorized For Release To (REL TO): A control marking which is used when a limited exception to the parameters of NOFORN may be made, to allow the release of information beyond USIC recipients.

C-1

SECRET/NOFORN
(U) **Brady Issue (Brady v. Maryland)**: Obligation of the Government to provide the defense any evidence favorable to the accused, and material favorable to guilt or punishment.

(U) **Briefing**: The preparation of an individual for a specific operation, by describing the objectives, the methods to be employed, and the situation(s) which will be encountered.

(U) **Buckley Amendment**: Governs the acquisition of education records from educational agencies and institutions.

(U) **Caveated Information**: Information that is subject to an authorized control marking.

(U) **Chief Of Mission**: The principal officer in charge of a diplomatic mission of the United States, or of a U.S. office abroad, which is designated by the Secretary of State as diplomatic in nature.

(U) **Cipher**: Any cryptographic system in which arbitrary symbols or groups of symbols represent units of plain text, and/or in which units of plain text are rearranged.

(U) **Cipher Pad (One Time Pad)**: A manual one-time cryptosystem produced in pad form.
(U) **Classification**: The determination that official information requires, in the interest of national security, a specific degree of protection against disclosure, coupled with a designation signifying that such a determination has been made.

(U) **Communication Deception**: The deliberate transmission, retransmission, alteration, absorption, or reflection of telecommunications, in a manner intended to cause misunderstanding.

(U) **Compartmentation**: The restriction of information to those who have a need-to-know.

(U) **Compromise**: A disclosure of information to unauthorized individuals, or a violation of the security policy of a system, in which unauthorized, intentional, or unintentional disclosure, modification, destruction, or loss of an object may have occurred.

(U) **Concealment Device**: An innocuous object designed or adapted as a container for secreting materials and/or equipment.

(U) **Confidential Human Source**: Any individual who is believed to be providing useful and credible information to the FBI for any authorized information collection activity, and from whom the FBI expects or intends to obtain additional useful and credible information in the future, and whose identity, information, and relationship with the FBI warrants confidential handling.

**C-3**
Counterintelligence Division Policy Implementation Guide

(U) Controlled Technology: All forms of restricted and embargoed unclassified technology.

(U) Counterespionage: An aspect of CI, designed to detect, destroy, neutralize, exploit, and/or prevent espionage activities through identification, penetration, manipulation, deception, and/or repression of individuals, groups or organizations which are conducting or suspected of conducting espionage activities.

(U) Countermeasure: An action taken to negate the opposition's ability to take advantage of its target's vulnerabilities.

(U) Counterterrorism: Measures taken to prevent, deter and respond to a terrorist act, or the threat of such an act, not including personnel, physical, document, or communications security programs.

(U) Covert Action: An operation which is designed to influence governments, events, organizations, or persons, and which is planned and executed in such a manner as to conceal the identity of the sponsoring power, or to permit plausible denial.

(U) Counterintelligence: Information gathered, and activities conducted, to protect against espionage and other intelligence activities, sabotage, or assassinations conducted by, for, or on behalf of foreign powers, organizations, or persons or international terrorism activities.

(U) Critical Technology: Any technology, selected on the basis of its ability to: (a) enhance U.S. national and economic prosperity, (b) provide for U.S. economic independence and competitiveness in the global marketplace, (c) contribute to a rising standard of living, (d) strengthen the U.S. industrial base, and/or (e) provide for an increased national security capability.
(U) Cryptanalysis: The conversion of an encrypted message to plain text, without the knowledge of the crypto-algorithm and/or key which was employed in the encryption.

(U) Dead Drop: An unattended place at which communications, materials, or equipment can be taken to by one individual, and from which they can be retrieved by another individual, without the two either meeting or seeing each other.

(U) Debriefing: A nonhostile interview of an individual who has completed an intelligence assignment, or who has knowledge (through observation, participation or otherwise) of operational or intelligence significance.

(U) Deception (Disinformation): A measure designed to induce an opponent into taking an action which is prejudicial to its own interests.

(U) Defector: A person of any nationality (though usually a country whose interests are hostile or inimical to those of the United States), who has escaped from the control of the person's home country, who is unwilling to return to that country, and who is of special value to the USG because...

(U) Defector Source: An individual who:

C-5
(U) Diplomatic Establishment: Any establishment which is directed and controlled by a foreign
government, and which deals with diplomatic, commercial, cultural, educational, news-gathering,
and/or tourism affairs.

(U) Diplomatic Officials: Personnel employed by a country, who act in official capacities, e.g.,
diplomats, attaches and consuls assigned to diplomatic missions, embassies and consulates
general; and members of international organizations or Establishments who are assigned to the
United States for a period of one year or more. Immediate family members, servants, and
personal employees are excluded from this class unless unusual circumstances exist. Such
persons usually enter the United States under A visas, although individuals posted to
international organizations use G visas, and persons from Taiwan use E visas.

(U) Diplomatic Pouch (Diplomatic Bag): A container bearing visible marks of its diplomatic
character, and protected from opening or detention by a treaty to which the United States is a
party.

(U) Dissemination: The timely distribution of an intelligence product, in a form suitable to
intelligence consumers.

(U) Dissemination and Extraction of Information Controlled by Originator (ORCON): A
security designation which is used to enable the originator of intelligence to control its wider
distribution and use on a continuing basis.

(U) Domestic Terrorism: Activities that: (a) involve acts dangerous to human life that are a
violation of the criminal laws of the United States or of any state; (b) appear to be intended to
intimidate or coerce a civilian population, influence the policy of a government by mass
destruction, assassination or kidnapping; and (c) occur primarily within the territorial jurisdiction
of the United States.

(U) Dual-Use Technology: Technology that has both civilian and military applications.

(U) Economic Espionage: Foreign power sponsored or coordinated intelligence activity directed
at the USG, or U.S. corporations, establishments, or persons, which involves: (a) the unlawful or
clandestine targeting or acquisition of sensitive financial, trade, or economic policy information,
proprietary economic information, or critical technologies; or (b) the unlawful or clandestine
targeting or influencing of sensitive economic policy decisions.

(U) Electronic Surveillance: (a) The acquisition (by electronic, mechanical, or other
surveillance device) of the contents of any wire or radio communication (sent by, or intended to
be received by, a U.S. person in the United States), if the contents are acquired by intentionally
targeting that U.S. person, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes; (b) the acquisition (by electronic, mechanical, or other surveillance device) of the contents of any wire or radio communication (to or from a person in the United States), without the consent of any party, if such acquisition occurs in the United States; (c) the intentional acquisition (by an electronic, mechanical, or other surveillance device) of the contents of any radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, and if both the sender and all intended recipients are located within the United States; or (d) the installation or use of an electronic, mechanical, or other surveillance device in the United States for monitoring, to acquire information (other than from a wire or radio communication), under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes.

(U) Embargoed Material: Material which is formally prohibited by U.S. law and administrative procedure from being transferred to certain recipients.

(U) Émigré: A person who departs from the person's country for any lawful reason, with the intention of permanently resettling elsewhere.

(U) Espionage: Intelligence activity directed toward the acquisition of intelligence through clandestine means.

(U) Fair Credit Reporting Act: Governs the acquisition of consumer reports from consumer reporting agencies.

(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 the control or policy direction; financial or material support; or leadership, assignments or discipline.

(U) Foreign Diplomatic Establishment: An embassy, mission, consulate, residential compound, or other premises owned or leased, and used for official purposes by a foreign government, whether or not recognized by the United States; premises of international organizations, as defined by Title 22, USC, Section 288; premises of establishments authorized to be treated as international organizations or diplomatic missions by specific statute (e.g., Title 22, USC,
Section 288f-1 through 288j); and the premises of establishments of foreign representatives to such international organizations.

(U) Foreign Intelligence: Information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, pertaining to foreign organizations or foreign persons, or international terrorists.

(U) Foreign Intelligence Agent: A person (other than a foreign IO) who is engaged in intelligence activities or sabotage, or international terrorism activities, for or on behalf of a foreign power, or who knowingly conspires with or aids or abets such a person in such activities.

(U) Foreign Intelligence Officer: A member of a foreign intelligence service.

(U) Foreign Liaison Officer: A government official who has been accredited to represent that government in the exchange and/or discussion of intelligence.

(U) Foreign Official: A foreign national in the United States who is: (a) acting in an official capacity for a foreign power, (b) attached to a foreign diplomatic establishment or an establishment under the control of a foreign power, or (c) employed by an international organization established under an agreement, to which the United States is a party.

(U) Foreign Power: (a) A foreign government or any component thereof, whether or not recognized by the United States; (b) A faction of a foreign nation or nations, not substantially composed of USPERs; (c) An entity that is openly acknowledged by (a) foreign government or governments to be directed and controlled by such foreign government or governments; (d) A group engaged in international terrorism or activities in preparation of international terrorism; (e) A foreign-based political organization, not substantially composed of USPERs; or (f) An entity that is directed and controlled by a foreign government or governments.

(U) Foreign Service National, also known as Locally Employed Staff (LES): An individual employed at a U.S. mission, who is a host country citizen.
(U) **Foreign Visitor**: A foreign national in the United States who is not a permanent resident alien of the United States.

(U) **FOUO (For Official Use Only)**: A marking, used on classified intelligence, which alerts readers that the information either clearly identifies, or would reasonably permit, ready identification of intelligence sources or methods, that are particularly susceptible to countermeasures that would either nullify or measurably reduce their effectiveness.

(U) **Front**: An organization or company which is used by a foreign intelligence service or terrorist group as a guise, to protect clandestine intelligence or terrorist activities.

(U) **Garrity Issue (Garrity v. New Jersey)**: Answers to questions under an explicit threat of termination by an employer cannot be used in a subsequent criminal proceeding.

(U) **Giglio Issue (Giglio v. United States)**: Obligation of the Government to provide the defense any evidence favorable to the accused regarding any witness.

(U) **Human Intelligence (HUMINT)**: Intelligence information that is collected from human sources, in either an overt or clandestine manner.

(U) **Illegal**: An officer or employee of an intelligence service, who has no overt connection with either the service or the government which controls it, and who is dispatched abroad for covert purposes.

(U) **Illegal Transfer**: The transfer of controlled, but unclassified technology.

(U) **Intelligence**: (a) Referring, collectively, to the functions, activities, or organizations that are involved in the process of planning, gathering, and analyzing information of potential value to decision makers; or (b) The product which results from the collection, collation, evaluation, analysis, integration, and interpretation of collected information.

(U) **Intelligence Activity**: An activity conducted for intelligence purposes or to affect political or governmental processes by, for, or on behalf of a foreign power.

(U) **Intelligence Community**: All components of a government which cooperate in the production of intelligence and CI.

(U) **Intelligence Officer**: A professionally trained member of an intelligence service.
Counterintelligence Division Policy Implementation Guide

(U) Intelligence Oversight Board (IOB): A committee of the President's Intelligence Advisory Board (PIAB). Among its responsibilities, the IOB must inform the President of intelligence activities that the IOB believes: (a) may be unlawful or contrary to executive order or presidential directive; and are not being adequately addressed by the Attorney General, the DNI, or the head of the department concerned; or (b) should be immediately reported to the President.

(U) International Terrorism: Activities that: (a) involve violent acts or acts dangerous to human life that violate federal, state, local, or tribal law, or would violate such law if committed within the United States or a state, local, or tribal jurisdiction; (b) 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 (c) occur totally outside the United States, or transcend national boundaries in terms of the means by which they are accomplished, the persons they appear intended to coerce or intimidate, or the locale in which their perpetrators operate or seek asylum.

(U) International Terrorist: An individual or group that knowingly engages in international terrorism or activities in preparation of international terrorism, or knowingly aids or abets any person engaged in such activities.

(U) Logical Sources of Information: Individuals who, by virtue of status or occupation, are believed to be in a position to provide valuable information regarding the subjects of investigations.

(U) National Security Letter: 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
Official Establishment: Any establishment controlled by a foreign government, regardless of its diplomatic or non-diplomatic status.

Open Storage: The storage of classified information within an accredited facility (though not within GSA-approved containers), while the facility is unoccupied by authorized personnel.

Operations Security (OPSEC): The process of detecting activities which, by themselves or combined with other data, may reveal the existence of sensitive information or operations.

Otherwise Illegal Activity: Any activity which would be illegal if it had not been appropriately authorized.

Need-to-Know: A determination by an authorized holder of classified information that access to that material is required by another person to perform a specific and authorized function. The recipient must possess an appropriate security clearance and necessary approvals.

Non-U.S. Person: An undocumented alien, or a foreign national lawfully in the United States, who is not a permanent resident alien.

NOFORN (Not Releasable To Foreign Nationals): A security designation which is used to identify classified intelligence which may not be released, in any form, to foreign governments, foreign nationals or non-U.S. citizens, without the originator's permission.

Notional: Referring to fabricated information.
Counterintelligence Division Policy Implementation Guide

(U) Permanent Resident Alien: A person who has received lawful permanent resident status in the United States, but who is not yet a U.S. citizen.

(U) Persona Non Grata: An official act, declaring a foreign national unacceptable or unwelcome in the country, usually when found to have been engaging in intelligence activities, or otherwise violating the law.

(U) Physical Search: Any physical intrusion within the United States into premises or property (including an examination by technical means), that is intended to result in a seizure, reproduction, inspection, or alteration of information, material, or property, under circumstances in which a person has a reasonable expectation of privacy, and a warrant would be required for law enforcement purposes.

(U) Positive Intelligence: Information about a foreign power that is significant to the national security, foreign relations or economic interests of the United States.

(U) PL 110 (Public Law 110): A law whereby vetted defectors are granted permanent resident alien status.

(U) President's Intelligence Advisory Board: An entity which has authority to: (a) assess the quality, quantity, and adequacy of intelligence collection, analysis and estimates, and counterintelligence and other intelligence activities; assess the adequacy of management, personnel, and organization in the intelligence community; and review the performance of all agencies of the federal government that are engaged in the collection, evaluation, or production of intelligence, or the execution of intelligence policy, and report the results of such assessments or reviews: (i) to the President, as necessary, but not less than twice each year; and (ii) to the and the heads of departments concerned, as the PIAB determines appropriate.

(U) Proprietary Economic Information: Any economic, scientific, or technical information; or design, process, procedure, formula, strategy or improvement (whether represented in a tangible or intangible form), which is not generally accessible or known in the trade, business, or scientific communities, and with which the owners have taken affirmative measures to prevent its entry into the public domain.

(U) Proprietary Enterprise: A sole proprietorship, partnership, corporation or other business entity which is created, owned or controlled, directly or indirectly by the FBI, in order to support an undercover operation, and whose relationship with the FBI is concealed (e.g. ).

(U) Proprietary Information and Technology: Sensitive material that is not yet embargoed or classified.

(U) Caution-Proprietary Information Involved (PROPIN): A marking used, with or without a security classification, to identify information which has been provided under an express or
implied understanding that the information will be protected as a proprietary trade secret, or proprietary data, believed to have actual or potential value.

(U) Publicly Available: Information which: (a) has been published or broadcast for general public consumption; (b) is available on request to any member of the general public; (c) could lawfully be seen or heard by any casual observer; or (d) is made available at a meeting open to the general public.

(U) Recruitment: The process of enlisting a person to work for an intelligence or CI service.

(U) Refugee: A person who: (a) has departed the person's country of nationality or habitual residence; (b) is unable to return to that country because of a well-founded fear of being persecuted for reasons of race, religion, nationality, membership in a particular social group, or political opinion; (c) does not possess another citizenship; and (d) has not acquired resident status in the country in which the person is currently residing.

(U) Residency—Legal: An intelligence establishment, which is overtly linked to its government.

(U) Right to Financial Privacy Act: An act that governs the acquisition of financial records of customers of financial institutions.

(U) Sanitization: The process of editing or otherwise altering intelligence products, to conceal sensitive sources, methods, capabilities, analytical procedures, and/or privileged information, in order to permit wider dissemination.

(U) Sensitive Compartmented Information (SCI): Classified information (concerning or derived from intelligence sources, methods, or analytical processes) which is required to be handled within formal access control systems.
Counterintelligence Division Policy Implementation Guide

(U) Sensitive Compartmented Information Facility (SCIF): An accredited area, room, group of rooms, building or installation where SCI may be stored, used, discussed, and/or processed.

(U) Sensitive Financial, Trade And Economic Policy Information: Data, details, facts, and/or knowledge, concerning strategy, methods, tactics, and/or procedures, which pertain to productivity, strategic goals, financial planning, and allocation of resources of the USG, U.S. corporations, establishments, and/or persons; which is not generally accessible or known in the financial, trade, business, or scientific community, the owners of which have taken affirmative measures to prevent its entry into the public domain.

(U) Special Access Program (SAP): Any program established under EO 12356, which imposes controls governing access to classified information, above and beyond those required by normal management and safeguarding practices.

(U) Substantially Composed Of U.S. Persons: In determining whether a group or organization is substantially composed of USPERs, the FBI should consider not only the citizenship or resident alien status of members of the group or organization in the United States, but also the relationship of that group or organization to a foreign-based international organization. If the group or organization in the United States operates directly under the control of the international organization, and has no independent program or activities in the United States, membership of the entire international organization should be considered, in determining if it is substantially composed of USPERs. If, however, the group or organization based in the United States has programs or activities separate from, or in addition to, those directed by the international organization, only the U.S. membership should be considered in determining whether it is substantially composed of USPERs.

(U) Tearline: A physical line on an intelligence message or document separating categories of information that have been approved for disclosure and release. Normally, the intelligence below the tearline is that which has been previously cleared for disclosure or release.
Counterintelligence Division Policy Implementation Guide

(U) **Terrorist**: An individual who engages in terrorist activities, which are intended to: (a) intimidate or coerce a civilian population; (b) influence the policy of a government by intimidation or coercion; or (c) affect the conduct of a government, by assassination or kidnapping.

(U) **Threat Analysis**: A comprehensive assessment of the threat posed, not only by an opposition intelligence service, but also those organizations and individuals whose interests are inimical to those of the United States.

(U) **Undercover Operation**: An operation that involves a series of related "undercover activities" over a period of time by an "undercover employee." A series of related undercover activities consists of more than five separate substantive contacts by an undercover employee with the individuals under investigation.

(U) **Undisclosed Participation (UDP)**: Joining or otherwise participating in any organization in the United States, on behalf of an agency within the USIC, without disclosing the IC tie to an appropriate official of that organization.

(U) **U.S. Economic Interests**: Those financial, trade, research and development, technological, and policy issues which define U.S. strategic economic goals, including: (a) the maintenance of U.S. economic health, (b) providing a higher standard of living, and (c) organizing a sustainable economic order.

(U) **U.S. Person (USPER)**: Any of the following, but not including any association or corporation that is a foreign power, as defined in DIOG subpart G.1.-3.: (a) an individual who is a United States citizen or an alien lawfully admitted for permanent residence; (b) an unincorporated association substantially composed of individuals who are United States persons; or (c) a corporation incorporated in the United States.

(U) **Volunteers**: (a) CHSs who approach the FBI offering to provide information; or (b) Individuals who are directed to initiate contacts with targeted groups, and to offer them their services.
(U) Walk-in: Generally speaking, an individual who literally walks into an FBI office with an offer to provide information of value to the FBI's CI, foreign intelligence, or international terrorism programs.
## (U) Appendix D: Acronyms

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AD</td>
<td>Assistant Director</td>
</tr>
<tr>
<td>ADIC</td>
<td>Assistant Director in Charge</td>
</tr>
<tr>
<td>AGG-Dom</td>
<td>Attorney General’s Guidelines for Domestic FBI Operations</td>
</tr>
<tr>
<td>AG</td>
<td>Attorney General</td>
</tr>
<tr>
<td>AGG CHS</td>
<td>Attorney General’s Guidelines Regarding the Use of FBI Confidential Human Sources</td>
</tr>
<tr>
<td>ASAC</td>
<td>Assistant Special Agent in Charge</td>
</tr>
<tr>
<td>CBP</td>
<td>Customs and Border Protection</td>
</tr>
<tr>
<td>CD</td>
<td>Counterintelligence Division</td>
</tr>
<tr>
<td>CDC</td>
<td>Chief Division Counsel</td>
</tr>
<tr>
<td>CHS</td>
<td>Confidential Human Source</td>
</tr>
<tr>
<td>CHSPM</td>
<td>Confidential Human Source Policy Manual</td>
</tr>
<tr>
<td>CHSVSM</td>
<td>Confidential Human Source Validation Standards Manual</td>
</tr>
<tr>
<td>CI</td>
<td>Counterintelligence</td>
</tr>
<tr>
<td>CTD</td>
<td>Counterterrorism Division</td>
</tr>
<tr>
<td>DAD</td>
<td>Deputy Assistant Director</td>
</tr>
<tr>
<td>DI</td>
<td>Directorate of Intelligence</td>
</tr>
<tr>
<td>DIDO</td>
<td>Designated Intelligence Disclosure Official</td>
</tr>
<tr>
<td>DIIOG</td>
<td>Domestic Investigations and Operations Guide</td>
</tr>
<tr>
<td>DOD</td>
<td>Department of Defense</td>
</tr>
<tr>
<td>DOJ</td>
<td>Department of Justice</td>
</tr>
<tr>
<td>DOS</td>
<td>Department of State</td>
</tr>
<tr>
<td>EAD</td>
<td>Executive Assistant Director</td>
</tr>
<tr>
<td>EC</td>
<td>Electronic Communication</td>
</tr>
<tr>
<td>ELSUR</td>
<td>Electronic Surveillance</td>
</tr>
</tbody>
</table>
Counterintelligence Division Policy Implementation Guide

EO  Executive Order
FBI  Federal Bureau of Investigation
FBIHQ  Federal Bureau of Investigation Headquarters
FIG  Field Intelligence Group

FISUR  Physical Surveillance
HIMU  Human Intelligence Management Unit
HUMINT  Human Intelligence
ICE  Immigration and Customs Enforcement

IOD  International Operations Division
INR  Bureau of Intelligence and Research
INS  Immigration and Naturalization Service
Legat  Legal Attaché
LHM  Letterhead Memorandum

NCIC  National Crime Information Center
NFIPM  National Foreign Intelligence Policy Manual

NSB  National Security Branch
NSLB  National Security Law Branch

OGC  Office of the General Counsel
OO  Office of Origin

RP&G  Reference and Procedure Guide
SA  Special Agent
SAC  Special Agent in Charge

D-2

ACLURM007074
### Counterintelligence Division Policy Implementation Guide

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SCI</td>
<td>Sensitive Compartmented Information</td>
</tr>
<tr>
<td>SCION</td>
<td>Sensitive Compartmented Information Operational Network</td>
</tr>
<tr>
<td>SSA</td>
<td>Supervisory Special Agent</td>
</tr>
<tr>
<td>UCA</td>
<td>Undercover Agent</td>
</tr>
<tr>
<td>UCO</td>
<td>Undercover Operation</td>
</tr>
<tr>
<td>USG</td>
<td>United States Government</td>
</tr>
<tr>
<td>USPER</td>
<td>United States Person, US Person; U.S. Person; USP; USPs; USPERS</td>
</tr>
<tr>
<td>WMD</td>
<td>Weapons of Mass Destruction</td>
</tr>
<tr>
<td>WMDD</td>
<td>Weapons of Mass Destruction Directorate</td>
</tr>
</tbody>
</table>
(U) Appendix E: Types of Investigations

<table>
<thead>
<tr>
<th>INITIATION &amp; APPROVAL</th>
<th>EXTENSION &amp; CLOSING</th>
<th>NOTIFICATION</th>
<th>AUTHORIZED INVESTIGATIVE METHODS</th>
</tr>
</thead>
<tbody>
<tr>
<td>FIELD OFFICE</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SSA approval; opening EC to FBIHQ unit</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FIELD OFFICE</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CDC review and SAC approval; opening EC (+LHM) to FBIHQ unit and section</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FBIHQ</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>UC approval with written notification to applicable Field Office</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FBIHQ</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>OGC review and SC approval with written notification to applicable Field Office</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>