DOMESTIC INVESTIGATIONS AND OPERATIONS GUIDE

FEDERAL BUREAU OF INVESTIGATION
RELEASED FEBRUARY 27, 2024

NOTICE OF SUPERSESSION AND UPDATE:

This document amends and supersedes the previous *Domestic Investigations and Operations Guide* (DIOG), released January 3, 2024.

PRINTED VERSIONS:

THE OFFICIAL VERSION OF THE DIOG IS POSTED ONLINE AT THE POLICY LIBRARY. PRINTED COPIES OF THE DIOG MAY NOT CONTAIN THE MOST CURRENT POLICY REQUIREMENTS.

CONTACT INFORMATION:

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

The Resource Planning Office (RPO), Internal Policy Office (IPO) at

HQ_DIV00_INTERNAL_POLICY_OFFICE
or the Office of the General Counsel (OGC)

PRIVILEGED INFORMATION:

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

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

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

TABLE OF CONTENTS

1 (U) Scope and Purpose 1-1

1.1 (U) Scope 1-1

1.2 (U) Purpose 1-1

2 (U) General Authorities and Principles 2-1

2.1 (U) Authority of the Attorney General's Guidelines for Domestic FBI Operations 2-1

2.2 (U) General FBI Authorities under AGG-Dom 2-1

2.2.1 (U) Conduct Investigations and Collect Intelligence and Evidence 2-1

2.2.2 (U) Provide Investigative Assistance 2-2

2.2.3 (U) Conduct Intelligence Analysis and Planning 2-2

2.2.4 (U) Retain and Share Information 2-2

2.3 (U) FBI as an Intelligence Agency 2-2

2.4 (U) FBI Lead Investigative Authorities 2-2

2.4.1 (U) Introduction 2-2

2.4.2 (U) Terrorism and Counterterrorism Investigations 2-3

2.4.2.1 (U) Federal Crimes of Terrorism 2-3

2.4.2.2 (U) Additional Offenses Not Defined as "Federal Crimes of Terrorism" 2-7

2.4.2.3 (U//~~FOUO~~) NSPD-46/HSPD-15, "U.S. Policy and Strategy in the War on Terror" 2-8

2.4.3 (U) Counterintelligence and Espionage Investigations 2-8

2.4.3.1 (U) Espionage Investigations of Persons in United States Diplomatic Missions Abroad 2-8

2.4.3.2 (U) Investigations of Unauthorized Disclosure of Classified Information to a Foreign Power or Agent of a Foreign Power 2-9

2.4.4 (U) Criminal Investigations 2-9

2.4.4.1 (U) Investigations Of Aircraft Piracy and Related Violations 2-9

2.4.4.2 (U) Violent Crimes Against Travelers 2-9

2.4.4.3 (U) Felonious Killings of State and Local Law Enforcement officers 2-9

2.4.4.4 (U) Investigations of Serial Killings 2-9

2.4.5 (U) Authority of an FBI Special Agent 2-9

2.5 (U) Status as Internal Guidance 2-10

2.6 (U) Departure from the AGG-Dom (AGG-Dom I.D.3) 2-10

2.6.1 (U) Definition 2-10

2.6.2 (U) Departure from the AGG-Dom in Advance 2-10
2.6.3 (U) Emergency Departures from the AGG-Dom 2-11
2.6.4 (U) Records of Departures from the AGG-Dom 2-11
2.7 (U) Departures from the DIOG and DIOG-Related Policies 2-11
2.7.1 (U) Definition 2-11
2.7.2 (U) Departure from the DIOG and DIOG-Related Policies 2-11
2.7.3 (U) Emergency Departures from the DIOG and DIOG-Related PGs 2-12
2.7.4 (U) Records of Departures from the DIOG and DIOG-Related Policies 2-12
2.8 (U) Discovery of Non-compliance with DIOG and DIOG-Related Policies Requirements after-the-fact 2-13
2.8.1 (U) Substantial Non-Compliance with the DIOG and DIOG-Related Policies 2-13
2.8.1.1 (U) Substantial Non-Compliance 2-13
2.8.1.2 (U) Other Non-Compliance 2-13
2.8.2 (U) Documentation of Substantial non-Compliance 2-14
2.8.3 (U) Reporting Authorities 2-14
2.8.4 (U) Role of OIC and OGC 2-14
2.8.4.1 (U) Discontinuation of Reporting 2-15
2.8.5 (U) Potential IOB Matters Involving the Reports of Substantial Non-Compliance 2-15
2.8.6 (U) Reporting Non-Compliance with Policy Guides 2-15
2.8.7 (U) Reporting Non-Compliance with Other FBI Policies and Procedures (Outside the DIOG) 2-15
2.9 (U) Other FBI Activities Not Limited by AGG-Dom 2-15
2.10 (U) Use of Classified Investigative Technologies 2-16
2.11 (U) Application of AGG-Dom and DIOG 2-16
2.12 (U) Joint Investigations 2-17
3 (U) Core Values, Roles, and Responsibilities 3-1
3.1 (U) The FBI's Core Values 3-1
3.1.1 (U) Compliance 3-1
3.2 (U) Investigative Authority, Roles and Responsibility of the Director's Office 3-2
3.2.1 (U) Director's Authority, Roles and Responsibility 3-2
3.2.2 (U) Deputy Director's Authority, Roles and Responsibility 3-2

3.3 (U) Special Agent/Task Force Officer (TFO)/Task Force Member (TFM)/Task Force Participant (TFP)/FBI Contractor/Others - Roles and Responsibilities 3-3
3.3.1 (U) Roles and Responsibilities 3-3
3.3.1.1 (U) Training 3-3
3.3.1.2 (U) Investigative Activity 3-3
3.3.1.3 (U) Privacy and Civil Liberties 3-3
3.3.1.4 (U) Protect Rights 3-3
3.3.1.5 (U) Compliance 3-4
3.3.1.6 (U) Report Non-Compliance 3-4
3.3.1.7 (U) Assist Victims 3-4
3.3.1.8 (U) Obtain Approval 3-4
3.3.1.9 (U) Attribute Information to Originator in Reports 3-4
3.3.1.10 (U) Serve as Investigation ("Case") Manager 3-4
3.3.1.11 (U) Create and Maintain Records/Files 3-5
3.3.1.12 (U) Index Documents 3-5
3.3.1.13 (U) Seek Federal Prosecution 3-5
3.3.1.14 (U) Retain Original Notes Made During An Investigation 3-5
3.3.2 (U) Definitions of Task Force Officer (TFO), Task Force Member (TFM), and Task Force Participant (TFP) 3-6
3.3.2.1 (U) Task Force Officer 3-6
3.3.2.2 (U) Task Force Member 3-6
3.3.2.3 (U) Task Force Participant 3-7
3.4 (U) Intelligence Analysts (IA) and Professional Investigative Staff 3-7
3.4.1 (U) Roles and Responsibilities 3-7
3.4.1.1 (U) Intelligence Analysts 3-7
3.4.1.2 (U) Professional Investigative Staff 3-8
3.4.2 (U) Investigative or Intelligence Activities 3-8
3.4.2.1 (U) Training 3-8
3.4.2.2 (U) Investigative Activities 3-8
3.4.2.3 (U) Assignment as Case Managers and Participants 3-8
3.4.2.4 (U//~~FOUO~~) Use and Approval Requirements of Authorized Investigative Methods 3-9
3.4.2.4.1 (U//~~FOUO~~) Methods Available Prior to Opening an Assessment and During an Assessment 3-9
3.4.2.4.2 (U//~~FOUO~~) Assisting SAs/TFOs in the Use of Other Investigative Methods in Assessments, Preliminary Investigations, and Full Investigations 3-9

3.4.2.5 (U) Privacy and Civil Liberties 3-10
3.4.2.6 (U) Protect Rights 3-10
3.4.2.7 (U) Compliance 3-10
3.4.2.8 (U) Report Noncompliance 3-10
3.4.2.9 (U) Assist Victims 3-10
3.4.2.10 (U) Obtain Approval 3-10
3.4.2.11 (U) Attribute Information to Originator in Reports 3-11
3.4.2.12 (U) Serve as Assessment ("Case") Manager 3-11
3.4.2.13 (U) Create and Maintain Records and Files 3-11
3.4.2.14 (U) Index Documents 3-11
3.5 (U) Supervisor Roles and Responsibilities 3-11
3.5.1 (U) Supervisor Defined 3-11
3.5.2 (U) Supervisor Responsibilities 3-12
3.5.2.1 (U) Approval/Review of Investigative or Collection Activities 3-12
3.5.2.2 (U) Oral Authority/Approval 3-13
3.5.2.3 (U) No Self-Approval Rule 3-13
3.5.2.4 (U) Ensure Compliance with U.S. Regulations and Other Applicable Legal and Policy Requirements 3-14
3.5.2.5 (U) Training 3-14
3.5.2.6 (U) Protect Civil Liberties and Privacy 3-14
3.5.2.7 (U) Report Compliance Concerns 3-14
3.5.2.8 (U) Non-Retaliation Policy 3-14
3.5.2.9 (U) Create and Maintain Records/Files 3-14
3.5.2.10 (U//~~FOUO~~) Certifications for Immigration Benefits 3-15
3.5.3 (U) Delegation and Succession in the FBI 3-15
3.5.3.1 (U) Delegation 3-15
3.5.3.2 (U) Succession: Acting Supervisory Authority 3-16
3.5.3.3 (U) Documentation 3-16
3.5.3.3.1 (U//~~FOUO~~) "Delegations of Authority Related to Senior Executives" – File 319X-HQ-A1700684-XX 3-16
3.5.3.3.2 (U//~~FOUO~~) "Delegations of Authority Related to Non-Senior Executives" (Including All Senior Executive Service [SES] and Other Supervisory Management Officials) and All ADHOC Designations – File 319X-HQ-A1700685-XX 3-16
3.5.3.3.3 (U//~~FOUO~~) Succession Plans – File 319X-HQ-A1538387 3-17
3.5.4 (U) File Reviews and Justification Reviews 3-17
3.5.4.1 (U) Overview 3-17

3.5.4.2 (U) Types of Files/Investigations Requiring File Reviews and Justification Reviews 3-18
3.5.4.3 (U) Frequency of File Reviews 3-18
3.5.4.4 (U) Delegation of File Reviews 3-18
3.5.4.5 (U) Predicated Investigations and Type 3, 4, and 6 Assessment – File Review Requirements 3-19
3.5.4.6 (U) Type 1 and 2 Assessments – Justification Review Requirements 3-22
3.5.4.7 (U) Type 5 Assessments – File Review Requirements 3-22
3.5.4.8 (U) Documentation of File Reviews 3-23
3.5.4.9 (U) File Review Example 3-23
3.6 (U) Chief Division Counsel (CDC) Roles and Responsibilities 3-24
3.7 (U) Office of the General Counsel (OGC) Roles and Responsibilities 3-24
3.8 (U) Internal Policy Office (IPO) Roles and Responsibilities 3-25
3.9 (U) Office of Integrity and Compliance (OIC) Roles and Responsibilities 3-26
3.10 (U) Operational Program Manager Roles and Responsibilities 3-26
3.11 (U) Division Compliance Officer Roles and Responsibilities 3-27
4 (U) Privacy and Civil Liberties, and Least Intrusive Methods 4-1
4.1 (U) Civil Liberties and Privacy 4-1
4.1.1 (U) Overview 4-1
4.1.2 (U) Purpose of Investigative Activity 4-1
4.1.3 (U) Oversight and Self-Regulation 4-2
4.2 (U) Protection of First Amendment Rights 4-4
4.2.1 (U) Free Speech 4-7
4.2.2 (U) Exercise of Religion 4-8
4.2.3 (U) Freedom of the Press 4-9
4.2.4 (U) Freedom of Peaceful Assembly and to Petition the Government for Redress of Grievances 4-10
4.3 (U) Equal Protection Under the Law 4-11
4.3.1 (U) Introduction 4-11
4.3.2 (U) Policy Principles 4-12
4.3.3 (U) Guidance on the Use of Race, Ethnicity, Gender, National Origin, Religion, Sexual Orientation, or Gender Identity in Assessments and Predicated Investigations 4-14

4.3.3.1 (U) Individual Race, Ethnicity, Gender, National Origin, Religion, Sexual Orientation, or Gender Identity as a Factor 4-14
4.3.3.2 (U) Community Race, Ethnicity, Gender, National Origin, Religion, Sexual Orientation, or Gender Identity as a Factor 4-14
4.3.3.2.1 (U) Collecting and Analyzing Demographics 4-14
4.3.3.2.2 (U) Geo-Mapping Ethnic/Racial Demographics 4-15
4.3.3.2.3 (U) General Ethnic/Racial Behavior 4-15
4.3.3.2.4 (U) Specific and Relevant Ethnic Behavior 4-15
4.3.3.2.5 (U) Exploitive Ethnic Behavior 4-16
4.4 (U) Least Intrusive Method 4-16
4.4.1 (U) Overview 4-16
4.4.2 (U) General Approach to Least Intrusive Method Concept 4-17
4.4.3 (U) Determining Intrusiveness 4-17
4.4.4 (U) Standard for Balancing Intrusion and Investigative Requirements 4-19
4.4.5 (U) Conclusion 4-20
5 (U) Assessments 5-1
5.1 (U) Assessment Purpose and Scope 5-1
5.1.1 (U) Situational Examples 5-2
5.1.1.1 (U) Example A 5-2
5.1.1.2 (U) Example B 5-3
5.1.1.3 (U) Example C 5-3
5.1.1.4 (U) Example D 5-3
5.1.1.1 (U) Example E 5-4
5.1.1.2 (U) Example F 5-4
5.1.1.3 (U) Example G 5-4
5.2 (U) Civil Liberties and Privacy 5-4
5.3 (U) Complaint Processing 5-5
5.3.1 (U) Overview 5-5
5.3.2 (U) Complaint Processing Categories 5-6
5.3.3 (U) Intake of Complaints 5-7
5.3.3.1 (U) Threat to Life Complaints 5-7
5.3.3.2 (U) Time Sensitive Complaints 5-8
5.3.3.3 (U) Routine Complaints 5-8
5.3.4 (U) Complaints Processed by the National Threat Operations Center 5-8
5.3.4.1 (U//~~FOUO~~) NTOC Processing of TTL and Time Sensitive Complaints and Tips 5-9
5.3.5 (U) Complaints Processed by Field Offices 5-9

5.3.5.1 (U//~~FOUO~~) Field Office Time Frame for Completing and Submitting a Guardian Incident 5-10
5.3.5.2 (U) Field Office Time Frame for Processing a Guardian Incident 5-10
5.3.6 (U) Supervisory Evaluation of a Complaint or Guardian Incident 5-11
5.3.6.1 (U) Option 1: Assign the Complaint or Guardian Incident for Processing 5-12
5.3.6.2 (U) Option 2: Convert the Complaint or Guardian Incident to an Assessment or Predicated Investigation 5-12
5.3.6.3 (U) Option 3: Close the Complaint or Guardian Incident as "Information Only" - Refer to Other Government Agency 5-12
5.3.6.4 (U) Option 4: Close the Complaint or Guardian Incident – No Investigative Activity Warranted at this Time 5-13
5.3.6.5 (U) Option 5: Close the Complaint or Guardian Incident - The Information Received is Based Solely on Activities that are Protected by the First Amendment or on Race, Ethnicity, Gender, National Origin, Religion, Disability, Sexual Orientation, or Gender Identity of the Subject, or a Combination of Only Such Factors. 5-14
5.3.6.6 (U//~~FOUO~~) Additional Supervisory Requirements for a Closing Complaint or Guardian Incident 5-14
5.3.6.7 (U//~~FOUO~~) Time Frame for Supervisory Evaluation of a Submitted Guardian Incident 5-15
5.3.7 (U//~~FOUO~~) Routine Guardian Incident Justification Reviews (Criminal, Cyber, and Counterintelligence) 5-15
5.3.8 (U) Documentation of Investigative Methods Authorized Prior to Opening an Assessment or Predicated Investigation 5-17
5.3.9 (U) Investigative Methods Authorized During the Processing of Complaints (i.e., Investigative Activities Permitted Prior to Opening an Assessment or Predicated Investigation) 5-17
5.3.9.1 (U) Public Information 5-18
5.3.9.2 (U) Records or Information - FBI and DOJ 5-18
5.3.9.3 (U) Records or Information – Other Federal, State, Local, Tribal, or Foreign Government Agency 5-18
5.3.9.4 (U) Online Services and Resources 5-18
5.3.9.5 (U) Clarifying Interview 5-18
5.3.9.6 (U) Information Voluntarily Provided by Governmental or Private Entities 5-18
5.3.10 (U//~~FOUO~~) Required Records Checks for All Initial Processing 5-19
5.3.11 (U) Convert, Transfer, or Recategorize a Guardian Incident During the Processing Phase 5-20
5.3.12 (U) Situational Complaint Examples 5-20
5.3.12.1 (U) Example A 5-21

5.3.12.2 (U) Example B 5-21
5.3.12.3 (U) Example C: 5-21
5.4 (U) Five Types of Assessments (*AGG-Dom*, Part II.A.3.) 5-22
5.4.1 (U) Assessment Types 5-22
5.5 (U) Standards for Opening or Approving an Assessment 5-22
5.6 (U) Position Equivalents, Effective Date, Duration, Documentation, Approval, Notice, File Review, and Responsible Entity 5-23
5.6.1 (U) Field Office and FBIHQ Position Equivalents 5-23
5.6.2 (U) Effective Date of Assessments 5-23
5.6.3 (U) Assessment Types 5-24
5.6.3.1 (U) Type 1 & 2 Assessments 5-24
5.6.3.1.1 (U) Duration 5-25
5.6.3.1.2 (U) Documentation 5-25
5.6.3.1.3 (U) Approval to Open 5-25
5.6.3.1.4 (U) Sensitive Investigative Matters 5-25
5.6.3.1.5 (U) Undisclosed Participation (UDP) 5-27
5.6.3.1.6 (U) Notice 5-27
5.6.3.1.7 (U) Justification Review 5-27
5.6.3.1.8 (U) Responsible Entity 5-27
5.6.3.1.9 (U) Type 1 & 2 Assessment Closing 5-28
5.6.3.1.10 (U) Examples and Scenarios of Type 1 & 2 Assessments 5-29
5.6.3.2 (U) Type 3 Assessments 5-30
5.6.3.2.1 (U) Duration 5-31
5.6.3.2.2 (U) Documentation 5-31
5.6.3.2.3 (U) Approval 5-32
5.6.3.2.4 (U) Sensitive Investigative Matters (SIM) 5-32
5.6.3.2.5 (U) Undisclosed Participation (UDP) 5-32
5.6.3.2.6 (U) Notice 5-32
5.6.3.2.7 (U) File Review 5-33
5.6.3.2.8 (U) Responsible Entity 5-33
5.6.3.2.9 (U) Authorized Investigative Methods in Type 3 Assessments 5-33
5.6.3.2.10 (U) Type 3 Assessment Closing 5-33
5.6.3.2.11 (U) Examples of Type 3 Assessments 5-33
5.6.3.3 (U) Type 4 Assessments 5-35
5.6.3.3.1 (U) Duration 5-36
5.6.3.3.2 (U) Documentation 5-36
5.6.3.3.3 (U) Approval 5-36
5.6.3.3.4 (U) Sensitive Investigative Matters (SIM) 5-36

5.6.3.3.5 (U) Notice 5-37
5.6.3.3.6 (U) File Review 5-37
5.6.3.3.7 (U) Responsible Entity 5-37
5.6.3.3.8 (U) Type 4 Assessment Closing 5-37
5.6.3.3.9 (U) Examples of Type 4 Assessments 5-37
5.6.3.4 (U) Type 5 Assessments 5-38
5.6.3.4.1 (U) Phases of Type 5 Assessments 5-39
5.6.3.4.2 (U) Duration 5-41
5.6.3.4.3 (U) Documentation 5-41
5.6.3.4.4 (U) Approval 5-43
5.6.3.4.5 (U) Notice 5-44
5.6.3.4.6 (U) File Review 5-44
5.6.3.4.7 (U) Responsible Entity 5-44
5.6.3.4.8 (U) Authorized Investigative Methods in Type 5 Assessments 5-44
5.6.3.4.9 (U) Closing Type 5 Assessments 5-45
5.6.3.4.10 (U) Examples of Type 5 Assessments 5-46
5.6.3.5 (U) Type 6 Assessments 5-48
5.6.3.5.1 (U) Duration 5-49
5.6.3.5.2 (U) Documentation 5-49
5.6.3.5.3 (U) Approval 5-49
5.6.3.5.4 (U) Sensitive Investigative Matters (SIM) 5-50
5.6.3.5.5 (U) Notice 5-50
5.6.3.5.6 (U) File Review 5-50
5.6.3.5.7 (U) Responsible Entity 5-50
5.6.3.5.8 (U) Type 6 Assessment Closing 5-50
5.6.3.5.9 (U) Examples/Scenarios of Type 6 Assessments 5-50

5.7 (U) Sensitive Investigative Matters (SIM) in Assessments and Sensitive Potential CHS or Sensitive Characteristic Designations in Type 5 Assessments 5-51

5.7.1 (U) SIM Categories in Assessments 5-51
5.7.2 (U) Academic Nexus in Assessments 5-52

5.8 (U) Standards for Opening or Approving the Use of an Authorized Investigative Method 5-52

5.9 (U) Authorized Investigative Methods in Assessments 5-53

5.9.1 (U) Type 1 & 2, Type 3, Type 4, and Type 6 Assessments 5-53
5.9.2 (U) Type 5 Assessments 5-53

5.10 (U) Other Investigative Methods Not Authorized During Assessments 5-54

5.11 (U) Intelligence Collection (i.e., Incidental Collection) 5-54
5.12 (U) Retention and Dissemination of Privacy Act Records 5-55
5.12.1 (U) Marking Closed Guardian Incidents and Assessments That Contain Personal Information 5-55
5.12.1.1 (U) Type 1 & 2 Assessments and Processing Complaints or Guardian Incidents 5-56
5.12.1.2 (U) Type 3, 4, and 6 Assessments 5-56
5.12.1.3 (U) Type 5 Assessments 5-56
5.13 (U) Assessment File Records Management and Retention 5-56
5.13.1 (U) Pending Inactive Status 5-57
5.14 (U) Other Program Specific Investigation Requirements 5-57
6 (U) Preliminary Investigations 6-1
6.1 (U) Overview 6-1
6.2 (U) Purpose and Scope 6-1
6.3 (U) Civil Liberties and Privacy 6-1
6.4 (U) Legal Authority 6-2
6.4.1 (U) Criminal Investigations 6-2
6.4.2 (U) Threats to the National Security 6-2
6.5 (U) Predication 6-3
6.6 (U) Standards for Opening or Approving a Preliminary Investigation 6-3
6.7 (U) Opening Documentation, Approval, Effective Date, Notice, Extension, Pending Inactive Status, Conversion, and File Review 6-3
6.7.1 (U) Opening Documentation 6-3
6.7.1.1 (U) Approval/Effective Date/Notice 6-4
6.7.1.2 (U) Additional Requirements for Presidential and Congressional Candidates and Campaigns 6-6
6.7.2 (U) Extension 6-7
6.7.2.1 (U) Good Cause 6-7
6.7.3 (U) Pending Inactive Status 6-8
6.7.4 (U) Conversion to Full Investigation 6-8
6.7.5 (U) File Review 6-8
6.8 (U) Standards for Opening or Approving the Use of an Authorized Investigative Method in Preliminary Investigations 6-8

6.9 (U) Authorized Investigative Methods in Preliminary Investigations . 6-8
6.10 (U) Sensitive Investigative Matters (SIM) in Preliminary Investigations 6-10
6.10.1 (U) SIM Categories in Preliminary Investigations 6-10
6.10.2 (U) Academic Nexus in Preliminary Investigations 6-10
6.11 (U) Intelligence Collection (i.e., Incidental Collection) 6-10
6.12 (U) Standards for Approving the Closing of a Preliminary Investigation 6-11
6.12.1 (U) Standards 6-11
6.12.2 (U) Approval Requirements to Close 6-12
6.13 (U) Other Program-Specific Investigative Requirements 6-13
7 (U) Full Investigations 7-1
7.1 (U) Overview 7-1
7.2 (U) Purpose and Scope 7-1
7.3 (U) Civil Liberties and Privacy 7-1
7.4 (U) Legal Authority 7-2
7.4.1 (U) Criminal Investigations 7-2
7.4.2 (U) Threats to the National Security 7-3
7.4.3 (U) Foreign Intelligence Collection 7-3
7.5 (U) Predication 7-3
7.6 (U) Standards for Opening or Approving a Full Investigation 7-4
7.7 (U) Opening Documentation, Approval, Effective Date, Notice, Pending Inactive Status, File Review, and Letter Head Memorandum 7-4
7.7.1 (U) Opening Documentation 7-4
7.7.1.1 (U) Approval/Effective Date/Notice 7-4
7.7.1.2 Additional Requirements for Presidential and Congressional Candidates and Campaigns 7-7
7.7.2 (U) Pending Inactive Status 7-8
7.7.3 (U) File Review 7-8
7.7.4 (U) Annual Letterhead Memorandum 7-8
7.8 (U) Standards for Opening or Approving the Use of an Authorized Investigative Method in Full Investigations 7-9

7.9 (U) Authorized Investigative Methods in Full Investigations 7-9
7.10 (U) Sensitive Investigative Matters (SIM) in Full Investigations..... 7-10
7.10.1 (U) SIM Categories in Full Investigations 7-10
7.10.2 (U) Academic Nexus in Full Investigations 7-10
7.11 (U) Intelligence Collection (i.e., Incidental Collection) 7-11
7.12 (U) Standards for Approving the Closing of a Full Investigation..... 7-12
7.12.1 (U) Standards 7-12
7.12.2 (U) Approval Requirements to Close 7-13
7.13 (U) Other Program Specific Investigative Requirements..... 7-13
8 (U) Enterprise Investigations (EI) 8-1
8.1 (U) Overview 8-1
8.2 (U) Purpose, Scope and Definitions 8-1
8.3 (U) Civil Liberties and Privacy..... 8-1
8.4 (U) Predication 8-2
8.5 (U) Standards for Opening or Approving an Enterprise Investigation 8-3
8.6 (U) Opening Documentation, Effective Date, Approval, Notice, and File Review 8-4
8.6.1 (U) Opening Documentation 8-4
8.6.2 (U) Effective Date 8-4
8.6.3 (U) Approval Requirements for Opening an Enterprise Investigation (EI) 8-5
8.6.3.1 (U) EI Opened by a Field Office 8-5
8.6.3.2 (U) Enterprise Investigations Opened by FBIHQ 8-5
8.6.3.3 (U) Notice Requirements to DOJ 8-5
8.6.3.4 (U) Additional Requirements for Presidential and Congressional Candidates and Campaigns 8-5
8.6.4 (U) Sensitive Investigative Matters 8-6
8.6.4.1 (U//~~FOUO~~) SIM Opened by a Field Office 8-6
8.6.4.2 (U//~~FOUO~~) SIM Opened by FBIHQ 8-7
8.6.5 (U) File Review 8-8
8.6.6 (U) Pending Inactive Status 8-9
8.7 (U) Authorized Investigative Methods in an Enterprise Investigation 8-9

8.8 (U) Sensitive Investigative Matters (SIM) in Enterprise Investigations 8-9
8.8.1 (U) SIM Categories in Enterprise Investigations 8-9
8.8.2 (U) Academic Nexus in Enterprise Investigations 8-9
8.9 (U) Intelligence Collection (i.e., Incidental Collection) 8-10
8.10 (U) Standards for Approving the Closing of an Enterprise Investigation 8-11
8.10.1 (U) Standards 8-11
8.10.2 (U) Approval Requirements to Close 8-11
9 (U) Foreign Intelligence 9-1
9.1 (U) Overview 9-1
9.2 (U) Purpose and Scope 9-2
9.3 (U) Civil Liberties and Privacy 9-2
9.4 (U) Legal Authority 9-3
9.4.1 (U) Full Investigation Activities 9-4
9.5 (U) General Requirements and FBIHQ Standards for Approving the Opening of Positive Foreign Intelligence Investigations 9-4
9.5.1 (U) General Requirements and Program Responsibilities 9-4
9.5.2 (U) Standards for Opening a Full Investigation to Collect Positive Foreign Intelligence 9-4
9.6 (U) Opening Documentation, Approval, Effective Date, and File Review 9-5
9.6.1 (U) Opening by a Field Office With FBIHQ HPMU UC Approval or Opening by FBIHQ 9-5
9.6.1.1 (U) Approval to Open a Full PFI Investigation 9-5
9.6.1.1.1 (U) Effective Date 9-5
9.6.1.2 (U) Approval to Open a Full PFI Investigation Involving a Sensitive Investigative Matter (SIM) 9-5
9.6.1.2.1 (U//~~FOUO~~) SIM Full PFI Investigation Opened by a Field Office 9-5
9.6.1.2.2 (U) SIM Full PFI Investigation Opened by FBIHQ 9-6
9.6.1.2.3 (U) Effective Date 9-6
9.6.1.2.4 (U) Additional Requirements for Presidential and Congressional Candidates and Campaigns 9-6
9.6.2 (U) Pending Inactive Status 9-7
9.6.3 (U) Notice to DOJ 9-7

9.6.3.1 (U) For a Full PFI Investigation 9-7
9.6.4 (U) Duration 9-7
9.6.5 (U) File Review 9-7
9.6.5.1 (U) Full Investigations 9-7
9.6.6 (U) Annual Letterhead Memorandum 9-8
9.6.6.1 (U) Field Office Responsibility 9-8
9.6.6.2 (U) FBIHQ Responsibility 9-8
9.7 (U) Standards for Opening or Approving the Use of an Authorized Investigative Method in a Full Positive Foreign Intelligence Investigation 9-8
9.8 (U) Authorized Investigative Methods in a Full Positive Foreign Intelligence Investigation 9-9
9.9 (U) Investigative Methods Not Authorized During A Full Positive Foreign Intelligence Investigation 9-10
9.10 (U) Sensitive Investigative Matters (SIM) in a Full Positive Foreign Intelligence Investigation 9-10
9.10.1 (U) Sensitive Investigative Matters (SIM) 9-10
9.10.2 (U) Academic Nexus 9-11
9.11 (U) Retention of Information 9-11
9.12 (U//~~FOUO~~) Standards for Approving the Closing of a Full Positive Foreign Intelligence Investigation 9-11
9.12.1 (U) Standards 9-11
9.12.2 (U) Approval Requirements 9-12
9.12.2.1 (U) Opened by a Field Office with FBIHQ Approval 9-12
9.12.2.2 (U) Opened by FBIHQ 9-12
9.12.2.3 (U) SIM Opened by a Field Office with FBIHQ Approval 9-12
9.12.2.4 (U) SIM Opened by FBIHQ 9-12
9.13 (U) Other Program Specific Investigation Requirements 9-12
10 (U//~~FOUO~~) Sensitive Investigative Matter (SIM) and Sensitive Operations Review Committee (SORC) 10-1
10.1 (U) Sensitive Investigative Matters (SIM) 10-1
10.1.1 (U) Overview 10-1
10.1.2 (U) Purpose, Scope, and Definitions 10-1
10.1.2.1 (U) Definition of Sensitive Investigative Matters (SIM) 10-1

10.1.2.2 (U) Definitions/Descriptions of SIM Officials and Entities 10-1
10.1.2.2.1 (U) Domestic Public Official 10-1
10.1.2.2.2 (U) Domestic Political Candidate 10-2
10.1.2.2.3 (U) Domestic Political Organization or Individual Prominent in Such an Organization 10-2
10.1.2.2.4 (U) Religious Organization or Individual Prominent in Such an Organization 10-2
10.1.2.2.5 (U) Member of the News Media or a News Organization 10-2
10.1.2.2.6 (U) Academic Nexus 10-3
10.1.2.2.7 (U) Other Matters 10-4
10.1.3 (U) Factors to Consider When Opening or Approving an Investigative Activity Involving a SIM 10-4
10.1.4 (U) Opening Documentation, Approval, Notice, Change in SIM Status, and Sensitive Potential CHS or Sensitive Characteristic Designations in Type 5 Assessments 10-4
10.1.4.1 (U) Review and Approval of SIM Assessments By A Field Office 10-5
10.1.4.1.1 (U) Type 1 & 2 Assessments 10-5
10.1.4.1.2 (U) Type 3 and 4 Assessments 10-5
10.1.4.1.3 (U) Type 5 Assessments 10-5
10.1.4.1.4 (U) Type 6 Assessments 10-5
10.1.4.2 (U) Notice for SIM Assessments by a Field Office 10-5
10.1.4.3 (U) Review and Approval of SIM Predicated Investigations by a Field Office 10-6
10.1.4.3.1 (U) Preliminary and Full Investigations Involving a SIM 10-6
10.1.4.3.2 (U) Enterprise Investigations Involving a SIM 10-6
10.1.4.3.3 (U) Positive Foreign Intelligence Full Investigations Involving a SIM 10-6
10.1.4.4 (U) Notice for SIM Predicated Investigations Opened by a Field Office 10-6
10.1.4.4.1 (U) Notice for SIM Preliminary Investigations 10-6
10.1.4.4.2 (U) Notice for SIM Full Investigations 10-6
10.1.4.4.3 (U) Notice for SIM Enterprise Investigations 10-6
10.1.4.4.4 (U) Notice for SIM Positive Foreign Intelligence Full Investigations 10-6
10.1.4.5 (U) Review and Approval of SIM Assessments Opened by FBIHQ 10-7
10.1.4.5.1 (U) Type 1 & 2 Assessments 10-7
10.1.4.5.2 (U) Type 3 and 4 Assessments 10-7
10.1.4.5.3 (U) Type 5 Assessments 10-7
10.1.4.5.4 (U) Type 6 Assessments 10-7
10.1.4.6 (U) Notice Requirements for SIM Assessments by FBIHQ 10-7
10.1.4.7 (U) Review and Approval of SIM Predicated Investigations by FBIHQ 10-7
10.1.4.7.1 (U) Preliminary and Full Investigations Involving a SIM 10-7
10.1.4.7.2 (U) Enterprise Investigations Involving a SIM 10-8
10.1.4.7.3 (U) Positive Foreign Intelligence Full Investigations Involving a SIM 10-8
10.1.4.8 (U) Notice for SIM Predicated Investigations Opened by FBIHQ 10-8

10.1.4.8.1 (U) Notice for SIM Preliminary Investigations 10-8
10.1.4.8.2 (U) Notice for SIM Full Investigations 10-8
10.1.4.8.3 (U) Notice for SIM Enterprise Investigations 10-8
10.1.4.8.4 (U) Notice for SIM Full Positive Foreign Intelligence Investigations 10-8
10.1.4.9 (U) Additional Requirements for Presidential and Congressional Candidates and Campaigns 10-8
10.1.4.9.1 (U) Assessments 10-8
10.1.4.9.2 (U) Predicated Investigations 10-9
10.1.4.10 (U) Change in SIM Status 10-10
10.1.4.10.1 (U) Documentation 10-10
10.1.4.11 (U) Closing SIM Investigations 10-12
10.1.4.11.1 (U) SIM Assessments Closed by a Field Office 10-12
10.1.4.11.2 (U) SIM Predicated Investigations Closed by a Field Office 10-12
10.1.4.11.3 (U) SIM Assessments Closed by FBIHQ 10-12
10.1.4.11.4 (U) SIM Predicated Investigations Closed by FBIHQ 10-12
10.1.5 (U) Distinction Between SIM and Sensitive Circumstance in Undercover Operations 10-12
10.1.6 (U) Distinction Between SIM and Sensitive Undisclosed Participation 10-13
10.1.6.1 (U) Scenarios 10-13
10.2 (U//~~FOUO~~) Sensitive Operations Review Committee 10-14
10.2.1 (U) Membership and Staffing 10-14
10.2.2 (U) Function 10-14
10.2.3 (U) Review and Recommendation 10-14
10.2.3.1 (U) Factors to Consider for Review and Recommendation 10-15
10.2.3.2 (U) Process for Review and Recommendation 10-16
10.2.4 (U) Emergency Authorization 10-17
10.2.4.1 (U) Notice/Oversight Function of SORC 10-17
10.2.5 (U) Logistics 10-18
11 (U) Liaison Activities and Tripwires 11-1
11.1 (U) Overview 11-1
11.2 (U) Purpose and Scope 11-1
11.3 (U) Approval Requirements for Liaison and Tripwires 11-1
11.3.1 (U) Scenario 1 11-1
11.3.2 (U) Scenario 2 11-1
11.4 (U) Documentation & Records Retention Requirements 11-2

12 (U) Assistance to Other Agencies 12-1

12.1 (U) Overview 12-1

12.2 (U) Purpose and Scope 12-1

12.2.1 (U) Investigative Assistance 12-1

12.2.2 (U) Technical Assistance 12-2

12.3 (U) Investigative Assistance to Other Agencies - Standards, Approvals and Notice Requirements 12-2

12.3.1 (U) Standards for Providing Investigative Assistance to Other Agencies 12-3

12.3.2 (U) Authority, Approval and Notice Requirements for Providing Investigative Assistance to Other Agencies 12-3

12.3.2.1 (U) Investigative Assistance to United States Intelligence Community (USIC) Agencies 12-3

12.3.2.1.1 (U) Authority 12-3

12.3.2.1.2 (U) Approval Requirements 12-3

12.3.2.1.3 (U) Notice Requirements 12-3

12.3.2.1.4 (U) Documentation Requirements 12-4

12.3.2.2 (U) Investigative Assistance to Other United States Federal Agencies 12-4

12.3.2.2.1 (U) Authority 12-4

12.3.2.2.2 (U) Approval Requirements 12-6

12.3.2.2.3 (U) Notice Requirements 12-6

12.3.2.2.4 (U)Documentation Requirements 12-6

12.3.2.3 (U) Investigative Assistance to State, Local, and Tribal Agencies 12-7

12.3.2.3.1 (U) Approval Requirements 12-12

12.3.2.3.2 (U) Notice Requirements 12-13

12.3.2.3.3 (U) Documentation Requirements 12-13

12.3.2.3.4 (U) Examples of Expert Assistance in Investigations of Non-Federal Crimes. 12-14

12.3.2.4 (U) Investigative Assistance to Foreign Agencies 12-15

12.3.2.4.1 (U) Authorities 12-16

12.3.2.4.2 (U) Approval Requirements 12-16

12.3.2.4.3 (U) Notice Requirements 12-17

12.3.2.4.4 (U) Documentation Requirements 12-17

12.3.2.4.5 (U) Examples 12-17

12.4 (U) Technical Assistance to Other Agencies – Standards, Authority and Approval Requirements 12-18

12.4.1 (U) Authority 12-18

12.4.2 (U) Approval Requirements 12-19

12.4.2.1 (U) Technical Assistance to USIC Agencies 12-19

12.4.2.2 (U) Technical Assistance to Federal, State, Local and Tribal (Domestic) Agencies Regarding Electronic Surveillance, Equipment, and Facilities 12-19
12.4.2.3 (U) Technical Assistance to Federal, State, Local and Tribal (Domestic) Agencies Involving Equipment or Technologies Other than Electronic Surveillance Equipment 12-20
12.4.2.4 (U) Technical Assistance to Foreign Agencies 12-20
12.4.2.4.1 (U) Authorities 12-20
12.4.2.4.2 (U) Approval Requirements 12-21
12.4.2.4.3 (U) Notice Requirements 12-21
12.4.2.4.4 (U) Documentation Requirements 12-21
12.5 (U) Documentation Requirements for Investigative Assistance to Other Agencies 12-21
12.5.1 (U) Documentation Requirements in General 12-21
12.5.2 (U) Documentation Requirements for Investigative Assistance (Including Expert Assistance) to Other Agencies (Domestic or Foreign) 12-22
12.5.3 (U) Documentation Requirements for Technical Assistance to Other Agencies (Domestic or Foreign) 12-22
12.6 (U) Dissemination of Information to Other Agencies – Documentation Requirements 12-22
12.7 (U) Records Retention Requirements 12-23
12.7.1 (U) Serializing the FD-999 for Dissemination of Information 12-23
12.7.2 (U) Serializing the FD-999 for Investigative Assistance 12-24
12.7.3 (U) Request for FD-999 Exemption 12-24
12.7.4 (U//~~FOUO~~) 343 File Classification - Domestic Police Cooperation Files 12-25
12.7.5 (U//~~FOUO~~) 163 File Classification – Foreign Police Cooperation Files 12-25
13 (U) Extraterritorial Provisions 13-1
14 (U) Retention and Sharing of Information 14-1
14.1 (U) Purpose and Scope 14-1
14.2 (U) The FBI's Records Retention Plan 14-1
14.2.1 (U) Database or Records System 14-1
14.2.2 (U) Information Management Division Disposition Plan and Retention Schedules 14-2
14.3 (U) Information Sharing 14-2
14.3.1 (U) Permissive Sharing 14-2
14.3.2 (U) Required Sharing 14-3
14.3.3 (U) Information Sharing Pursuant to Executive Order (EO) 12333 14-3

14.4 (U) Information Related to Criminal Matters 14-4
14.4.1 (U) Coordinating with Prosecutors 14-4
14.4.2 (U) Criminal Matters Outside FBI Jurisdiction 14-5
14.4.3 (U) Reporting Criminal Activity of an FBI Employee or CHS 14-5
14.4.4 (U) The White House 14-5
14.4.5 (U) Congress 14-6
14.5 (U) Information Related to National Security and Foreign Intelligence Matters 14-6
14.5.1 (U) Department of Justice 14-7
14.5.2 (U) The White House 14-7
14.5.2.1 (U) Requests Sent Through NSC or HSC 14-8
14.5.2.2 (U) Approval by the Attorney General 14-8
14.5.2.3 (U) Information Suitable for Dissemination 14-8
14.5.2.4 (U) Notification of Communications 14-9
14.5.2.5 (U) Dissemination of Information Relating to Background Investigations 14-9
14.5.3 (U) Congress 14-9
14.6 (U) Special Statutory Requirements 14-9
14.7 (U) Threat To Life – Dissemination Of Information 14-10
14.7.1 (U) Overview 14-10
14.7.2 (U//~~FOUO~~) Information Received through FISA Surveillance 14-11
14.7.3 (U) Dissemination of Information Concerning Threats against Intended Victims (Persons) 14-11
14.7.3.1 (U) Warning to the Intended Victim (Person) 14-11
14.7.3.1.1 (U) Expeditious Warnings to Identifiable Intended Victims 14-11
14.7.3.1.2 (U) Warnings When Intended Victim is in Custody or is a Protectee 14-12
14.7.3.2 (U) Notification to Law Enforcement Agencies That Have Investigative Jurisdiction 14-12
14.7.3.2.1 (U) Expeditious Notification 14-12
14.7.3.2.2 (U) Exceptions to Notification 14-13
14.7.3.2.3 Means, Manner, and Documentation of Notification 14-13
14.7.4 (U//~~FOUO~~) Dissemination of Information Concerning Threats, Possible Violence or Demonstrations Against Foreign Establishments or Officials in the United States 14-13
14.7.5 (U) Dissemination of Information Concerning Threats Against the President and Other Designated Officials 14-14
14.8 (U) Suspected Child Abuse – Dissemination Of Information 14-14

14.9 (U) Suspected Abuse of the Elderly or Otherwise Vulnerable Individuals–Dissemination Of Information 14-14

14.10 (U//~~FOUO~~) Required Sharing with the White House Situation Room Regarding Critical Incident Information (Presidential Critical Information Requirements) 14-14

14.10.1 (U) Reportable Events 14-14

14.10.1.1 (U//~~FOUO~~) Tier One Events 14-14

14.10.1.2 (U//~~FOUO~~) Tier Two Events 14-18

14.10.2 (U) Reporting Procedures 14-18

14.10.2.1 (U) Standard Reporting Procedures for All FBI Employees 14-18

14.10.2.2 (U) Specific Reporting Procedures for Field Offices 14-19

14.10.2.3 (U) Specific Reporting Procedures for FBI Headquarters 14-20

14.10.3 (U//~~FOUO~~) Dissemination Procedures for the Strategic Information and Operations Center 14-21

14.10.4 (U) Requests for Modifications to Notification Requirements 14-22

15 (U) Intelligence Analysis and Planning 15-1

15.1 (U) Overview 15-1

15.2 (U) Purpose and Scope 15-1

15.2.1 (U) Functions Authorized 15-1

15.2.2 (U) Integration of Intelligence Activities 15-1

15.2.3 (U) Analysis and Planning Not Requiring the Opening of an Assessment (See DIOG Section 5) 15-2

15.3 (U) Civil Liberties and Privacy 15-2

15.4 (U) Legal Authority 15-2

15.5 (U) Intelligence Analysis and Planning – Requiring a Type 4 Assessment 15-3

15.6 (U) Authorized Activities in Intelligence Analysis and Planning 15-3

15.6.1 (U) Intelligence Analysis 15-3

15.6.1.1 (U) Analytic Intelligence Products 15-3

15.6.1.2 (U) United States Person (USPER) Information 15-4

15.6.1.3 (U) Intelligence Systems 15-4

16 (U) Undisclosed Participation (UDP) 16-1

16.1 (U) Overview 16-1

16.1.1 (U) Authorities 16-1
16.1.2 (U) Mitigation of Risk 16-1
16.1.3 (U) Sensitive UDP Defined 16-2
16.1.4 (U) Non-Sensitive UDP Defined 16-2
16.1.5 (U)Type of Activity 16-2
16.2 (U) Purpose, Scope, and Definitions 16-2
16.2.1 (U) Organization 16-2
16.2.2 (U) Legitimate Organization 16-2
16.2.3 (U) Participation 16-3
16.2.3.1 (U) Undisclosed Participation 16-4
16.2.3.2 (U//~~FOUO~~) Influencing the Activities of the Organization 16-4
16.2.3.3 (U//~~FOUO~~) Influencing the Exercise of First Amendment Rights 16-4
16.2.3.4 (U) Appropriate Official 16-4
16.2.3.5 (U) Sensitive Undisclosed Participation 16-4
16.2.3.6 (U) Already a Member of the Organization or a Participant in its Activities 16-5
16.3 (U) Requirements for Approval 16-5
16.3.1 (U) General Requirements 16-5
16.3.1.1 (U) Undercover Activity 16-5
16.3.1.2 (U) Concurrent Approval 16-6
16.3.1.3 (U) Delegation and "Acting" Status 16-6
16.3.1.4 (U) Specific Requirements for General Undisclosed Participation (Non-Sensitive UDP) 16-6
16.3.1.4.1 (U//~~FOUO~~) [redacted] 16-6
16.3.1.4.2 (U//~~FOUO~~) [redacted] 16-7
16.3.1.5 (U) Specific Requirements for Sensitive Undisclosed Participation (Sensitive UDP) 16-7
16.3.1.5.1 (U//~~FOUO~~) [redacted] 16-7
16.3.1.5.2 (U//~~FOUO~~) [redacted] 16-8
16.3.1.5.3 (U//~~FOUO~~) [redacted] 16-8
16.4 (U) Supervisory Approval Not Required 16-8
16.5 (U) Standards for Review and Approval 16-9
16.6 (U) Requests for Approval of Undisclosed Participation 16-10

b7E

16.7 (U) Duration 16-11
16.8 (U//~~FOUO~~) Sensitive Operations Review Committee (SORC) 16-11
16.8.1 (U//~~FOUO~~) SORC Notification 16-11
16.8.2 (U//~~FOUO~~) SORC Review 16-11
16.9 (U) FBIHQ Approval Process of UDP Requests 16-11
16.9.1 (U) Submitting the UDP request to FBIHQ 16-11
16.9.2 (U//~~FOUO~~) [redacted] 16-12 b7E
16.9.3 (U//~~FOUO~~) [redacted] 16-12
16.9.4 (U//~~FOUO~~) Procedures for Approving Emergency UDP Requests that Otherwise Require FBIHQ Approval 16-14
16.10 (U) UDP Examples 16-14
17 (U) Otherwise Illegal Activity (OIA) 17-1
17.1 (U) Overview 17-1
17.2 (U) Purpose and Scope 17-1
17.3 (U//~~FOUO~~) Application 17-1
17.4 (U) Legal Authority 17-1
17.5 (U//~~FOUO~~) Standards and Approval Requirements for OIA 17-1
17.5.1 (U) General Approval Requirements 17-1
17.5.2 (U) OIA in an Undercover Activity 17-2
17.5.3 (U//~~FOUO~~) Field Office Review and Approval of OIA for an FBI Agent or Employee 17-2
17.5.3.1 *(U//~~FOUO~~) Written Operations Orders for Controlled Firearms Transactions* 17-3
17.5.4 (U//~~FOUO~~) OIA by a Confidential Human Source (CHS) Approval 17-5
17.5.5 (U//~~FOUO~~) OIA Related to [redacted] Investigations 17-5 b7E
17.5.5.1 (U//~~FOUO~~) Procedures on Requests and Approval for OIA Related to [redacted] 17-6
17.6 (U//~~FOUO~~) Documentation of Requests to Engage in OIA by an FBI Agent or Employee 17-6
17.7 (U//~~FOUO~~) Standards for Review and Approval of OIA 17-6
17.8 (U) OIA Not Authorized 17-7
17.9 Approval and Documentation of Emergency OIA 17-7

17.10 Other Governmental Approvals 17-7

18 (U) Investigative Methods 18-1

18.1 (U) Overview 18-1

18.1.1 (U) Investigative Methods Listed by Sub-Section Number 18-1

18.1.2 (U) Investigative Methods Listed by Name (Alphabetized) 18-2

18.1.3 (U) General Overview 18-3

18.1.4 (U) Conducting Investigative Activity in Another Field Office's AOR 18-3

18.2 (U) Least Intrusive Method 18-3

18.3 (U) Particular Investigative Methods 18-4

18.3.1 (U) Use of Criminal Investigative Methods in National Security Investigations 18-4

18.4 (U) Information or Evidence Obtained in Assessments and Predicated Investigations 18-4

18.5 (U) Authorized Investigative Methods in Assessments 18-5

18.5.1 (U) Investigative Method: Public Information ("Publicly Available Information") 18-7

18.5.1.1 (U) Scope 18-7

18.5.1.2 (U) Application 18-8

18.5.1.3 (U) Approval 18-8

18.5.1.3.1 (U//~~FOUO~~) Special Rules: "Special Rule for Religious Services" and "Special Rule for Other Sensitive Organizations" 18-8

18.5.1.4 (U) Use/Dissemination 18-8

18.5.2 (U) Investigative Method: Records or Information – FBI and Department of Justice (DOJ) 18-9

18.5.2.1 (U) Scope 18-9

18.5.2.1.1 (U//~~FOUO~~) Facial Recognition Technology 18-9

18.5.2.2 (U) Application 18-9

18.5.2.3 (U) Approval 18-9

18.5.2.4 (U) Pattern-Based Data Mining (PBDM) 18-10

18.5.2.5 (U) Use, Dissemination, and Recordkeeping 18-10

18.5.3 (U) Investigative Method: Records or Information – Other Federal, State, Local, Tribal, or Foreign Government Agency 18-11

18.5.3.1 (U) Scope 18-11

18.5.3.1.1 (U//~~FOUO~~) Facial Recognition Technology 18-11

18.5.3.2 (U) Application 18-11

18.5.3.3 (U) Approval and Coordination 18-11

18.5.3.3.1 (U) Requests to other Federal Agencies 18-12

18.5.3.3.2 (U) Requests to Foreign Agencies 18-12
18.5.3.4 (U) Use, Dissemination, and Recordkeeping 18-12
18.5.4 (U) Investigative Method: Online Services and Resources 18-13
18.5.4.1 (U) Scope 18-13
18.5.4.1.1 (U//~~FOUO~~) Facial Recognition Technology 18-13
18.5.4.2 (U) Application 18-13
18.5.4.3 (U) Approval 18-13
18.5.4.4 (U) Use, Dissemination, and Recordkeeping 18-14
18.5.5 (U) Investigative Method: CHS Use and Recruitment 18-16
18.5.5.1 (U) Scope 18-16
18.5.5.2 (U) Application 18-16
18.5.5.3 (U) Approvals 18-16
18.5.5.4 (U//~~FOUO~~) Applicability of the Misplaced Confidence Doctrine During CHS Online Activity 18-18
18.5.5.5 (U) Use/Dissemination 18-19
18.5.6 (U) Investigative Method: Interview or Request Information from the Public or Private Entities 18-20
18.5.6.1 (U) Scope 18-20
18.5.6.2 (U) Application 18-21
18.5.6.3 (U) Voluntariness 18-21
18.5.6.4 (U) Approval/Procedures 18-22
18.5.6.4.1 (U) Domestic Custodial Interviews 18-22
18.5.6.4.2 (U//~~FOUO~~) Miranda Warnings for Suspects in Custody Overseas 18-26
18.5.6.4.3 (U) Constitutional Rights to Silence and Counsel Under Miranda 18-26
18.5.6.4.4 (U) Sixth Amendment Right to Counsel 18-27
18.5.6.4.5 (U) Contact with Represented Persons 18-27
18.5.6.4.6 (U) Members of the United States Congress and Their Staffs 18-27
18.5.6.4.7 (U) White House Personnel 18-28
18.5.6.4.8 (U) Members of the News Media 18-28
18.5.6.4.9 (U) During an Assessment - Requesting Information without Revealing FBI Affiliation or the True Purpose of a Request 18-30
18.5.6.4.10 (U) Consultation and Discussion 18-31
18.5.6.4.11 (U) Examples 18-31
18.5.6.4.12 (U//~~FOUO~~) Predicated Investigations - Requesting Information without Revealing FBI Affiliation or the True Purpose of a Request 18-34
18.5.6.4.13 (U) Interviews of Particularly Vulnerable Victims 18-34
18.5.6.4.14 (U) Interviews of Juvenile Subjects 18-35
18.5.6.4.15 (U) Documentation 18-37
18.5.6.4.16 (U) Use of the FD-302 18-38

18.5.6.4.17 (U) Electronic Recording of Interviews 18-40
18.5.6.4.18 (U) Interviews Relating to Closed Files 18-49
18.5.6.4.19 (U) FBIHQ Operational Division Requirements 18-49
18.5.6.5 (U) Use/Dissemination 18-50
18.5.6.6 (U//~~FOUO~~) Overseas Interviews 18-50
18.5.7 (U) Investigative Method: Information Voluntarily Provided by Governmental or Private Entities 18-51
18.5.7.1 (U) Scope 18-51
18.5.7.2 (U) Application 18-51
18.5.7.3 (U) Approval 18-51
18.5.7.4 (U) Use/Dissemination 18-51
18.5.8 (U) Investigative Method: Physical Surveillance (Not Requiring a Court Order) 18-53
18.5.8.1 (U) Scope 18-53
18.5.8.2 (U) Application 18-54
18.5.8.3 (U) Approval 18-54
18.5.8.3.1 (U//~~FOUO~~) Standards for Opening or Approving Physical Surveillance During an Assessment 18-54
18.5.8.3.2 (U//~~FOUO~~) [redacted] for Assessments 18-54 b7E
18.5.8.3.3 (U//~~FOUO~~) [redacted] 18-55
18.5.8.3.4 (U) [redacted] 18-55
18.5.8.4 (U) Other Physical Surveillance 18-57
18.5.8.5 (U) Maintain a "Surveillance Log" During Physical Surveillance 18-57
18.5.8.6 (U) Use/Dissemination 18-57
18.5.9 (U) Investigative Method: Grand Jury Subpoenas – To Providers of Electronic Communication Services or Remote Computing Services for Subscriber or Customer Information (Only in Type 1 & 2 Assessments) 18-59
18.5.9.1 (U) Scope 18-59
18.5.9.2 (U) Application 18-59
18.5.9.3 (U) Approval 18-59
18.5.9.3.1 (U) Members of the News Media 18-59
18.5.9.4 (U) Grand Jury Subpoenas to Providers of Electronic Communication Services or Remote Computing Services for Subscriber or Customer Information (ECPA 18 U.S.C. § 2703) 18-60
18.5.9.5 (U) Restrictions on Use and Dissemination 18-60
18.6 (U) Authorized Investigative Methods in Preliminary Investigations . 18-63

18.6.1 (U) Investigative Method: Consensual Monitoring of Communications, Including Electronic Communications 18-65
18.6.1.1 (U) Summary 18-65
18.6.1.2 (U) Application 18-65
18.6.1.3 (U) Legal Authority 18-65
18.6.1.4 (U) Definition of Investigative Method 18-65
18.6.1.5 (U) Standards and Approval/Review Requirements for Consensual Monitoring 18-66
18.6.1.5.1 (U) General Approval and Legal Review Requirements 18-66
18.6.1.6 (U) Consensual Monitoring Situations Requiring Additional Notice or Approval 18-70
18.6.1.6.1 (U) Party Located Outside the United States 18-70
18.6.1.6.2 (U) Sensitive Monitoring Circumstance 18-71
18.6.1.7 (U) Documenting the Use of Consensual Monitoring with an FD-302 18-73
18.6.1.8 (U) Compliance and Monitoring 18-73
18.6.1.9 (U) Evidence Handling 18-73
18.6.2 (U) Investigative Method: Intercepting the Communications of a Computer Trespasser 18-75
18.6.2.1 (U) Summary 18-75
18.6.2.2 (U) Application 18-75
18.6.2.3 (U) Legal Authority 18-75
18.6.2.4 (U) Definition of the Communications of a Computer Trespasser 18-75
18.6.2.5 (U//~~FOUO~~) Use and Approval Requirements for Intercepting the Communications of a Computer Trespasser 18-77
18.6.2.5.1 (U) General Approval Requirements 18-77
18.6.2.6 (U) Duration of Approval for Intercepting the Communications of a Computer Trespasser 18-78
18.6.2.7 (U) Specific Procedures for Intercepting the Communications of a Computer Trespasser 18-78
18.6.2.7.1 (U) Documenting Authorization to Intercept 18-79
18.6.2.7.2 (U) Acquiring Only the Trespasser Communications 18-79
18.6.2.7.3 (U) Reviewing the Accuracy of the Interception 18-80
18.6.2.7.4 (U) Reviewing the Relevancy of the Interception 18-80
18.6.2.7.5 (U) Duration of Approval 18-81
18.6.2.7.6 (U) ELSUR Requirements 18-81
18.6.2.7.7 (U) Multiple Communications. 18-81
18.6.2.7.8 (U) Investigation Specific Approval 18-81
18.6.2.8 (U) Compliance and Monitoring 18-81
18.6.2.9 (U) Evidence Handling 18-81

18.6.3 (U//~~FOUO~~) Investigative Method: [redacted] Closed-Circuit Television/Video Surveillance, Direction Finders, and Other Monitoring Devices ... 18-83 b7E
18.6.3.1 (U) Summary ... 18-83
18.6.3.2 (U) Application ... 18-83
18.6.3.3 (U) Legal Authority ... 18-83
18.6.3.4 (U) Definition of Investigative Method ... 18-83
18.6.3.5 (U//~~FOUO~~) Standards for Use and Approval Requirements for Investigative Method ... 18-84
18.6.3.6 (U) Duration of Approval ... 18-84
18.6.3.7 (U) Specific Procedures ... 18-84
18.6.3.8 (U) CCTV/Video Surveillance Where There is a Reasonable Expectation of Privacy in the Area to be Viewed or for the Installation of the Equipment ... 18-85
18.6.3.8.1 (U) Warrant or Court Order ... 18-85
18.6.3.8.2 (U//~~FOUO~~) Required Consultation with Technical Advisor (TA) or Technically Trained Agent (TTA) ... 18-85
18.6.3.9 (U) Evidence Handling ... 18-86
18.6.3.10 (U) [redacted] ... 18-86 b7E
18.6.3.11 (U) CCTV/Video Surveillance Equipment – Types, Availability, Repair and Disposal ... 18-86
18.6.3.11.1 (U) Equipment Types ... 18-86
18.6.3.11.2 (U) Equipment Availability ... 18-87
18.6.3.11.3 (U) Equipment Repair ... 18-87
18.6.3.11.4 (U) Equipment Disposal ... 18-87
18.6.3.12 (U) Compliance and Monitoring ... 18-87
18.6.4 (U) Investigative Method: Administrative Subpoenas (Compulsory Process) ... 18-89
18.6.4.1 (U) Overview of Compulsory Process ... 18-89
18.6.4.2 (U) Application ... 18-89
18.6.4.3 (U) Administrative Subpoenas ... 18-89
18.6.4.3.1 (U) Summary ... 18-89
18.6.4.3.2 (U) Legal Authority and Delegation ... 18-90
18.6.4.3.3 (U) Approval Requirements ... 18-92
18.6.4.3.4 (U) Limitations on Use of Administrative Subpoenas ... 18-93
18.6.4.3.5 (U) Compliance/Monitoring ... 18-96
18.6.5 (U) Investigative Method: Grand Jury Subpoenas (Compulsory Process) ... 18-99
18.6.5.1 (U) Overview of Compulsory Process ... 18-99
18.6.5.2 (U) Application ... 18-99
18.6.5.3 (U) Legal Authorities ... 18-99
18.6.5.4 (U) Scope ... 18-100

18.6.5.4.1 (U) Scope of FGJ Policy on Administrative Personnel 18-100
18.6.5.5 (U) Approval Requirements 18-101
18.6.5.6 (U) Duration of Approval 18-101
18.6.5.7 (U) Members of the News Media 18-101
18.6.5.8 (U) Notice and Reporting Requirements 18-102
18.6.5.9 (U) Definition of Matters Occurring Before the Grand Jury 18-102
18.6.5.9.1 (U) Examples of Matters Occurring Before the Grand Jury 18-102
18.6.5.9.2 (U) Federal Grand Jury Physical Evidence and Statements of Witnesses 18-102
18.6.5.9.3 (U) Documents Created Independent of Grand Jury but Obtained by Grand Jury Subpoena 18-103
18.6.5.9.4 (U//~~FOUO~~) Data Extracted from Records Obtained by Grand Jury Subpoena 18-103
18.6.5.10 (U) Restrictions on Disclosure 18-103
18.6.5.11 (U) Disclosures by the Government Requiring the Court's Permission 18-104
18.6.5.11.1 (U) Disclosures by the Government Not Requiring the Court's Permission 18-104
18.6.5.11.2 (U) Rule 6(e) Exceptions Permitting Disclosure of FGJ Material 18-105
18.6.5.11.3 (U) Rule 6(e)(3)(d) Disclosure Exception for Intelligence or National Security Purposes 18-105
18.6.5.11.4 (U) FBI's Conduit Rule 18-106
18.6.5.11.5 (U) Other Statutory Disclosure Restrictions Not Affected 18-106
18.6.5.11.6 (U) Rule 6(e)(3)(d) Receiving Official Rules and Restrictions 18-106
18.6.5.11.7 (U) Violations 18-108
18.6.5.12 (U) Limitation of Use 18-108
18.6.5.13 (U//~~FOUO~~) Marking, Physical Storage, and Mailing of Grand Jury Material 18-109
18.6.5.13.1 (U//~~FOUO~~) Physical Storage of FGJ Material 18-110
18.6.5.13.2 (U//~~FOUO~~) Electronic Storage of FGJ Material 18-112
18.6.5.13.3 (U//~~FOUO~~) Handling and Storage of FGJ Material after the Closure of a Case 18-112
18.6.5.13.4 (U//~~FOUO~~) Deletion of Electronically Stored Material Identified as Matters Occurring Before the Grand Jury 18-113
18.6.5.13.5 (U//~~FOUO~~) FGJ Material Containing Classified or Other Sensitive Information 18-113
18.6.5.14 (U) Requests for FGJ Subpoenas in Fugitive Investigations 18-113
18.6.5.15 (U) FGJ Overproduction 18-114
18.6.5.16 (U) FGJ Material Compliance and Monitoring 18-114
18.6.6 (U) Investigative Method: National Security Letter (Compulsory Process) 18-117
18.6.6.1 (U) Overview of Compulsory Process 18-117
18.6.6.2 (U) Application 18-117
18.6.6.3 (U) National Security Letters 18-117
18.6.6.3.1 (U) Legal Authority 18-117

18.6.6.3.2 (U) Definition of Method 18-118
18.6.6.3.3 (U) Review and Approval Requirements 18-118
18.6.6.3.4 (U) Standards for Issuing NSLs 18-119
18.6.6.3.5 (U) Special Procedures for Requesting Communication Subscriber Information 18-120
18.6.6.3.6 (U) Duration of Approval 18-120
18.6.6.3.7 (U) Specific Procedures for Creating NSLs 18-120
18.6.6.3.8 (U) Notice and Reporting Requirements 18-125
18.6.6.3.9 (U) Receipt of NSL Information, Review for Overproduction, and Releasing the Information 18-125
18.6.6.3.10 (U) Overproduction 18-126
18.6.6.3.11 (U) Retention of NSL Information 18-127
18.6.6.3.12 (U) Service and Returns of NSLs 18-128
18.6.6.3.13 (U) Dissemination of NSL Information 18-130
18.6.6.3.14 (U) Special Procedures for Handling Right to Financial Privacy Act Information and Other Information 18-130
18.6.6.3.15 (U) Payment for NSL-Derived Information 18-131
18.6.6.3.16 (U) Judicial Review of NSLs 18-132
18.6.6.3.17 (U) Review of Nondisclosure Requirement in NSLs 18-132
18.6.7 (U) Investigative Method: FISA Order for Business Records (Compulsory Process) 18-135
18.6.7.1 (U) Overview of Compulsory Process 18-135
18.6.7.2 (U) Application 18-135
18.6.7.3 (U) Business Records Under FISA 18-135
18.6.7.3.1 (U) Legal Authority 18-135
18.6.7.3.2 (U) Definition of Method 18-135
18.6.7.3.3 (U) Approval Requirements 18-136
18.6.7.3.4 (U) Duration of Court Approval 18-136
18.6.7.3.5 (U) Notice and Reporting Requirements 18-136
18.6.7.3.6 (U) Compliance Requirements 18-136
18.6.7.3.7 (U) FISA Overcollection and Standard Minimization Procedures 18-137
18.6.8 (U) Investigative Method: Stored Wire or Electronic Communications and Transactional Records 18-139
18.6.8.1 (U) Summary 18-139
18.6.8.2 (U) Application 18-139
18.6.8.2.1 (U) Stored Data 18-139
18.6.8.2.2 (U) Legal Process 18-140
18.6.8.2.3 (U) Retrieval 18-140
18.6.8.2.4 (U) Basic Subscriber Information 18-140
18.6.8.2.5 (U) Preservation of Stored Data 18-140

18.6.8.2.6 (U) Cost Reimbursement 18-140
18.6.8.3 (U) Legal Authority 18-141
18.6.8.4 (U) ECPA Disclosures 18-141
18.6.8.4.1 (U) Definitions 18-141
18.6.8.4.2 (U) Compelled Disclosure 18-142
18.6.8.4.3 (U) Voluntary Disclosure 18-148
18.6.8.5 (U) Voluntary Emergency Disclosure 18-151
18.6.8.5.1 (U) Summary 18-151
18.6.8.5.2 (U) Application 18-152
18.6.8.5.3 (U) Duration of Approval 18-152
18.6.8.5.4 (U) Specific Procedures 18-152
18.6.8.5.5 (U) Cost Reimbursement 18-153
18.6.8.5.6 (U) Congressional Reporting Requirements 18-153
18.6.9 (U) Investigative Method: Pen Registers and Trap/Trace Devices (PR/TT) 18-155
18.6.9.1 (U) Summary 18-155
18.6.9.2 (U) Application 18-155
18.6.9.3 (U) Legal Authority 18-155
18.6.9.4 (U) Definition of Investigative Method 18-155
18.6.9.5 (U) Standards for Use and Approval Requirements for Investigative Method .. 18-155
18.6.9.5.1 (U) Pen Register/Trap and Trace Under FISA 18-155
18.6.9.5.2 (U) Criminal Pen Register/Trap and Trace Under Title 18 18-158
18.6.9.6 (U) Duration of Approval 18-160
18.6.9.7 (U) Specific Procedures 18-160
18.6.9.8 (U) Use of FISA Derived Information in Other Proceedings 18-161
18.6.9.9 (U) Congressional Notice and Reporting Requirements 18-161
18.6.9.9.1 (U) Criminal Pen Register/Trap and Trace- Annual Report 18-161
18.6.9.9.2 (U) National Security Pen Registers and Trap and Trace – Semi-Annual Report 18-162
18.6.9.10 (U) Post Cut-Through Dialed Digits (PCTDD) 18-162
18.6.9.10.1 (U) Overview 18-162
18.6.9.10.2 (U) Collection of PCTDD 18-163
18.6.9.10.3 (U) Use of PCTDD 18-163
18.6.9.10.4 (U) What Constitutes PCTDD Content 18-164
18.6.9.11 (U//~~FOUO~~) [redacted] 18-165
18.6.9.11.1 (U//~~FOUO~~) To Locate a Known Phone Number 18-165
18.6.9.11.2 (U//~~FOUO~~) To Identify an Unknown Target Phone Number 18-166
18.6.9.11.3 (U) PR/TT Order Language 18-167
18.6.10 (U) Investigative Method: Mail Covers 18-169

b7E

18.6.10.1 (U) Summary 18-169
18.6.10.2 (U) Application 18-169
18.6.10.3 (U) Legal Authority 18-169
18.6.10.4 (U) Definition of Investigative Method 18-169
18.6.10.5 (U) Standard for Use and Approval Requirements for Investigative Method 18-170
18.6.10.6 (U) Duration of Approval 18-172
18.6.10.7 (U) Mail Cover Documentation 18-172
18.6.10.8 (U) Storage of Mail Cover Responsive Records–Special Procedures for Criminal Cases 18-173
18.6.10.9 (U) Compliance and Monitoring 18-173
18.6.11 (U) Investigative Method: Polygraph Examinations 18-175
18.6.11.1 (U) Summary 18-175
18.6.11.2 (U) Application 18-175
18.6.11.3 (U) Legal Authority 18-175
18.6.11.4 (U) Standards for Use and Approval Requirements for Investigative Method 18-175
18.6.11.5 (U) Duration of Approval 18-176
18.6.11.6 (U) Specific Procedures 18-176
18.6.11.7 (U) Compliance and Monitoring 18-176
18.6.12 (U) Investigative Method: Searches that Do Not Require a Warrant or Court Order (Trash Cover, Abandoned Property from a Public Receptacle, Administrative Inventory Search of a Lost/Misplaced Item) And Inventory Searches Generally 18-177
18.6.12.1 (U) Summary 18-177
18.6.12.2 (U) Application 18-177
18.6.12.3 (U) Legal Authority 18-177
18.6.12.4 (U) Definition of Investigative Method 18-178
18.6.12.4.1 (U) Distinction Between a Trash Cover, a Search of Abandoned Property in a Public Receptacle, and Administrative Inventory Search of a Lost or Misplaced Item 18-178
18.6.12.4.2 (U) Determination of an Area of Curtilage Around a Home 18-179
18.6.12.5 (U) Standards for Use and Approval Requirements for a Trash Cover 18-179
18.6.12.6 (U) Standards for Use and Approval Requirements Retrieval of Discarded or Abandoned Property, Administrative Searches of Lost or Misplaced Property, and Inventory Searches Generally 18-180
18.6.13 (U) Investigative Method: Undercover Operations 18-181
18.6.13.1 (U) Summary 18-181
18.6.13.2 (U) Legal Authority 18-181
18.6.13.3 (U) Definition of Investigative Method 18-181

18.6.13.3.1 (U) Distinction Between Sensitive Circumstance and Sensitive Investigative Matter 18-182
18.6.13.4 (U//~~FOUO~~) Standards for Use and Approval Requirements for Investigative Method 18-182
18.6.13.4.1 (U) Standards for Use of Investigative Method 18-182
18.6.13.4.2 (U//~~FOUO~~) Approval Requirements for UCOs (Investigations of Violations of Federal Criminal Law That Do Not Concern Threats to National Security or Foreign Intelligence) 18-183
18.6.13.4.3 (U//~~FOUO~~) Approval Requirements for UCOs (Investigations of Violations that Concern Threats to National Security or Foreign Intelligence) 18-184
18.6.13.5 (U) [redacted] of OIA in Undercover Operations 18-185 b7E
18.6.13.5.1 (U//~~FOUO~~) Written Operations Orders for Controlled Firearms Transactions.. 18-186
18.6.13.6 (U) Duration of Approval 18-187
18.6.13.7 (U) Additional Guidance 18-188
18.6.13.8 (U) Compliance and Monitoring, and Reporting Requirements 18-188
18.7 (U) Authorized Investigative Methods in Full Investigations 18-189
18.7.1 (U) Investigative Method: Searches – With a Warrant or Court Order (Reasonable Expectation of Privacy) 18-191
18.7.1.1 (U) Summary 18-191
18.7.1.2 (U) Legal Authority 18-191
18.7.1.3 (U) Definition of Investigative Method 18-192
18.7.1.3.1 (U) Requirement for Reasonableness 18-192
18.7.1.3.2 (U) Reasonable Expectation of Privacy 18-192
18.7.1.3.3 (U) Issuance of Search Warrant 18-192
18.7.1.3.4 (U) Property or Persons that May be Seized with a Warrant 18-193
18.7.1.4 (U) Approval Requirements for Investigative Method 18-197
18.7.1.5 (U) Duration of Approval 18-198
18.7.1.6 (U) Specific Procedures 18-198
18.7.1.6.1 (U) Obtaining a Warrant under FRCP Rule 41 18-198
18.7.1.6.2 (U) Obtaining a FISA Warrant 18-202
18.7.2 (U) Investigative Method: Electronic Surveillance – Title III 18-209
18.7.2.1 (U) Summary 18-209
18.7.2.2 (U) Legal Authority 18-209
18.7.2.3 (U) Definition of Investigative Method 18-209
18.7.2.4 (U) Title III Generally 18-209
18.7.2.5 (U) Standards for Use and Approval Requirements for Non-Sensitive Title IIIs 18-210
18.7.2.6 (U) Standards for Use and Approval Requirements for Sensitive Title IIIs 18-210

18.7.2.7 (U) Procedures For Emergency Title III Interceptions 18-211
18.7.2.7.1 (U) Obtaining Emergency Authorization 18-212
18.7.2.7.2 (U) Post-Emergency Authorization 18-213
18.7.2.8 (U) Pre-Title III Electronic Surveillance (ELSUR) Search Policy 18-214
18.7.2.9 (U) Duration of Approval for Title III 18-215
18.7.2.10 (U) Specific Procedures for Title III Affidavits 18-215
18.7.2.11 (U) Dispute Resolution for Title III Applications 18-216
18.7.2.12 (U) Title III – Documenting, Reporting, and Notice Requirements 18-216
18.7.2.12.1 (U//~~FOUO~~ [redacted] 18-216 b7E
18.7.2.12.2 (U//~~FOUO~~) Serializing Title III Documents 18-216
18.7.2.12.3 (U//~~FOUO~~) [redacted] 18-217
18.7.2.12.4 (U//~~FOUO~~) Title III Activity Reports 18-217
18.7.2.12.5 (U//~~FOUO~~) Notice to FBIHQ of the Authorization and the Termination of a Title III 18-217
18.7.2.12.6 (U//~~FOUO~~) Notice Requirement for Sensitive Investigative Matters (SIM) that Involve Title III Interceptions 18-217
18.7.2.12.7 (U//~~FOUO~~) Title III Inventory Notices 18-218
18.7.2.12.8 (U//~~FOUO~~) Title III Wiretap Report 18-218
18.7.2.13 (U) Joint Title III Operations with Other Law Enforcement Agencies 18-219
18.7.2.13.1 (U) Federal Law Enforcement Agencies 18-219
18.7.2.13.2 (U) State and Local Law Enforcement Agencies 18-220
18.7.2.14 (U) Evidence Handling 18-220
18.7.3 (U) Investigative Method: Electronic Surveillance – FISA and FISA Title VII (Acquisition of Foreign Intelligence Information) 18-221
18.7.3.1 (U) Summary 18-221
18.7.3.2 (U) Foreign Intelligence Surveillance Act (FISA) 18-221
18.7.3.2.1 (U) Legal Authority 18-221
18.7.3.2.2 (U) Definition of Investigative Method 18-222
18.7.3.2.3 (U) Standards for Use and Approval Requirements for FISA 18-222
18.7.3.2.4 (U) Duration of Approval for FISA 18-223
18.7.3.2.5 (U//~~FOUO~~) Specific Procedures for FISA 18-223
18.7.3.2.6 (U) Notice and Reporting Requirements for FISA 18-225
18.7.3.2.7 (U) Compliance and Monitoring for FISA 18-226
18.7.3.2.8 (U) Special Circumstances for FISA 18-226
18.7.3.2.9 (U) FISA Overcollection 18-226
18.7.3.2.10 (U) Other Applicable Policies 18-226
18.7.3.2.11 (U)Collection handling 18-226
18.7.3.3 (U) FISA Title VII (Acquisition of Foreign Intelligence Information) 18-228
18.7.3.3.1 (U) Summary 18-228

18.7.3.3.2 (U) Legal Authority 18-228
18.7.3.3.3 (U) Definition of Investigative Method 18-228
18.7.3.3.4 (U//~~FOUO~~) Standards for Use and Approval Requirements for Investigative Method 18-228
18.7.3.3.5 (U) Duration of Approval 18-229
18.7.3.3.6 (U//~~FOUO~~) Specific Collection Procedures for Title VII 18-229

19 (U) Arrest Procedure Policy 19-1

19.1 (U) Arrest Warrants 19-1
19.1.1 (U) Complaints 19-1
19.1.2 (U) Arrest Warrants 19-1
19.1.3 (U) Jurisdiction 19-1
19.1.4 (U) Person to be Arrested 19-1

19.2 (U) Arrest with Warrant 19-1
19.2.1 (U) Policy 19-1
19.2.2 (U) Prompt Execution 19-2
19.2.3 (U) Written Operations Orders for Planned Arrests 19-2
19.2.4 (U) Arrest Techniques – General 19-4
19.2.4.1 (U) Initial Approach during an Arrest Operation 19-4
19.2.4.2 (U) Possession and Display of Warrant 19-5
19.2.4.3 (U) Handcuffing 19-5
19.2.4.4 (U) Search of the Person Incident to Arrest 19-5
19.2.4.4.1 (U) High-Risk Search/Full-Body Search 19-5
19.2.4.4.2 (U) Final Search and Collection of Evidence 19-6
19.2.4.5 (U) Transportation of Arrested Persons 19-7
19.2.4.6 (U) Joint Arrests 19-7
19.2.4.7 (U) Eyewitness Identifications 19-8

19.3 (U) Arrest without Warrant 19-8
19.3.1 (U) Federal Crimes 19-8
19.3.2 (U) Notification to U.S. Attorney 19-8
19.3.3 (U) Non-Federal Crimes 19-8
19.3.4 (U) Adherence to FBI Policy 19-9

19.4 (U) Prompt Appearance before Magistrate 19-9
19.4.1 (U) Definition of Unnecessary Delay 19-9
19.4.2 (U) Effect of Unnecessary Delay 19-10
19.4.3 (U) Necessary Delay 19-10
19.4.4 (U) Initial Processing 19-11

19.4.4.1 (U) Requests of Subjects in Custody 19-11
19.4.5 (U) Collection of DNA after Arrest or Detention 19-11
19.5 (U) Use of Force 19-12
19.5.1 (U) Identification 19-12
19.5.2 (U) Physical Force 19-12
19.5.3 (U) Restraining Devices 19-12
19.5.4 (U) Pregnant Arrestees 19-12
19.6 (U) Manner of Entry 19-13
19.6.1 (U) Knock and Announce 19-13
19.6.2 (U) Suspect's Dwelling 19-13
19.6.3 (U) Third Party Dwelling 19-14
19.6.4 (U) Exigent Circumstances 19-14
19.7 (U) Search Incident to Arrest 19-14
19.7.1 (U) Prerequisite: Lawful Arrest 19-14
19.7.2 (U) Scope and Timing Requirement 19-15
19.7.2.1 (U) Scope of Search 19-15
19.7.2.2 (U) Vehicles 19-15
19.7.2.3 (U) Cell Phones 19-15
19.7.2.4 (U) Protective Sweep 19-16
19.7.2.5 (U) Timing 19-16
19.7.3 (U) Inventory of Personal Property 19-16
19.8 (U) Medical Attention for Arrestees 19-17
19.9 (U) Arrest of Foreign Nationals 19-18
19.9.1 (U) Requirements Pertaining to Foreign Nationals 19-18
19.9.2 (U) Steps to Follow When a Foreign National is Arrested or Detained 19-18
19.9.3 (U) Suggested Statements to Arrested or Detained Foreign Nationals 19-20
19.9.3.1 (U) Statement 1: When Consular Notification is at the Foreign National's Option .. 19-20
19.9.3.2 (U) Statement 2: When Consular Notification is Mandatory 19-20
19.9.4 (U) Diplomatic Immunity 19-20
19.9.4.1 (U) Territorial Immunity 19-20
19.9.4.2 (U) Personal Immunity 19-21
19.10 (U) Arrest of Members of the News Media 19-21
19.10.1 (U) Exigent Circumstances 19-21
19.11 (U) Arrest of Armed Forces Personnel 19-22

19.12 (U) Arrest of Juveniles 19-22
19.12.1 (U) Definition of Juvenile Delinquency 19-22
19.12.2 (U) Arrest Procedures 19-22
20 (U) Other Investigative Resources 20-1
20.1 (U) Overview 20-1
20.1.1 (U//~~FOUO~~) [redacted] 20-1 b7E
20.1.2 (U//~~FOUO~~) [redacted] 20-1
20.1.3 (U//~~FOUO~~) Behavioral Analysis – Operational Behavioral Support Program 20-1
20.1.4 (U//~~FOUO~~) Sensitive Technical Equipment 20-1
20.2 (U//~~FOUO~~) [redacted] 20-1
20.2.1 (U) Authorized Investigative Activity 20-1
20.3 (U//~~FOUO~~) [redacted] 20-1 b7E
20.3.1 (U) Authorized Investigative Activity 20-1
20.4 (U//~~FOUO~~) Operational Behavioral Support Program – CIRG's Behavioral Analysis Units (BAUs) and/or CD's Behavioral Analysis Program 20-2
20.4.1 (U) Authorized Investigative Activity 20-2
20.5 (U//~~FOUO~~) Sensitive Technical Equipment 20-2
20.5.1 (U) Authorized Investigative Activity 20-2
20.6 (U//~~FOUO~~) [redacted] 20-2
20.6.1 (U) Authorized Investigative Activity 20-3
21 (U) Intelligence Collection 21-1
21.1 (U) Incidental Collection 21-1
21.2 (U) FBI National Collection Requirements 21-1
21.3 (U//~~FOUO~~) FBI Field Office Collection Requirements 21-3
A Appendix A: (U) The Attorney General's Guidelines For Domestic FBI Operations 1
B Appendix B: (U) Executive Order 12333 1
C Appendix C: (U//~~FOUO~~) Use and Targeting of a Federal Prisoner Held in the Custody of the BOP or USMS During an FBI Predicated Investigation; Interview of a Federal Prisoner Held in the Custody

of the BOP or USMS During an FBI Assessment or Predicated Investigation 1

C.1 (U) Overview/Summary 1

C.2 (U) Legal Authority 1

C.3 (U) Definitions 1

C.3.1 (U) Use and Targeting a Federal Prisoner 2

C.3.2 (U) Interview a Federal Prisoner 2

C.4 (U) Approval Requirements 2

C.4.1 (U) Approval - Use and Targeting of a Federal Prisoner 2

C.4.2 (U) Approval - Interview a Federal Prisoner 3

C.5 (U) Exemptions to DOJ Approval Requirement 4

C.6 (U) Extension Requests 4

C.7 (U) Transportation of Federal Prisoner 5

D Appendix D: (U) DEPARTMENT OF JUSTICE MEMORANDA ON COMMUNICATIONS WITH THE WHITE HOUSE AND CONGRESS 1

D.1 (U) Communications with the White House 2

D.2 (U) Communications with Congress 7

E Appendix E: (U//~~FOUO~~) Attorney General Memorandum – Revised Policy on the Use or Disclosure of FISA information, dated January 10, 2008 1

F Appendix F: (U) DOJ Policy on Use of Force 1

F.1 (U) Use of Less-Than-Lethal Devices 1

F.2 (U) Use of Deadly Force ..... Error! Bookmark not defined.

G Appendix G: (U) Classified Provisions 1

H Appendix H: (U) Pre-Title III Electronic Surveillance (ELSUR) Search Policy 1

H.1 (U) Scope 1

H.1.1 (U) Compliance With The Previous Application Provision 1

H.1.1.1 (U) When To Search 1

H.1.1.2 (U) How To Search 1

H.1.1.2.1 (U) Persons 2
H.1.1.2.2 (U) Facilities 2
H.1.1.2.3 (U) Places 3
H.1.1.2.4 (U) ADDITIONS 3
H.1.1.3 (U) Where To Search 3
H.1.1.4 (U) How To Initiate A Search Request 4
H.1.1.4.1 (U) Search Procedure 4
H.1.1.5 (U) Affidavit Language Examples 4
H.1.1.6 (U) Documentation Provided to EOT 5
H.1.1.7 [redacted] 5 b7E

I Appendix I: (U) Accessing Student Records Maintained by an Educational Institution ("Buckley Amendment") 1

I.1 (U) Summary 1

I.2 (U//~~FOUO~~) Accessing Student Information or Records During an Assessment 1

I.2.1 (U) Directory Information 1
I.2.2 (U) Observations 2
I.2.3 (U) Law Enforcement Unit Records 2
I.2.4 (U) Health or Safety Emergency 2
I.2.5 (U) Non-Students 2

I.3 (U//~~FOUO~~) Accessing Student Information or Records in Predicated Investigations 3

I.3.1 (U) Federal Grand Jury Subpoena 3
I.3.2 (U) Administrative Subpoenas 3
I.3.3 (U) FISA Order for Business Records 3
I.3.4 (U) Ex Parte Orders 3

J Appendix J: (U) Case File Management and Indexing 1

J.1 (U) Investigative File Management 1

J.1.1 (U) Office of Origin (OO) 1
J.1.2 (U) Investigative Leads and Lead Office (LO) 2
J.1.2.1 (U) Action Required Lead 2
J.1.2.2 (U) Information Only Lead 2
J.1.3 (U) Office of Origin's Supervision of Cases 2
J.1.4 (U) Investigation and Other Files 3

J.1.4.1 (U) Zero "0" Files 3
J.1.4.2 (U) Double Zero "00" Files 3
J.1.4.3 (U) Administrative "A" Files 4
J.1.4.4 (U) Control "C" Files 4
J.1.4.5 (U) Investigative Files 5
J.1.4.5.1 (U) Assessment Files 5
J.1.4.5.2 (U) Preliminary and Full Investigation (Predicated) Files 5
J.1.4.5.3 (U) Pending/Inactive Full Investigation Files 5
J.1.4.5.4 (U) National Incident-Based Reporting System 6
J.1.4.5.5 (U) Unaddressed Work Files 6
J.1.4.5.6 (U) Spin Off Investigation Files 6
J.1.5 (U) Sub-Files 7
J.2 (U) Indexing - The Role of Indexing in the Management of FBI Information 9
K Appendix K: (U) REQUIREMENT FOR ALL FBI PERSONNEL TO REPORT SUSPECTED ABUSE 1
K.1 (U) Mandatory Reporting 1
K.2 (U) Reporting to Applicable Agencies 2
K.2.1 (U) Reporting Suspected Child Abuse on Federal Land/Property 3
K.2.2 (U) Reporting Suspected Abuse in Foreign Jurisdictions 3
K.3 (U) FBI Internal Notification And Documentation Procedures for Suspected Child Abuse 3
K.3.1 (U) Electronic Communications for Internal Documentation of Child Abuse Reports 4
K.4 (U) Special Notification Requirement for Suspected Human Trafficking of Foreign National Minors 5
K.5 (U//~~FOUO~~) Authorization to Temporarily Delay Reporting 6
K.6 (U) Training 7
K.7 (U) Definitions 7
K.7.1 (U) General Definitions 7
K.7.2 (U) Definitions Specific to Child Abuse 8
K.7.3 (U) Definitions Specific to Elder Abuse 9

L Appendix L: (U) OnLine Investigations 1

M Appendix M: (U) The Fair Credit Reporting Act (FCRA) 1

N Appendix N: (U) FEDERAL TAXPAYER INFORMATION (FTI) 1

N.1 (U) Summary 1

N.2 (U) Application 2

N.3 (U) Definitions 2

N.3.1 (U) Federal Tax Information 2

N.3.2 (U) Return 2

N.3.3 (U) Return Information 2

N.3.4 (U//~~FOUO~~) Taxpayer Return Information 3

N.3.5 (U//~~FOUO~~) Return Information (Information Returns) Other Than Taxpayer Return Information (OTRI) 3

N.3.6 (U) Derivative Tax Information 3

N.4 (U) Department Of Justice Requirements For Obtaining And Safeguarding Federal Taxpayer Information 4

N.5 (U) Disclosure To Federal Officers Or Employees For Administration Of Federal Laws Not Relating To Federal Tax Administration 4

N.5.1 (U) Legal Process For Obtaining FTI in FBI Investigations 4

N.5.1.1 (U) *Ex Parte* Orders (26 U.S.C. § 6103(I)(1)) 4

N.5.1.2 (U) Written Request (Letterhead) 5

N.5.1.3 (U) Disclosure Of Return Information By The IRS Related To Criminal, Terrorist Activities Or Emergency Circumstances (26 U.S.C. § 6103(I)(3)) 6

N.5.1.3.1 (U) Possible Violations Of Federal Criminal Law 6

N.5.1.3.2 (U) Emergency Circumstances 6

N.5.1.3.3 (U) Disclosure By The IRS Of Information Relating To Terrorist Activities (26 U.S.C. § 6103(I)(3)(C)) 6

N.5.2 (U) Terrorism Investigations 7

N.5.2.1 (U) FBI Approval Requirements For Obtaining FTI Via An *Ex Parte* Order In Terrorism Cases 7

N.5.2.2 (U) Written Request Related To Terrorist Activities 8

N.5.3 (U) Background Investigation Requests 9

N.5.4 (U) Information Obtained From State Tax Administration/Agency 9

N.5.5 (U) Other Than FTI 9

N.6 (U) Handling, Storing, And Safeguarding FTI 10
N.6.1 (U) Tracking FTI 10
N.6.2 (U) Marking FTI 11
N.6.3 (U) Handling And Transporting Of FTI 11
N.7 (U) Removable Electronic Media 11
N.8 (U) Disposal Of Material Upon Disposition Of Case 12
N.8.1 (U) Return of FTI 12
N.8.2 (U) Final Disposition of FTI Serialized into Sentinel 13
N.9 (U) Training And Certification 13
O Appendix O: (U) Right to financial Privacy Act 1
O.1 (U) Summary 1
O.2 (U) Definitions 1
O.2.1 (U) Financial Institution (12 U.S.C. § 3401(1)) 1
O.2.2 (U) Financial Records 1
O.2.3 (U) Customers Covered (12 U.S.C. § 3401(5)) 2
O.2.4 (U) Government Authority 2
O.2.5 (U) Law Enforcement Inquiry 2
O.3 (U) Methods For Obtaining Records 2
O.3.1 (U) Written Request 2
O.3.1.1 (U) Forms Required For A Written Request 3
O.3.2 (U) Judicial Subpoena 3
O.3.3 (U) Administrative Subpoena 3
O.3.4 (U) Grand Jury Subpoena 3
O.3.5 (U) Criminal Search Warrants 4
O.3.6 (U) Customer Authorization 5
O.3.7 (U) National Security Letters (NSL) 5
O.3.8 (U) Emergency Access 5
O.3.9 (U) Access To Financial Records For Certain Intelligence And Protective Purposes 6
O.4 (U) Customer Notice Requirements And Procedures 6
O.4.1 (U) Exceptions To Customer Notice 6
O.4.1.1 (U) Delay Of Notice 7
O.4.2 (U) Customer Challenge 7
O.4.3 (U) Certificate Of Compliance (12 U.S. C. § 3403(B)) 8
O.4.4 (U) Receipt Of Records 9

O.5 (U) Dissemination Of Information 9
O.5.1 (U) To The Department Of Justice (DOJ) 9
O.5.2 (U) To Other Federal Departments (Non-DOJ) 9
O.5.3 (U) Transfers To State, Local, And Foreign Governments 9
O.6. (U) Matters Outside The Scope Of The RFPA 9
O.6.1 (U) Financial Institutions 9
O.6.2 (U) Corporations Or Other Legal Entities 10
O.6.3 (U) Not Identifiable With Customer 10
O.6.4 (U) Parties In Interest 10
O.6.5 (U) Other 10
O.7 (U) Roles And Responsibilities 10
O.7.1 (U) FBI Supervisory Personnel 10
O.7.2 (U) Special Agents And Task Force Officers (TFO) 10
O.7.3 (U) Chief Division Counsel (CDC) 11
O.7.4 (U) Office Of The General Counsel (OGC) 11
O.8 (U) Remedies And Sanctions 11
O.9 (U) Reimbursement Cost 11
P Appendix P: (U) Acronyms 1
Q Appendix Q: (U) Definitions 1
R Appendix R: (U) Superseded Documents and NFIPM, MIOG, and MAOP Section 1
S Appendix S: (U) Lists of Investigative Methods 1
S.1 Investigative Methods Listed by Name (Alphabetized) 1
S.2 Investigative Methods Listed by order in DIOG Section 18 2

(U) APPENDICES

Appendix A: (U) The Attorney General's Guidelines for Domestic FBI Operations

Appendix B: (U) Executive Order 12333

Appendix C: (U//~~FOUO~~) Use and Targeting of a Federal Prisoner Held in the Custody of the BOP or USMS During an FBI Predicated Investigation; Interview of a Federal Prisoner Held in the Custody of the BOP or USMS During an FBI Assessment or Predicated Investigation

Appendix D: (U) Department of Justice Memorandum on Communications with the White House and Congress, dated May 11, 2009

Appendix E: (U//~~FOUO~~) Attorney General Memorandum – Revised Policy on the Use or Disclosure of FISA information, dated January 10, 2008

Appendix F: (U) DOJ Policy on Use of Force

Appendix G: (U) Classified Provisions

Appendix H: (U) Pre-Title III Electronic Surveillance (ELSUR) Search Policy

Appendix I: (U) Accessing Student Records Maintained by an Educational Institution ("Buckley Amendment")

Appendix J: (U) Case File Management and Indexing

Appendix K: (U) Reporting of Suspected Child Abuse, Neglect and/or Sexual Exploitation

Appendix L: (U) On-Line Investigations

Appendix M: (U) The Fair Credit Reporting Act (FCRA)

Appendix N: (U) Federal Taxpayer Information (FTI)

Appendix O: (U) Right to Financial Privacy Act (RFPA)

Appendix P: (U) Acronyms

Appendix Q: (U) Definitions

Appendix R: (U) Superseded Documents and NFIPM, MIOG, and MAOP Sections

Appendix S: (U) Lists of Investigative Methods

1 (U) SCOPE AND PURPOSE

1.1 (U) SCOPE

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

A) *(U) The Attorney General's Guidelines for Extraterritorial FBI Operations (AGG-ET)* (December 2, 2020)

B) *(U) Memorandum of Understanding Concerning Overseas and Domestic Activities of the Central Intelligence Agency and the Federal Bureau of Investigation* (July 20, 2005)

C) (U) *Memorandum of Understanding between the Department of State, the Department of Treasury and the Department of Justice Regarding the U.S. Chief of Mission* (November 14, 1996)

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

1.2 (U) PURPOSE

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

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

(U) In addition to this policy document, each FBI Headquarters (FBIHQ) operational division has a policy guide (PG) or several PGs that supplement the DIOG. No policy or PG may contradict, alter, or otherwise modify the standards of the DIOG. A DIOG-related policy or PG must adhere to the standards, requirements and procedures established by the DIOG. Requests for DIOG modifications can be made to the Internal Policy Office (IPO) pursuant to DIOG Section 3.2.2 paragraphs (A), (B), (C) and (D). As a result, numerous FBI manuals, electronic communications, letterhead memoranda (LHM), and other policy documents are incorporated into the DIOG and operational division PGs, thus, consolidating FBI policy.

This Page is Intentionally Blank.

2 (U) GENERAL AUTHORITIES AND PRINCIPLES

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

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

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

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

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

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

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

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

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

2.2 (U) GENERAL FBI AUTHORITIES UNDER AGG-DOM

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

2.2.1 *(U) CONDUCT INVESTIGATIONS AND COLLECT INTELLIGENCE AND EVIDENCE*

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

(U) By regulation, the Attorney General has directed the FBI to investigate violations of the laws of the United States and to collect evidence in investigations in which the United States is or may be a party in interest, except in investigations in which such responsibility is by statute or otherwise specifically assigned to another investigative agency. The FBI's authority to investigate and to collect evidence involving criminal drug laws of the United States is

concurrent with such authority of the Drug Enforcement Administration (DEA) (28 Code of Federal Regulations [CFR] Section [§] 0.85[a]).

2.2.2 *(U) PROVIDE INVESTIGATIVE ASSISTANCE*

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

2.2.3 *(U) CONDUCT INTELLIGENCE ANALYSIS AND PLANNING*

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

2.2.4 *(U) RETAIN AND SHARE INFORMATION*

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

2.3 (U) FBI AS AN INTELLIGENCE AGENCY

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

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

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

2.4 (U) FBI LEAD INVESTIGATIVE AUTHORITIES

2.4.1 *(U) INTRODUCTION*

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

granted other authorities to the Director of the FBI (28 CFR § 0.85[a]). Some of these authorities apply both inside and outside the United States.

2.4.2 *(U) TERRORISM AND COUNTERTERRORISM INVESTIGATIONS*

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

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

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

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

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

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

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

2.4.2.1 (U) FEDERAL CRIMES OF TERRORISM

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

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

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

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

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

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

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

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

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

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

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

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

L) (U) Arson or bombing of government property risking or causing death (18 U.S.C. § 844[f][2] or [3]) (18 U.S.C. § 846[a] grants FBI and the Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF) concurrent authority to investigate violations of this statute). See Section 2.4.2.C above regarding DOJ Memorandum dated 08/03/2010 on ATF/FBI Lead Agency Jurisdiction;

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

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

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

P) (U) Using a computer for unauthorized access, transmission, or retention of protected information (18 U.S.C. § 1030[a][1]) (18 U.S.C. § 1030[d][2] grants the FBI "primary authority" to investigate Section 1030[a][1] offenses involving espionage, foreign counterintelligence, information protected against unauthorized disclosure for reasons of national defense or foreign relations, or

Restricted Data as defined in the Atomic Energy Act, except for offenses affecting United States Secret Service (USSS) duties under 18 U.S.C. § 3056[a]);

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

NN) (U) Prohibitions against the financing of terrorism (applies to offenses occurring outside the United States in certain situations including on board a vessel flying the flag of the United States or an aircraft registered under the laws of the United States) (18 U.S.C. § 2339C). See the *Memorandum of Agreement between the Department of Justice and Department of Homeland Security Concerning Terrorist Financing Investigations* (May 13, 2003);

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

C) (U) Damages or destroys by means of fire or explosive any building, vehicle, or other personal or real property, possessed, owned, or leased to the United States or any agency thereof, or any institution receiving federal financial assistance (18 U.S.C. § 844[f][1]) (18 U.S.C. § 846[a] grants FBI and ATF concurrent authority to investigate violations of this statute). See Section 2.4.2C above regarding DOJ Memorandum dated 08/03/2010 on ATF/FBI Lead Agency Jurisdiction;

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

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

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

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

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

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

[redacted]

(U//~~FOUO~~) Areas addressed in Annex II [redacted]

[redacted] Both NSPD-46/HSPD-15 and Annex II thereto are classified.

2.4.3 *(U) COUNTERINTELLIGENCE AND ESPIONAGE INVESTIGATIONS*

(U//~~FOUO~~) A representative list of federal statutes applicable to counterintelligence and espionage investigations appears below. For additional information, refer to the classified *Counterintelligence Division Policy Directive and Policy Guide (0717DPG* [redacted] b7E

[redacted]

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

(U) Section 603 of the Intelligence Authorization Act of 1990 (P.L. 101-193) states that, subject to the authority of the Attorney General, "the FBI shall supervise the conduct of all investigations of violations of the espionage laws of the United States by persons employed by or assigned to United States diplomatic missions abroad. All departments and agencies shall provide appropriate assistance to the FBI in the conduct of such investigations." Consult *The Attorney General's Guidelines for FBI Supervision or Conduct of Espionage Investigations of U.S. Diplomatic Missions Personnel Abroad* [links to ~~SECRET//NOFORN~~ document] (April 17, 1990).

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

(U) The National Security Act of 1947, as amended, establishes procedures for the coordination of counterintelligence activities (50 U.S.C. § 3381). Part of that statute requires that, absent extraordinary circumstances as approved by the President in writing on a case-by-case basis, the head of each executive branch department or agency must ensure that the FBI is "advised immediately of any information, regardless of its origin, which indicates that classified information is being, or may have been, disclosed in an unauthorized manner to a foreign power or an agent of a foreign power."

2.4.4 *(U) CRIMINAL INVESTIGATIONS*

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

2.4.4.1 (U) INVESTIGATIONS OF AIRCRAFT PIRACY AND RELATED VIOLATIONS

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

2.4.4.2 (U) VIOLENT CRIMES AGAINST TRAVELERS

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

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

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

2.4.4.4 (U) INVESTIGATIONS OF SERIAL KILLINGS

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

2.4.5 *(U) AUTHORITY OF AN FBI SPECIAL AGENT*

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

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

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

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

D) (U) Serve and execute arrest warrants and seize property under warrant; issue and/or serve administrative subpoenas; serve subpoenas issued by other proper authority; and

make civil investigative demands (18 U.S.C. §§ 3052, 3107; 21 U.S.C. § 876; 15 U.S.C. § 1312);

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

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

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

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

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

2.5 (U) STATUS AS INTERNAL GUIDANCE

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

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

2.6.1 *(U) DEFINITION*

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

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

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

2.6.3 *(U) EMERGENCY DEPARTURES FROM THE AGG-DOM*

(U//~~FOUO~~) If a departure from the AGG-Dom is necessary without prior approval because of the immediacy or gravity of a threat to the safety of persons or property or to the national security, an FBI employee may, at his/her discretion, depart from the requirements of the AGG-Dom when the designated approving authority for the investigative activity cannot be contacted through reasonable means. The Director, the Deputy Director, or a designated EAD, the GC and IPO must be notified by EC of the departure as soon thereafter as practicable, but not more than 5 business days after the departure using file number 333-HQ-C1629406. The OGC must provide timely written notice of departures from the AGG-Dom to either the DOJ Criminal Division or NSD, whichever is appropriate, or to both of them, and the Criminal Division or NSD must notify the Attorney General and the Deputy Attorney General. Notwithstanding this paragraph, all activities in all circumstances must be carried out in a manner consistent with the Constitution and laws of the United States. (AGG-Dom, Part I.D.3.)

2.6.4 *(U) RECORDS OF DEPARTURES FROM THE AGG-DOM*

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

2.7 (U) DEPARTURES FROM THE DIOG AND DIOG-RELATED POLICIES

2.7.1 *(U) DEFINITION*

(U//~~FOUO~~) A "departure" from the DIOG is a deliberate deviation from a specific known requirement or action governed by the DIOG. The word "deliberate" means the employee was aware of the DIOG requirement and affirmatively chose to depart from it for operational reasons before the activity took place. Approval of a departure must be based upon a specific circumstance involving a specific administrative or operational need. An approval may be for the duration of an investigation or relate to a specific classification, cannot extend beyond the scope of authority of the approving official, and must be approved in accordance with the guidance provided in this subsection. (See list of DIOG-related policies.)

(U//~~FOUO~~) DIOG-related policies and policy guides (PG) must follow this departure review and approval process.

2.7.2 *(U) DEPARTURE FROM THE DIOG AND DIOG-RELATED POLICIES*

(U//~~FOUO~~) A request for a departure from the DIOG must be submitted with an EC using file number 333-HQ-C1629406 and must be approved by the appropriate operational program Assistant Director (AD) and the AD of OIC, with notice to the GC and IPO. The approving EC must document the scope; necessity; program-related value; specific circumstances that limit the departure's application; and an evaluation of what, if any, risk the departure may create for systemic or unintended non-compliance with the DIOG or other policies. Notwithstanding this paragraph, all activities in all circumstances must be carried out in a manner consistent with the Constitution, laws of the United States, Executive Orders, Presidential Directives, Department of Justice guidelines, Office of the Director of National Intelligence policy directives and interagency agreements. (See list of DIOG-related policies.)

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

2.7.3 *(U) EMERGENCY DEPARTURES FROM THE DIOG AND DIOG-RELATED PGS*

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

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

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

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

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

2.7.4 *(U) RECORDS OF DEPARTURES FROM THE DIOG AND DIOG-RELATED POLICIES*

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

[1] (U//~~FOUO~~) This is not a permissible factor for departing from the AGG-Dom. Thus, this factor may only provide a basis for a departure from the DIOG that does not require a departure from the AGG-Dom.

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

2.8.1 *(U) SUBSTANTIAL NON-COMPLIANCE WITH THE DIOG AND DIOG-RELATED POLICIES*

2.8.1.1 (U) SUBSTANTIAL NON-COMPLIANCE

(U//~~FOUO~~) "Substantial non-compliance" means non-compliance that is of significance to the matter and is more than a minor deviation from a DIOG requirement.[2] Non-compliance that relates solely to administrative or peripheral requirements is not substantial. While the examples listed below do not comprise an exhaustive list and are not required elements, substantial noncompliance specifically includes any of the following:

A) (U//F~~OUO~~) The unauthorized use of an investigative method:

B) (U//F~~OUO~~) The failure to obtain required supervisory approval;[3] and

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

(U//~~FOUO~~) **Example A:** During an Assessment, ASAC approval was not obtained before [redacted] to conduct surveillance. b7E
Because the approval was not obtained in advance nor was it done pursuant to an emergency situation as described in 2.7.3, this would be "substantial" non-compliance with DIOG sections 18.5.8.3.3 and 18.5.8.3.4 and must be reported to OIC as set forth in 2.8.2 below.

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

2.8.1.2 (U) OTHER NON-COMPLIANCE

(U//F~~OUO~~) An employee who discovers non-compliance that appears to be non-substantial must report the non-compliance to the Division Compliance Officer (DCO). Normally, non-compliance that is not "substantial" need not be reported to OIC. If there is uncertainty regarding whether a particular matter is substantial or not, the matter should be reported to OIC via EC using the "Report of Non-compliance with DIOG" template in Sentinel. Nevertheless, whenever non-compliance is discovered (whether reported or not), appropriate remedial action must be taken by the relevant employee(s) to correct the non-compliance, including implementing any preventative measures that would help eliminate possible future non-compliance.

(U//~~FOUO~~) **Example:** An SSA discovers that she conducted a file review 20 days late. This relates to an administrative requirement and, without more, is not "substantial"

---

[2] (U//~~FOUO~~) Departures from the AGG-Dom and the DIOG do not fall within the definition of "non-compliance" as used in this section. Departures are to be handled as described Sections 2.6 and 2.7 and should not be reported as "non-compliance" matters.

[3] (U//~~FOUO~~) If supervisory approval was obtained pursuant to Section 2.7.3 (Emergency Departure from the DIOG), the failure to document this approval within 5 business days is a reportable "substantial non-compliance" matter.

noncompliance and does not have to be reported to OIC. The SSA should, however, report the noncompliance to the DCO and take appropriate preventative measures to avoid recurrence.

2.8.2 *(U) DOCUMENTATION OF SUBSTANTIAL NON-COMPLIANCE*

(U//~~FOUO~~) Substantial non-compliance with the DIOG must be reported. The report should be submitted by the party committing the non-compliance, if at all possible. It must be reported via EC using the "Report of Non-Compliance for DIOG and DIOG-Related Policies" template in Sentinel. The EC must include the following information:

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

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

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

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

E) (U//~~FOUO~~) If the substantial non-compliance was the result of the failure to obtain appropriate supervisory approval, a statement as to whether that official, or the current official in the appropriate supervisory position, would have approved the action if a timely request had been made based on the facts and circumstances then known;

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

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

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

2.8.3 *(U) REPORTING AUTHORITIES*

(U//~~FOUO~~) If the substantial non-compliance occurred in a field office, the EC must be approved by the DCO and addressed to the ADIC/SAC. If the substantial non-compliance occurred at FBI Headquarters (FBIHQ), the EC must be approved by the DCO and addressed to the employee's Assistant Director. A copy of the EC must be provided to the Office of Integrity and Compliance (OIC) and to the Office of the General Counsel (OGC) using file number 380C-HQ-A3613620 and 380C-HQ-A3613620-(field office designator). In addition, if the ADIC/SAC or AD assesses that the non-compliance appears to reflect intentional or willful misconduct; it must be reported separately by EC to the Internal Affairs Section of the Inspection Division.

2.8.4 *(U) ROLE OF OIC AND OGC*

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

intelligence activities and/or national security investigations, either division or FBI wide, OIC must notify OGC/NSCLB of this systemic problem.

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

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

2.8.4.1 (U) DISCONTINUATION OF REPORTING

(U//~~FOUO~~) If OIC determines that a sufficient amount of data has been received regarding a particular substantial non-compliance issue to identify a systemic trend, the OIC AD may eliminate the reporting requirement by providing written notification to the field and headquarters divisions indicating that the reporting of a particular substantial non-compliance matter to OIC is no longer necessary or required. OIC must coordinate with OGC and IPO before written notification is provided to field and headquarters divisions to ensure no reporting obligations outside the FBI will be affected, and to ensure all logical data collection pertaining to the substantial non-compliance has been acquired. The OIC written notification must be documented in case file number 380C-HQ-A3613620.

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

(U//~~FOUO~~) If the substantial non-compliance is also a potential IOB matter, the matter must be reported in accordance with the requirements and procedures for reporting potential IOB matters to OGC/NSCLB. See DIOG Section 4. No additional reporting of the incident needs to be made to OIC under this section.

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

(U//~~FOUO~~) Substantial non-compliance with DIOG-related Policy/Program Guides must be reported by EC or subsequent form to the SAC/ADIC, with a copy to the pertinent Headquarters Program Manager, and to the OIC, OGC, and the IPO using file number 380C-HQ-A3613620.

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

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

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

(U) The *AGG-Dom* applies to FBI domestic investigative activities and do not limit other authorized activities of the FBI. The authority for such other activities may be derived from the

authority of the Attorney General as provided in federal statutes, guidelines, or Executive Orders. The scope and approval of these other authorized activities are addressed in the policies that govern the activity and these policies must be relied on when engaging in such activities. Examples of authorized FBI activities not governed by the AGG-Dom include, but are not limited to, the FBI's responsibilities to conduct background checks and inquiries concerning applicants and employees under federal personnel security programs (e.g., background investigations), FBI physical building security issues, Office of Professional Responsibility/personnel issues, activities conducted by the Insider Threat Office concerning potential FBI insider threats, certain administrative claims/civil actions, the FBI's maintenance and operation of national criminal records systems and preparation of national crime statistics, and the forensic assistance and administration functions of the FBI Laboratory. (AGG-Dom, Part I.D.4.) FBI employees must be cognizant that the authority underpinning these responsibilities cannot be utilized to further the objectives of FBI activities governed by the AGG-Dom without recognizing and mitigating the potential negative impact on public trust and the privacy and civil liberties of the affected person(s). For instance, FBI employees should not conduct or participate in the personnel security related background interview of an applicant to further the objectives of a separate criminal investigation of the applicant without appropriately considering sensitivities and the potential impact(s) upon public trust. Likewise, a strategic or defensive intelligence briefing provided to a federal official cannot be designed as an intelligence or evidence collection platform directed at that official, unless significant operational considerations preclude other means to achieve the intelligence or investigative activity.

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

2.10 (U) USE OF CLASSIFIED INVESTIGATIVE TECHNOLOGIES

(U) Inappropriate use of classified investigative technologies may risk the compromise of such technologies. Hence, in an investigation relating to activities in violation of federal criminal law that does not concern a threat to the national security or foreign intelligence, the use of such technologies must be in conformity with the Procedures for the Use of Classified Investigative Technologies in Criminal Cases (AGG-Dom, Part V.B.2), *Domestic Technical Assistance Policy Directive and Policy Guide* (0554DPG) (DTA DPG), and any other FBI policies concerning such technology use.

2.11 (U) APPLICATION OF AGG-DOM AND DIOG

(U//~~FOUO~~) The AGG-Dom and DIOG apply to all FBI domestic investigations and operations conducted by an "FBI employee" or an FBI confidential human source (CHS), when operating pursuant to the tasking or instructions of an FBI employee. The term "FBI employee" includes, but is not limited to, an operational/administrative professional staff person, intelligence analyst, special agent, task force officer (TFO), task force member (TFM), task force participant (TFP),

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

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

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

2.12 (U) JOINT INVESTIGATIONS

(U//~~FOUO~~) In joint investigations, the policy and procedures for conducting any investigative method or investigative activity by employees or CHSs are usually governed by FBI policy. Similarly, employees from other agencies who are participating in a joint investigation with the FBI are generally governed by their agencies' policies regarding approvals. If, however, the FBI has assumed supervision and oversight of another agency's employee (e.g., a full time JTTF Task Force Officer), then FBI policy regarding investigative methods or investigative activity controls. Similarly, if another agency has assumed supervision and oversight of a FBI employee, unless otherwise delineated by MOU, the other agency's policy regarding investigative methods or investigative activity controls.

This Page is Intentionally Blank.

3 (U) CORE VALUES, ROLES, AND RESPONSIBILITIES

3.1 (U) THE FBI'S CORE VALUES

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

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

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

C) (U) Compassion

D) (U) Fairness

E) (U) Uncompromising personal integrity and institutional integrity

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

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

H) (U) Diversity

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

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

3.1.1 *(U) COMPLIANCE*

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

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

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

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

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

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

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

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

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

(U//~~FOUO~~) The Deputy Director works through the Internal Policy Office (IPO) to ensure the following:

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

B) (U//~~FOUO~~) The DIOG is continually reviewed, clarified, and updated based upon a number of factors, to include new or revised statutory requirements, executive orders, Attorney General Guidelines, and identified policy gaps or compliance issues. Therefore, the IPO, which is

responsible for all FBI policy matters, coordinates with FBIHQ divisions and field offices to make policy revisions to the DIOG and the PGs whenever necessary and appropriate;

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

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

3.3 (U) SPECIAL AGENT/TASK FORCE OFFICER (TFO)/TASK FORCE MEMBER (TFM)/TASK FORCE PARTICIPANT (TFP)/FBI CONTRACTOR/OTHERS - ROLES AND RESPONSIBILITIES

3.3.1 *(U) ROLES AND RESPONSIBILITIES*

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

3.3.1.1 (U) TRAINING

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

3.3.1.2 (U) INVESTIGATIVE ACTIVITY

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

3.3.1.3 (U) PRIVACY AND CIVIL LIBERTIES

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

3.3.1.4 (U) PROTECT RIGHTS

(U//~~FOUO~~) Conduct no investigative activity based solely on the exercise of First Amendment rights (i.e., the free exercise of speech, religion, assembly, press or petition) or on the race, ethnicity, gender, national origin, religion, disabilities, sexual orientation, or gender identity of the subject (See DIOG Section 4). Must carry out their operations consistent with their legal obligations to members of the public with disabilities under Section 504 of the Rehabilitation Act of 1973, 29 U.S.C. Section 794 and the implementing

regulations for federally conducted activities. Must not unlawfully discriminate against anyone with a disability and must treat persons with disabilities with professionalism and respect.

3.3.1.5 (U) COMPLIANCE

(U//~~FOUO~~) Ensure compliance with the DIOG, including standards for opening, conducting, and closing an investigative activity; collection activity; or use of an investigative method, as provided in DIOG section 18;

3.3.1.6 (U) REPORT NON-COMPLIANCE

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

3.3.1.7 (U) ASSIST VICTIMS

(U//~~FOUO~~) Identify victims who have suffered direct physical, emotional, or financial harm as result of the commission of federal crimes, offer the FBI's assistance to victims of these crimes, and provide victims' contact information to the responsible FBI victim specialist (VS). The VS is thereafter responsible for keeping victims updated on the status of the investigation to the extent permitted by law, regulation, or policy, unless the victim has opted not to receive assistance. The FBI's responsibility for assisting victims is continuous as long as there is an open investigation. Comprehensive requirements pertaining to the mandatory provision of services to victims are located in the *Victim Services Policy Guide* (1010PG);

3.3.1.8 (U) OBTAIN APPROVAL

(U//~~FOUO~~) Ensure appropriate supervisory approval is obtained for investigative activity as required in the DIOG. Obtain and document oral approval as specified in Section 3.5.2.2 below. Self-approval of DIOG activities is not permitted. See "No Self-Approval Rule" set forth in Section 3.5.2.3 below;

3.3.1.9 (U) ATTRIBUTE INFORMATION TO ORIGINATOR IN REPORTS

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

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

(U//~~FOUO~~) If assigned responsibility for an investigation, manage all aspects of that investigation, until it is assigned to another person. It is the case manager's responsibility to ensure compliance with all applicable laws, rules, regulations, and guidelines, both investigative and administrative, from the opening of the investigation through disposition of the evidence, until the investigation is assigned to another person. If assigned as a co-case agent, co-case manager, or if assigned case-related activities or duties, it is that employee's

responsibility to ensure compliance with all applicable laws, rules, regulations, and guidelines, both investigative and administrative, from the opening of the investigation through disposition of the evidence, until the investigation is assigned to another person or the case related activity requirement(s) ends.

3.3.1.11 (U) CREATE AND MAINTAIN RECORDS/FILES

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

3.3.1.12 (U) INDEX DOCUMENTS

(U//~~FOUO~~) If assigned responsibility for an investigation, index information in documents. Current guidance for indexing documents may be found in DIOG Appendix J, the Sentinel homepage and on the IMD BuNET page.

3.3.1.13 (U) SEEK FEDERAL PROSECUTION

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

3.3.1.14 (U) RETAIN ORIGINAL NOTES MADE DURING AN INVESTIGATION

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

A) (U) Statements signed by the witness.

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

C) (U) Original notes of interview with prospective witnesses and/or suspects and subjects. In any interview in which preparation of an FD-302 is required (i.e., an interview in which it is anticipated the results will become the subject of court testimony), the handwritten notes must be retained. If interview notes are typed into a mobile electronic device (e.g., a laptop or an electronic tablet), the electronic notes must either be printed or saved to a removable electronic storage media in accordance with the *Mobile Devices and Mobile Applications Policy Guide* (1119PG) and the *Removable Electronic Storage (RES) Media Protection* (0247D) policy directive, and retained in the same manner as original handwritten notes.

D) (U) Dictating the results of an interview onto an audio tape/media in lieu of taking handwritten interview notes may be viewed by a court as "original notes" and, therefore, the audio tape/media must be retained. In such circumstances, the audio tape/media becomes the "original note" material. Conversely, an audio tape/media used for dictation from handwritten interview notes for transcription to a final FD-302 is not "original note" material and the audio tape need not be retained.

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

(U) See also DIOG Section 18.5.6.4.15 (Interview Documentation).

(U) *Note*: For the purpose of this note retention policy, an interview and an interrogation are analogous.

(U//~~FOUO~~) All original handwritten interview notes must be retained as "original note material" in the 1A section of a file. The original handwritten notes may be scanned, but the physical original handwritten notes must be retained regardless of whether or not the notes are scanned. Also see the *Importing Nontransitory Records into Sentinel and Preserving Certain Investigative Nontransitory Records in Original Formats* (1001D) policy directive.

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

(U//~~FOUO~~) In some situations, the sponsoring agency of a TFO, a TFM, or a TFP[4] is required to enter into a memorandum of understanding (MOU) with the FBI that governs the activities of the task force. For purposes of the DIOG, "TFO", "TFM", and "TFP" are defined as follows:

3.3.2.1 (U) TASK FORCE OFFICER

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

A) (U//~~FOUO~~) The individual is a certified federal, state, local, territorial, or tribal law enforcement officer.

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

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

D) (U//~~FOUO~~) The individual is eligible and has initiated the FBI's process for obtaining federal law enforcement credentials.

E) (U//~~FOUO~~) The individual is assigned under the supervision of an FBI-led task force.

F) (U//~~FOUO~~) The individual has initiated a request for a security clearance issued by the FBI. ***Note:*** If the TFO fails to complete the security clearance process, he or she must be removed as a TFO.

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

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

3.3.2.2 (U) TASK FORCE MEMBER

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

[4] (U) A TFO, a TFM, or a TFP must follow their own agency's deadly force policy; however, a TFO, a TFM, or a TFP is bound by the FBI's *Less-Than-Lethal Devices Policy Guide* (1111PG).

A) (U//~~FOUO~~) The individual is an employee of a federal, state, local, territorial, or tribal agency.

B) (U//~~FOUO~~) The individual is assigned under the supervision of an FBI-led task force.

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

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

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

3.3.2.3 (U) TASK FORCE PARTICIPANT

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

A) (U//~~FOUO~~) The individual is an employee of a federal, state, local, territorial, or tribal agency[5].

B) (U//~~FOUO~~) The individual does not otherwise qualify as a TFO or a TFM.

C) (U//~~FOUO~~) The individual has been approved as a TFP by the supervisor responsible for the task force, and the approval has been documented in the appropriate task force file.

Example: A civilian employee of another federal agency may have a particular expertise that is needed by the task force, but the employee does not satisfy the requirements to be a TFO (e.g., not a sworn law enforcement officer) or a TFM (e.g., does not have a security clearance).

(U//~~FOUO~~) When participating as an FBI TFP, the TFP is bound by the rules, regulations, and policies set forth in the DIOG. DIOG-related training for a TFP may be required by the head of the field office/FBIHQ division that governs the activities of the task force.

3.4 (U) INTELLIGENCE ANALYSTS (IA) AND PROFESSIONAL INVESTIGATIVE STAFF[6]

3.4.1 *(U) ROLES AND RESPONSIBILITIES*

3.4.1.1 (U) INTELLIGENCE ANALYSTS

(U) IAs review and analyze internal and public information to identify its intelligence value; prepare and disseminate intelligence products; identify new sources of information; and communicate with other members of the intelligence and law enforcement communities to gain a better understanding of threats, sources of information, operations, missions, and intelligence requirements. The roles and responsibilities of IAs further investigative operations by identifying emerging threats and trends; enhancing collection capabilities in the field and at FBIHQ; and assessing and communicating to investigators, relevant FBI entities,

---

[5] (U//~~FOUO~~) While persons or entities in the private sector may be asked or may volunteer to assist in FBI investigations, they cannot be TFPs on FBI-led task forces.

[6] This subsection does not include guidance o[redacted] b7E
position. See th[redacted] for information on the position.

and members of the intelligence and law enforcement communities real-time, analytic judgments regarding specific threats. IAs may provide support to investigative and intelligence operations as set forth in this subsection.

3.4.1.2 (U) PROFESSIONAL INVESTIGATIVE STAFF

(U) Professional investigative staff includes forensic accountants, staff operations specialists (SOS), nonagent computer scientists, nonagent Computer Analysis and Response Team members, operational support technicians (OST), language analysts (LA), and contract linguists. Oftentimes, professional investigative staff may be asked to participate in investigative or intelligence operations and/or provide administrative support to FBIHQ operational units and/or field office squads. Professional investigative staff may provide support to investigative and intelligence operations as set forth in this subsection.

(U) For the specific roles and responsibilities of Language Analysts and Contract Linguists, see the *Foreign Language Program Policy Guide* (1172PG).

(U) For the specific roles and responsibilities of SOSs, see the *Intelligence Program Policy Guide* (1170PG), subsection 2.15.

3.4.2 *(U) INVESTIGATIVE OR INTELLIGENCE ACTIVITIES*

(U//~~FOUO~~) When involved in investigative or intelligence activities, IAs and professional investigative staff are bound by the AGG-Dom, other applicable investigative AG Guidelines, and the DIOG.

3.4.2.1 (U) TRAINING

(U//~~FOUO~~) IAs and professional investigative staff must obtain training on the DIOG standards relevant to their respective positions, and must perform activities consistent with those standards.

3.4.2.2 (U) INVESTIGATIVE ACTIVITIES

(U//~~FOUO~~) IAs and professional investigative staff must ensure that all investigative and intelligence activities in which they are involved comply with the Constitution, federal law, executive orders, Presidential directives, the AGG-Dom, other AGGs, treaties, memorandums of agreement (MOA)/memorandums of understanding (MOU), the DIOG, and applicable policy directives (PD) and policy guides (PG). If an IA or a professional investigative staff employee is unsure of the legality of any action, he or she must consult with his or her supervisor, the chief division counsel (CDC), or the Office of General Counsel (OGC).

(U//~~FOUO~~) IAs and professional investigative staff must ensure that briefing materials, presentations, and reports are produced and disseminated in accordance with FBI polices and must ensure that proper protocols and dissemination controls are used in accordance with the DIOG and other FBI information-sharing policies.

3.4.2.3 (U) ASSIGNMENT AS CASE MANAGERS AND PARTICIPANTS

(U) IAs may be assigned as case managers or co-case managers for Type 3 and Type 4 Assessments. For additional requirements on opening Type 3 and Type 4 Assessments, see subsections 5.6.3.2.8 and 5.6.3.3.7. The case management responsibilities in Type 5 Assessments can be found in Section 3 of the *Confidential Human Source Policy Guide* (1212PG) (CHSPG).

IAs and professional investigative staff employees may be assigned as case participants for other Assessments and in predicated investigations; however, IAs and professional investigative staff

b7E

3.4.2.4 (U//~~FOUO~~) USE AND APPROVAL REQUIREMENTS OF AUTHORIZED INVESTIGATIVE METHODS

3.4.2.4.1 *(U//~~FOUO~~) METHODS AVAILABLE PRIOR TO OPENING AN ASSESSMENT AND DURING AN ASSESSMENT*

(U//~~FOUO~~) Only the following investigative methods, as set forth in subsection 5.1.1, may be used by an IA or a professional investigative staff employee prior to opening an Assessment or in an Assessment assigned to them:

A. (U//~~FOUO~~) Subsection 5.1.1.1., "Public Information" (except that they may not be approved to attend religious services or events or activities of sensitive organizations (see subsection 18.5.1.3.1)

B. (U//~~FOUO~~) Subsection 5.1.1.2, "Records or Information – FBI and DOJ"

C. (U//~~FOUO~~) Subsection 5.1.1.3, "Records or Information – Other Federal, State, Local, Tribal, or Foreign Government Agency"

D. (U//~~FOUO~~) Subsection 5.1.1.4, "Online Services and Resources" (see Appendix L)

E. (U//~~FOUO~~) Subsection 5.1.1.5, "Clarifying Interview" of the complainant or the person who initially furnished the information. A clarifying interview is limited for the sole purpose of eliminating confusion in the original allegation or information provided. It is not intended to be an "interview" as described in 18.5.6.

F. (U//~~FOUO~~) Subsection 5.1.1.6, "Information Voluntarily Provided by Government or Private Entities" (except that they may not perform consent searches. Instead, such searches must be performed by SAs or TFOs).

(U//~~FOUO~~) In Type 5 Assessments (only), IAs are permitted to use the investigative methods as set forth in DIOG subsection 5.6.3.4.8 and in Section 3 of the *CHSPG*.

3.4.2.4.2 *(U//~~FOUO~~) ASSISTING SAS/TFOS IN THE USE OF OTHER INVESTIGATIVE METHODS IN ASSESSMENTS, PRELIMINARY INVESTIGATIONS, AND FULL INVESTIGATIONS*

(U//~~FOUO~~) If requested by an SA or TFO, IAs and professional investigative staff employees may assist SAs or TFOs in the use of investigative methods beyond those outlined in subsection 3.4.2.4.1. However, in some circumstances, it would be inappropriate or unsafe for an IA or a professional investigative staff employee to assist an SA or TFO in the use of investigative methods beyond those outlined in subsection 3.4.2.4.1. Therefore, the SA or TFO is responsible for exercising sound judgment in determining whether to request an IA or professional investigative staff employee to assist in the use of an investigative method beyond those outlined in subsection 3.4.2.4.1, as well as in determining whether the use of such methods requires the physical presence of an SA or TFO.

(U//~~FOUO~~) **Example 1**: An SA may request an IA or professional investigative staff employee to electronically serve an administrative subpoena for telephone subscriber records in a drug investigation.

(U//~~FOUO~~) **Example 2**: An SA may request a language specialist to accompany and participate with him or her in an office interview of a human trafficking victim who speaks a foreign language. A different determination concerning the language specialist's assistance would likely be made if the interview were to take place at an unsafe location.

(U//~~FOUO~~) (**Note**: See *CHSPG*, Section 2, for guidance regarding contact with, or debriefing of, a Potential CHS or CHS).

3.4.2.5 (U) PRIVACY AND CIVIL LIBERTIES

(U//~~FOUO~~) IAs and professional investigative staff must ensure that civil liberties and privacy are protected throughout the Assessment or investigative process.

3.4.2.6 (U) PROTECT RIGHTS

(U//~~FOUO~~) IAs and professional investigative staff must not conduct investigative activity based solely on the exercise of First Amendment rights (i.e., the free exercise of speech, religion, assembly, press, or petition) or on the race, ethnicity, gender, national origin, religion, disabilities, sexual orientation, or gender identity of the subject. (See DIOG Section 4.)

3.4.2.7 (U) COMPLIANCE

(U//~~FOUO~~) IAs and professional investigative staff must ensure compliance with the DIOG, including standards for opening, conducting, and closing investigative activities; collection activities; or the use of investigative methods, as provided in DIOG section 18.

3.4.2.8 (U) REPORT NONCOMPLIANCE

(U//~~FOUO~~) IAs and professional investigative staff must comply with laws, rules, and regulations, and must report any noncompliance concerns to the proper authorities. For specific requirements and procedures for reporting departures and noncompliance with the AGG-Dom and the DIOG, see DIOG subsections 2.6 through 2.8.

3.4.2.9 (U) ASSIST VICTIMS

(U//~~FOUO~~) IAs and professional investigative staff may assist agents and TFOs in identifying victims who have suffered direct physical, emotional, or financial harm as a result of the commission of federal crimes by providing victim contact information to the responsible FBI victim specialist (VS). The VS is thereafter responsible for keeping victims updated on the status of the investigation—to the extent permitted by laws, regulations, or policies, unless the victim has opted to not receive assistance. The FBI's responsibility for assisting victims is continuous, as long as there is an open investigation. Comprehensive requirements pertaining to the mandatory provision of services to victims are located in the *Victim Services Policy Guide (1010PG)*.

3.4.2.10 (U) OBTAIN APPROVAL

(U//~~FOUO~~) Ensure appropriate supervisory approval is obtained for investigative activity, as required in the DIOG. Obtain and document oral approval as specified in this subsection and in

subsection 3.5.2.2 below. Self-approval of DIOG activities is not permitted. See subsection 3.5.2.3 below.

3.4.2.11 (U) ATTRIBUTE INFORMATION TO ORIGINATOR IN REPORTS

(U//~~FOUO~~) Ensure that if the originator of information reported to the FBI characterizes an individual, a group, or an activity in a certain way, FBI records (e.g., FD-302s, electronic communications [EC], and letterhead memorandums [LHM]) reflect that another party, and not the FBI, is the originator of the characterization.

(U//~~FOUO~~) **Example**: An FBI document should state: "The complainant advised that the subject was prejudiced and motivated by ethnic bias" rather than "The subject was prejudiced and motivated by ethnic bias."

3.4.2.12 (U) SERVE AS ASSESSMENT ("CASE") MANAGER

(U//~~FOUO~~) If an IA is assigned responsibility for a Type 3, a Type 4, or a Type 5[7] Assessment, he or she is to manage all aspects of that Assessment until it is assigned to another person. It is the IA's responsibility to ensure compliance with all applicable laws, rules, regulations, and guidelines, both investigative and administrative, from the opening of the Assessment through disposition of the evidence, until the Assessment is assigned to another person or the case-related activity requirement(s) ends.

3.4.2.13 (U) CREATE AND MAINTAIN RECORDS AND FILES

(U//~~FOUO~~) Create and maintain authentic, reliable, and trustworthy records; establish files; set leads; index documents; and retain and share information, as specified in DIOG Section 14 and Appendix J. Ensure the proper storage, handling, and maintenance of accumulated data or documents. Original notes taken while participating in an interview, as well as substantive e-communications, must be preserved in accordance with DIOG subsections 3.3.1.14 and 3.3.1.15.

3.4.2.14 (U) INDEX DOCUMENTS

(U//~~FOUO~~) If assigned responsibility for an Assessment, IAs and professional investigative staff must index information in documents. Current guidance for indexing documents may be found in DIOG Appendix J, the Sentinel homepage, and on the Information Management Division (IMD) BuNET page.

3.5 (U) SUPERVISOR ROLES AND RESPONSIBILITIES

3.5.1 *(U) SUPERVISOR DEFINED*

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

A) (U) Supervisory Special Agent (SSA)

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

C) (U) Supervisory Intelligence Analyst (SIA)

---

[7] (U//~~FOUO~~) Per DIOG subsection 5.6.3.4.1.3, an IA is not permitted to be the case manager for the recruitment phase of a Type 5 Assessment.

D) (U) Senior Supervisory Intelligence Analyst (SSIA)

E) (U) Legal Attaché (LEGAT)

F) (U) Deputy Legal Attaché (DLAT)

G) (U) Unit Chief (UC)

H) (U) Assistant Special Agent in Charge (ASAC)

I) (U) Assistant Section Chief (ASC)

J) (U) Section Chief (SC)

K) (U) Special Agent in Charge (SAC)

L) (U) Deputy Assistant Director (DAD)

M)(U) Assistant Director (AD)

N) (U) Assistant Director in Charge (ADIC)

O) (U) Executive Assistant Director (EAD)

P) (U) Associate Deputy Director (ADD)

Q) (U) Deputy Director (DD)

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

(U//~~FOUO~~) The official position equivalents between the field offices and FBIHQ are outlined below. In general, an equivalent position at either the field or FBIHQ may exercise DIOG authority, unless the DIOG specifically limits a given authority, or whenever a specific position is assigned the authority as part of its responsibilities (e.g., ASAC). The equivalent positions are:

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

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

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

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

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

F) (U//~~FOUO~~) SAC = FBIHQ SC

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

3.5.2 *(U) SUPERVISOR RESPONSIBILITIES*

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

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

(U//~~FOUO~~) Only FBI supervisory employees and representatives from other government agencies (OGA) assigned to the FBI under the Joint Duty Assignment Program or the

Intergovernmental Personnel Act as supervisors (as defined in DIOG subsection 3.5.1) may approve the serialization of investigative records into Sentinel. Additionally, whenever an OGA supervisor (as described above) approves an investigative record, an FBI supervisor must also approve the record into Sentinel. An OGA supervisor may not approve investigative methods (i.e., DIOG Section 18 methods) or investigative activities (e.g., UDP and OIA).

(U//~~FOUO~~) Nonsupervisory employees, nonsupervisory OGA personnel, government contractors, detailees, task force officers (TFO), task force members (TFM), and task force participants (TFP) are not permitted to approve investigative records into Sentinel; however, they may draft such records for supervisory review and approval.

3.5.2.2 (U) ORAL AUTHORITY/APPROVAL

(U//~~FOUO~~) Unless otherwise specified by the AGG–Dom or FBI policy, any authority/approval required in the DIOG necessary to conduct investigative activities may be granted orally by the appropriate approving official. Should such oral authorization be granted, appropriate written documentation of the oral authorization must be documented by the FBI employee to the authorizing official as soon as practicable, but not more than five business days after the oral authorization. The effective date of any such oral authorization is the date on which the oral authority was granted, and that date and the name of the approving official must be included in the subsequent written documentation.

(U//~~FOUO~~) Supervisors are not permitted to self-approve investigative or intelligence collection activity or methods in assessments or investigations assigned to them as case agents or analysts. An independent evaluation and approval of these activities must be obtained including the opening and closing of any Assessment or predicated investigation. See Section 3.5.2.3 below.

3.5.2.3 (U) NO SELF-APPROVAL RULE

(U//~~FOUO~~) When approval/authority is required in the DIOG (or related policy guides), to open, utilize an investigative method, close, or perform any administrative requirement within the scope of the DIOG (e.g. initial paperwork to a file, perform a file review), an approving official (supervisor) is not permitted to "self-approve" his or her own work or activity[8]. The supervisor must obtain an independent evaluation, and approval of these activities must be obtained from a supervisor in a position of higher rank.

(U//~~FOUO~~) In the event of an emergency, an employee may exercise an Emergency Departure from the AGG-Dom or from the DIOG, see DIOG subsections 2.6.3 and 2.7.3, respectively. If an FBI employee errantly conducts a self-approval, the approval is considered "substantial non-compliance" (as described in DIOG subsection 2.8.1.1.B) and must be documented in accordance with DIOG subsection 2.8.2.

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

[8] (U) *Note*: See subsection 4.3.4.2. of the *Records and Information Management Policy Guide* (1223PG) for policy on administrative case files.

themselves. The relief SSA/SIA must instead seek approval from the ASAC/SSIA, or wait until the permanent SSA/SIA returns from leave.

(U//~~FOUO~~) Example: An SSA conducts a follow-up interview of a complainant, who provides material information regarding criminal activity. The SSA drafts an FD-302 of the interview to document the information for serialization into the investigative file. The SSA must seek approval of the FD-302 from a supervisor at a higher level (e.g., ASAC or SAC). A "peer" supervisor (i.e., an SSA at the equivalent rank) cannot approve the FD-302.

3.5.2.4 (U) Ensure Compliance with U.S. Regulations and Other Applicable Legal and Policy Requirements

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

3.5.2.5 (U) Training

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

3.5.2.6 (U) Protect Civil Liberties and Privacy

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

3.5.2.7 (U) Report Compliance Concerns

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

3.5.2.8 (U) Non-Retaliation Policy

(U//~~FOUO~~) Supervisors must not retaliate or take adverse action against persons who raise compliance concerns. (See the *Non-Retaliation for Reporting Compliance Risks* [0727D] policy directive.)

3.5.2.9 (U) Create and Maintain Records/Files

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

(U//~~FOUO~~) Supervisors must periodically review investigative, control, and administrative files assigned to their areas of program responsibility or management in accordance with DIOG subsection 3.5.4 below.

3.5.2.10 (U//~~FOUO~~) CERTIFICATIONS FOR IMMIGRATION BENEFITS

(U//~~FOUO~~) Pursuant to the *Delegation of Authority to Sign U-1 Nonimmigrant Status Certifications* (December 13, 2014), the SAC (nondelegable) has the authority to sign OMB Form I-918b as the certifying official to assist non-U.S. citizens who have suffered federal, state or local offenses such as rape, torture, human trafficking, slave trade, and extortion who are residing temporarily in the United States, if that person can provide specific relevant facts to the investigation or prosecution of the criminal activity in question. Whenever the SAC serves as the certifying official, the USAO prosecuting the matter must be notified in writing of the action as soon as practicable, but no more than [redacted] from the date of certification." b7E

(U//~~FOUO~~) Additionally, field office heads (i.e., ADICs/SACs) have the authority to sign Department of Homeland Security (DHS) forms as the certifying official for Continued Presence requests (a program to assist victims of a severe form of trafficking). See the *Victim Services Policy Guide* (1010PG) for complete requirements and procedures.

3.5.3 *(U) DELEGATION AND SUCCESSION IN THE FBI*

(U//~~FOUO~~) The ability to exercise legal authority within the FBI through delegations of legal authority and orderly succession to positions of authority is set forth in the *Succession and Delegation Policy* (0259D) policy directive. A DIOG related policy or PG must adhere to the delegation and succession of authority standards, requirements and procedures established by the DIOG.

3.5.3.1 (U) DELEGATION

(U//~~FOUO~~) As used in the DIOG, the term "delegation" refers to the conveyance of authority to another official (either by position or to a named individual). FBI authority is delegable one supervisory level unless expressly permitted, prohibited, or restricted by law, regulation, or policy. For example, an SAC may delegate his/her authority to approve Sensitive Investigative Matters (SIMs) to an ASAC, but the ASAC cannot further delegate this authority to an SSA. Delegations will continue in effect until modified, revoked, superseded, the position no longer exists, or the named individual vacates the position. A supervisor may only delegate authority to another supervisor one level junior to himself or herself, unless specified otherwise (e.g., an ASAC may delegate authority to an SSA). SACs may restrict delegations within their field offices (e.g., an SAC may prohibit an ASAC from delegating authorities that are assigned to them).

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

(U//~~FOUO~~) It is recognized that the first line supervisor's role in mentoring and training relief supervisors is often accomplished by assigning tasks to those employees while the supervisor is present or available. This type of activity is permitted so long as the supervisor is

monitoring the progress and outcome(s) of the assignments and is not abdicating the responsibilities associated with his or her supervisory position. For example, an SSA may assign a relief supervisor to routinely review and assign investigative leads to others on the squad. This type of task promotes effective supervision and provides a monitored opportunity for the relief supervisor to hone his or her management abilities.

3.5.3.2 (U) SUCCESSION: ACTING SUPERVISORY AUTHORITY

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

(U//~~FOUO~~) The FBI follows the general rule, recognized in law, that employees properly designated as "acting" in a position exercise the full legal authorities of that position, unless specifically precluded by higher authority or by an applicable law, regulation, or policy. Accordingly, unless expressly precluded, any authority vested in an FBI supervisor pursuant to the DIOG may be exercised by someone who occupies that position in an acting status. An employee may be designated to an acting position either through a succession plan or ad hoc designation. See the *Succession and Delegation Policy* (0259D) policy directive for additional details.

3.5.3.3 (U) DOCUMENTATION

(U//~~FOUO~~) Delegations of authority as well as succession plans and ad hoc designations must be documented in writing and maintained in the appropriate administrative file identified below whenever practicable, unless specifically required by the DIOG. Administrative files have been created by IMD to maintain documentation of delegations of authority, to include ad hoc designations and succession plans.

3.5.3.3.1 *(U//~~FOUO~~) "DELEGATIONS OF AUTHORITY RELATED TO SENIOR EXECUTIVES" – FILE 319X-HQ-A1700684-XX*

(U//~~FOUO~~) File 319X-HQ-A1700684-XX, with the last two alpha characters designating a particular field office, FBIHQ Division, or LEGAT, must be used to document delegations of authority related to the responsibilities of senior executive positions (defined in the Director & Senior Officials [07-01] Retention Schedule) as only the Director, Deputy Director, Chief of Staff, Associate Deputy Director, and Executive Assistant Director(s). (*Note*: This file does **not** include Senior Executive Service [SES] delegations of authority. Such delegations of authority by SES and all other supervisory management officials must be documented using the file specified below in DIOG Section 3.5.3.3.2)

3.5.3.3.2 *(U//~~FOUO~~) "DELEGATIONS OF AUTHORITY RELATED TO NON-SENIOR EXECUTIVES" (INCLUDING ALL SENIOR EXECUTIVE SERVICE [SES] AND OTHER SUPERVISORY MANAGEMENT OFFICIALS) AND ALL ADHOC DESIGNATIONS – FILE 319X-HQ-A1700685-XX*

(U//~~FOUO~~) File 319X-HQ-A1700685-XX, with the last two alpha characters designating a particular field office, FBIHQ Division, or LEGAT, must be used to document delegations of

authority related to the responsibilities of non-senior executive positions, to include all SES level and other supervisory management officials not included above in DIOG Section 3.5.3.3.1, as well as to document ad hoc designations, as specified.

(U//~~FOUO~~) Documentation of acting authority may take place subsequent to the actual ad hoc designation. For example, an SSA orally advises his principal relief supervisor that he/she has an emergency and will not be able to come into the office. The ad hoc designation of the relief supervisor as acting SSA can be documented upon the SSA's return to the office. Failure to document an ad hoc designation does not invalidate the designation but may result in difficulty proving the appropriate exercise of authority if required to do so. (See Section 3.5.2.2 above concerning oral authorizations and related documentation requirements).

3.5.3.3.3 *(U//~~FOUO~~) Succession Plans – File 319X-HQ-A1538387*

(U//~~FOUO~~) An administrative file has also been created to maintain documentation of succession plans (319X-HQ-A1538387-XX with the last two alpha characters designating the particular field office, FBIHQ Division or LEGAT).

3.5.4 *(U) File Reviews and Justification Reviews*

3.5.4.1 (U) Overview

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

(U//~~FOUO~~) Supervisory review of investigative files (main file and all subfiles) are especially important with regard to tracking the progress and development of new employees. This provides an opportunity for supervisors to guide employees on how properly manage and document investigative files and to use and document investigative methods, while emphasizing the importance of compliance and recognition of risk. In addition, the file review process is an opportunity to begin to evaluate an employee's level of performance and to identify his or her strengths and weaknesses. Performance evaluation must not be documented on the file review itself; rather, any notes regarding performance must be documented using the Performance Management Tool (i.e., Check-In, Quick Feedback, or Wrap-up). See DIOG subsection 3.5.4.8 for further guidance.

(U//~~FOUO~~) File reviews help supervisors ensure that their offices are effectively supervising activities in their respective territories and are monitoring investigative activities carried out on their behalf in other field offices. For example, a supervisor may use a file review to ensure that an employee assigned to an investigation has addressed all logical investigation in a timely manner or that the employee has successfully set necessary leads. Additionally, the periodic review of control files and relevant administrative files permits supervisors to evaluate progress in meeting program-related objectives and helps to ensure that FBI resources are aligned with strategic objectives and are being utilized and managed properly and in accordance with policy standards.

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

(U//~~FOUO~~) File reviews (including the main file and all subfiles) must be conducted for all predicated investigations, including investigations placed in "pending inactive" status, unaddressed work files, and Type 3–6 Assessments. Type 1 & 2 Assessments must have 30-calendar-day justification reviews, as specified below.

(U//~~FOUO~~) Note: It is not necessary to separately document the review of individual subfiles in Sentinel, independent of the review of the main case file.

3.5.4.3 (U) Frequency of File Reviews

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

A) **(U//~~FOUO~~) For agents, resident agents, TFOs, IAs, and other employees assigned investigative files – 90 Days.** The supervisor must review the files (i.e., main file and sub-files) for all investigations (including pending predicated investigations, pending inactive investigations, unaddressed work files, and Type 3–6 assessments, or special event 300A files) for each consecutive 90-calendar-day period.

   1. **(U//~~FOUO~~) 30 additional calendar days:** The case manager and the supervisor must complete the file review process and file review documentation, as described in DIOG subsections 3.5.4.5–3.5.4.9 below, including tasks identified while conducting the in person or telephonic session, must be completed within 30 calendar days following each consecutive 90 calendar day file review period. The ASAC's (or, as appropriate, SSIA's) review of the file review package, while mandatory, does not need to be completed within this 30-calendar-day window.

B) **(U//~~FOUO~~) For probationary employees (agents, resident agents, IAs, and other employees assigned investigative files) – 60 Days.** The supervisor must review the files (i.e., main file and sub-files) for all investigations (including pending predicated investigations, pending inactive investigations, unaddressed work files, and Type 3-6 assessments, special event 300A files) for each consecutive 60-calendar-day period.

   1. **(U//~~FOUO~~) 30 additional calendar days:** The case manager and the supervisor must complete the file review process and file review documentation, as described in DIOG subsections 3.5.4.5–3.5.4.9 below, including tasks identified while conducting the in person or telephonic session, must be completed by the case manager and supervisor within 30 calendar days following each consecutive 60 calendar day file review period. The ASAC's (or, as appropriate, SSIA's) review of the file review package, while mandatory, does not need to be completed within this 30-calendar-day window.

3.5.4.4 (U) Delegation of File Reviews

(U//~~FOUO~~) Thorough and complete file reviews are an important part of the compliance regimen, provide valuable and needed information for the purpose of evaluating the performance of employees, and are critical to the effective management of a squad. For these reasons, file reviews are an important duty and responsibility for supervisors, and supervisors are discouraged from routinely delegating these reviews. However, because conducting a file review is an important developmental opportunity for primary relief supervisors, file reviews may be conducted by duly designated acting supervisors or duly designated primary relief supervisors. Acting supervisors may conduct file reviews just as they would conduct any other supervisory duty while functioning in an acting capacity. Primary relief supervisors may

conduct file reviews; however, when they do so, the next required file review must be conducted by a supervisor or a duly designated acting supervisor. In other words, every other file review of any given investigative file must be conducted by a supervisor or a duly designated acting supervisor. Acting supervisors may not review their own files under any circumstances; they must either reassign their investigations or have their investigations reviewed by a supervisor in a position of higher rank. (See DIOG subsection 3.5.2.3)

3.5.4.5 (U) PREDICATED INVESTIGATIONS AND TYPE 3, 4, AND 6 ASSESSMENT – FILE REVIEW REQUIREMENTS

(U//~~FOUO~~) A file review must be conducted in person, or by telephone, Skype, or another similar method, when necessary (e.g., if an employee is on a TDY assignment or is located in a remote resident agency [RA]); must be conducted in private; and must be documented as specified in DIOG subsection 3.5.4.8.

(U//~~FOUO~~) The file review process requires the supervisor to (1) review the investigative files (including the main file and all sub-files) assigned to the employee; (2) discuss progress made in the last 60- or 90-calendar-day period toward specified investigative or intelligence collection objectives, (3) discuss the projected work or future objectives being contemplated and the method(s) to achieve them during the next review period and (4) document that information in the file review package generated by Sentinel.

(U//~~FOUO~~) When reviewing the employee's assigned investigative files (i.e., main file and sub-files), the supervisor should consider the following, whenever applicable, whether evaluating an Assessment or a predicated investigation:

A) (U//~~FOUO~~) That no investigative activity is based solely on activity that is protected by the First Amendment or on the race, ethnicity, gender, national origin, religion, disability, sexual orientation, or gender identity of an individual, group, or organization or a combination of only those factors.

B) (U//~~FOUO~~) Whether the activities that occurred in the prior 60 or 90 calendar days were appropriate based upon the investigative category, the type of case classification, and the stated objectives and whether investigative methods were used in compliance with applicable DIOG requirements.

C) (U//~~FOUO~~) Whether subject(s) have been indexed in compliance with indexing guidelines.

D) (U//~~FOUO~~) Whether threat issues and Topic Tags for the investigation or Assessment were identified and current.

E) (U//~~FOUO~~) Whether victim services policies have been followed (i.e., identification, notification to the VS, documentation, case status updates) in compliance with the DIOG and the *Victim Services Policy Guide* (1010PG).

F) (U//~~FOUO~~) Whether information shared with domestic or foreign agencies was conducted in accordance with dissemination policies.

G) (U//~~FOUO~~) Whether liaison and tripwire activity was documented.

H) (U//~~FOUO~~) Whether statistical accomplishments (i.e., accomplishments in the "Accomplishments" module of Sentinel) were entered within established timeframes.

I) (U//~~FOUO~~) Whether evidence was stored and disposed of properly and whether documentation was completed according to evidence control policies.

J) (U//~~FOUO~~) Whether leads were covered within established deadlines.

K) (U//~~FOUO~~) Whether any intelligence in the investigation or Assessment resulted in the production of intelligence products (e.g., intelligence information reports [IIR], situational information reports [SIR], intelligence bulletins, intelligence assessments) and whether the reports were released to the intelligence or law enforcement community and were properly documented in the INTELPRODS subfile, in compliance with the DIOG.

L) (U//~~FOUO~~) Whether national security letters (NSL) were issued in accordance with policies, including whether responsive materials were appropriately examined (e.g., examined for overproduction).

M) (U//~~FOUO~~) Whether federal grand jury (FGJ) subpoenas were issued in accordance with policies, including whether responsive materials were appropriately examined (e.g., examined for overproduction), and whether FGJ materials covered by Rule 6e were properly marked and handled, including being appropriately restricted in Sentinel.

N) (U//~~FOUO~~) Whether documents obtained pursuant to a criminal mail cover request were returned to the USPS within 60 calendar days of the criminal mail cover's termination date and if the return was documented in the investigative file.

O) (U//~~FOUO~~) Whether administrative subpoenas were issued in accordance with policies, including whether responsive materials were appropriately examined (e.g., examined for overproduction).

P) (U//~~FOUO~~) Whether case-related electronic communications, including e-mail, text messages, phone calls, and instant messages, were appropriately uploaded into Sentinel or another IMD-authorized recordkeeping system. See the *Records and Management Management Policy Guide* (1223PG).

Q) (U//~~FOUO~~) Whether the watch-list status of any subjects was appropriately documented.

R) (U//~~FOUO~~) For Preliminary Investigations, whether the status of the investigation is current (i.e., has not expired or will not expire before the next file review).

S) (U//~~FOUO~~) Whether any potential Intelligence Oversight Board (IOB) violations have been reported in accordance with policies.

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

U) (U//~~FOUO~~) For predicated investigations, whether the predication for continuing the investigation continues to exist.

V) (U//~~FOUO~~) For Assessments, whether it is reasonably likely that information relevant to the authorized purpose and clearly defined objectives will be obtained, thereby warranting continuing the Assessment for another 60/90 calendar days.

W) (U//~~FOUO~~) For Assessments, whether adequate predication has been developed to open a predicated investigation.

(U//~~FOUO~~) Supervisors must evaluate the proper use of investigative methods and ensure that they are adequately documented in the appropriate file. When evidence has been obtained, supervisors must ensure that the evidence was treated and/or disposed of appropriately. Supervisors should use the file review process as an opportunity to determine whether employees have adequately used liaison and external contacts to further their investigations/Assessments. In addition, supervisors must assess whether employees need

additional assistance, training, guidance, or resources to successfully advance their investigations/Assessments.

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

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

(U//~~FOUO~~) The supervisor must consider the employee's collateral duties (e.g., membership on the special weapons and tactics [SWAT] team, the evidence response team [ERT], the hazardous materials [HAZMAT] team, or the hostage negotiator team), training schedule, TDY assignments, and other activities constituting official business that could limit the employee's ability to address his or her assigned caseload. The supervisor must take into account planned annual and sick leave, holidays, and similar time constraints when estimating the employee's overall work responsibilities for the next 60/90-calendar-day period.

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

(U//~~FOUO~~) At the conclusion of the file review, the supervisor must ensure that the employee understands the objectives to be accomplished over the next 60/90 calendar days and must specifically document those expectations in the file review package.

(U) While conducting file reviews pursuant to this subsection, a supervisor must ensure that all investigative activities conducted online are in accordance with *DIOG Appendix L, Online Investigations*. Supervisors must pay special attention to information relating to the exercise of First Amendment rights. This type of information may only be collected if (1) the collection is logically related to an authorized investigative purpose, (2) the collection does not materially interfere with the ability of an individual or a group to engage in the exercise of constitutionally protected rights, and (3) the method of collection is the least intrusive alternative that is reasonable, based upon the circumstances of the investigation. The FBI must

not base investigative activities solely on an individual's legal exercise of his or her First Amendment rights. Further, every FBI employee has the responsibility to ensure that the activities of the FBI are "lawful, appropriate, and ethical, as well as effective in protecting the civil liberties and privacy of individuals in the United States." (See DIOG subsection 4.1.3.)

3.5.4.6 (U) TYPE 1 AND 2 ASSESSMENTS – JUSTIFICATION REVIEW REQUIREMENTS

(U//~~FOUO~~) Supervisors must conduct 30-calendar-day justification reviews for Type 1 & 2 Assessments. Following the end of the 30-calendar-day period, the agent, TFO, or IA and the supervisor have up to ten calendar days to complete all aspects of the justification review and to document the review. The justification review may be documented in Guardian or by using a Sentinel "Change Case Request." These justification reviews must address the following:

A) (U//~~FOUO~~) Has progress been made toward achieving the authorized purpose and clearly defined objective(s)?

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

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

D) (U//~~FOUO~~) Has adequate predication been developed to open a predicated investigation?

E) (U//~~FOUO~~) Should the Assessment be terminated?

3.5.4.7 (U) TYPE 5 ASSESSMENTS – FILE REVIEW REQUIREMENTS

(U//~~FOUO~~) b7E

A) (U

1. (U//~~FOUO~~

2. (U//~~FOUO~~

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

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

B) (U

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

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

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

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

3.5.4.8 (U) DOCUMENTATION OF FILE REVIEWS

(U//~~FOUO~~) File review packages are generated by Sentinel. These must be completed by an assigned case manager and the supervisor as part of the file review process. Once finalized, the completed packages can be viewed within Sentinel and used as a tool in determining an employee's performance rating. Documents maintained for evaluations, including printed copies of file review packages, must be maintained or destroyed in accordance with the FBI's performance appraisal system (see the *Performance and Development Program Policy Guide* [1129PG]). Upon completion of the file review, the electronic file review package must be submitted to field office executive management (e.g., an ASAC or an SSIA), who is responsible for ensuring that the file reviews were conducted properly by reviewing and signing the file review package. The Sentinel-generated file review package must be maintained for inspection review and other purposes not related to the performance appraisal process for a period of at least two years after being created or, if the material is related to a pending internal investigation, a performance action, a complaint, or a charge, the file review package must be maintained for one year from the date on which that case or action was closed, whichever is the longer period of time.

(U//~~FOUO~~) The Performance Management Tool is now accessible from the file review package in Sentinel. Employee performance notes are not required to be completed by the supervisor as part of the file review process. However, if the supervisor chooses to document performance notes, then the Performance Management Tool must be used. Using the Performance Management Tool in conjunction with the file review process can assist the supervisor and the employee in evaluating performance and providing developmental feedback.

3.5.4.9 (U) FILE REVIEW EXAMPLE

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

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

(U//~~FOUO~~) *Note*: While file reviews must be conducted every 90/60 calendar days respectively, the case manager and supervisor have 30 days following the 90- or 60-calendar-

day period to conduct the in person or telephonic meeting, complete the file review package in Sentinel, and complete any outstanding tasks. For example, if a file review identifies a missing LHM, FD-759, or accomplishment, those tasks should be completed during the 30-calendar-day period.

3.6 (U) CHIEF DIVISION COUNSEL (CDC) ROLES AND RESPONSIBILITIES

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

(U//~~FOUO~~) For investigative activities involving a SIM, the CDC must also independently consider the factors articulated in Section 10 and provide the approving authority with a recommendation as to whether, in the CDC's judgment, the investigative activity should be approved.

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

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

(U//~~FOUO~~) The mission of the FBI's Office of the General Counsel (OGC) is to provide comprehensive legal advice to the Director, other FBI officials and divisions, and field offices on a wide array of national security, investigative, and administrative operations. In addition to providing legal advice as requested, OGC reviews the legal sufficiency of sensitive Title III affidavits and a wide variety of operational documents relating to foreign counterintelligence/ international terrorism investigations, including requests for surveillance and physical searches pursuant to the Foreign Intelligence Surveillance Act (FISA) and undercover proposals, and

manages the physical flow of FISA requests, applications, orders, and returns. OGC maintains liaison with the intelligence community on legal issues and reviews for legal sufficiency proposals to share information or form partnerships with other federal, state, local, and international agencies. OGC also supports federal criminal prosecutions by assisting in criminal discovery and by conducting reviews of personnel files, coordinates the defense of the FBI and its employees in civil actions which arise out of the FBI's investigative mission and personnel matters, and assists the Office of Congressional Affairs (OCA) in responding to Congressional inquiries, including Congressional requests for FBI documents. OGC addresses legal issues associated with the impact of communication and information technology on the ability of the FBI and other law-enforcement and intelligence agencies to execute their public safety and national security missions, including their ability to conduct authorized electronic surveillance.

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

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

(U//~~FOUO~~) Throughout the DIOG, any requirement imposed on the General Counsel may be delegated and performed by a designated OGC attorney. All delegations must be made as set forth in Section 3.5.3 above.

3.8 (U) INTERNAL POLICY OFFICE (IPO) ROLES AND RESPONSIBILITIES

(U//~~FOUO~~) Subject to the guidance of the Deputy Director, the IPO has oversight of the implementation of the DIOG. Working with the Deputy Director's office, the IPO may make revisions to the DIOG as necessary, following appropriate coordination with the OIC, OGC and other FBIHQ or field office entities. In the process of implementing and analyzing the DIOG, the

IPO should report any apparent compliance risk areas directly to the OIC. Additionally, the IPO will work directly with the OIC to ensure that the policies, training, and monitoring are adequate to meet compliance monitoring procedures.

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

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

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

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

D) (U//~~FOUO~~) If the IPO makes any changes to the DIOG or other policy pursuant to 3.8.B and/or C above, the IPO will immediately advise by e-mail all FBIHQ Division Policy Officers (DPO) and field office policy officers (FPO) of such changes and all DPOs and FPOs must further advise their respective FBI employees of such changes. The electronic version of the DIOG maintained in the IPO's Policy Library is the official current policy of the FBI.

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

(U//~~FOUO~~) OIC is responsible for reviewing the DIOG and working with each FBIHQ division and the IPO to identify compliance risk areas and to ensure the adequacy of policy statements, training and monitoring. When compliance risk areas are identified, OIC must work with the divisions, field offices, and/or programs affected by the risk and develop programs to review the adequacy of policy statements, training, and monitoring in order to mitigate those concerns appropriately.

3.10 (U) Operational Program Manager Roles and Responsibilities

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

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

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

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

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

D) (U//~~FOUO~~) Policy conflict;

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

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

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

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

3.11 (U) Division Compliance Officer Roles and Responsibilities

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

This Page is Intentionally Blank.

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

4.1 (U) CIVIL LIBERTIES AND PRIVACY

4.1.1 *(U) OVERVIEW*

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

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

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

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

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

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

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

4.1.2 *(U) PURPOSE OF INVESTIGATIVE ACTIVITY*

(U) One of the most important safeguards in the AGG-Dom—one that is intended to ensure that FBI employees respect the constitutional rights of Americans—is the threshold requirement that all investigative activities be conducted for an authorized purpose. Under the AGG-Dom that

authorized purpose must be an authorized national security, criminal, or foreign intelligence collection purpose.

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

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

4.1.3 *(U) OVERSIGHT AND SELF-REGULATION*

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

A) (U) Required notification by the FBI to the DOJ NSD concerning a Full Investigation that involves foreign intelligence collection, a Full Investigation of a United States person (USPER) in relation to a threat to the national security, or a national security investigation involving a "sensitive investigative matter" (SIM) (see DIOG Section 10).

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

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

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

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

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

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

B) (U) The Whistleblower Protection Acts of 1989 and 1998, and the Whistleblower Protection Enhancement Act of 2016. These laws protect whistleblowers from retaliation.

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

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

E) (U) Documents describing First Amendment rights that are subsequently determined to have been collected or retained in violation of the Privacy Act must be destroyed as set forth in *Handling of Privacy Act Records Maintained in Violation of the Privacy Act's Provision Concerning First Amendment Activity Policy Directive* (1270D).

(U) Congress, acting primarily through the Judiciary and Intelligence Committees, exercises regular, vigorous oversight into all aspects of the FBI's operations. To this end, the National Security Act of 1947 requires the FBI to keep the intelligence committees (for the Senate and House of Representatives) fully and currently informed of substantial intelligence activities. This oversight has significantly increased in breadth and intensity since the 1970's, and it provides important additional assurance that the FBI conducts its investigations according to the law and the Constitution. Guidance on what activities fall within the scope of required congressional notification can be obtained from OCA. See the *Congressional Affairs Policy Guide* (1288PG).

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

(U) Internal FBI safeguards include:

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

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

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

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

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

4.2 (U) PROTECTION OF FIRST AMENDMENT RIGHTS

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

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

(U) The First Amendment states:

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

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

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

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

(U) As fully defined elsewhere in this policy, a "sensitive investigative matter" is one that involves certain activities of a domestic public official or domestic political candidate, a religious or domestic political organization (or an individual prominent in such an organization), or the news media; activities with an academic nexus; or any other matter meriting the attention of FBIHQ and other DOJ officials in the judgment of the authorizing official. (See DIOG Section

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

(U) Furthermore, FBI employees should be particularly mindful that, in addition to the opening of an investigation, the use of certain investigative methods involving these sensitivities often require additional scrutiny, approvals, or procedures. For instance, the use of compulsory process, the issuance of a National Security Letter, or the search of FBI holdings in certain circumstances (such as those involving the activities of members of Congress or the news media) may implicate traditionally sensitive conduct requiring additional approvals. These additional approvals may be required whether or not the underlying investigation itself was opened as a sensitive investigative matter.

(U) Additional approvals required may include approval from the Attorney General, the Deputy Attorney General, the Director, or the Deputy Director, with review by the Office of the General Counsel. It is essential that FBI employees recognize when investigative activity may involve or implicate a sensitive investigative matter or First Amendment sensitivities and seek and obtain the necessary approvals. (See DIOG Section 10.)

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

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

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

4.2.1 *(U) FREE SPEECH*

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

(U) It is important to understand the line between constitutionally protected speech and advocacy of violence or of conduct that may lead to violence or other unlawful activity. In *Brandenburg v. Ohio, 395 U.S. 444 (1969)*, the Supreme Court established a two-part test to determine whether such speech is constitutionally protected: the government may not prohibit advocacy of force or violence except when such advocacy (i) is intended to incite imminent lawless action, and (ii) is likely to do so. Therefore, even heated rhetoric or offensive provocation that could conceivably lead to a violent response in the future is usually protected. Suppose, for example, a politically active group advocates on its web site taking unspecified "action" against persons or entities it views as the enemy, who thereafter suffer property damage and/or personal injury. Under the *Brandenburg* two-part test, the missing specificity and imminence in the message may provide it constitutional protection. For that reason, law enforcement may take no action that, in effect, blocks the message or punishes its sponsors.

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

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

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

4.2.2 *(U) EXERCISE OF RELIGION*

(U) Like the other First Amendment freedoms, the "free exercise of religion" clause is broader than commonly believed. First, it covers any form of worship of a deity—even forms that are commonly understood to be cults or fringe sects, as well as the right not to worship any deity. Second, protected religious exercise also extends to dress or food that is required by religious edict, attendance at a facility used for religious practice (no matter how unlikely it appears to be intended for that purpose), observance of the Sabbath, raising money for evangelical or missionary purposes, and proselytizing. Even in controlled environments like prisons, religious exercise must be permitted—subject to reasonable restrictions as to time, place, and manner. Another feature of this First Amendment right is that religion is a matter of heightened sensitivity to some Americans—especially to devout followers. For this reason, religion is a matter that is likely to provoke an adverse reaction if the right is violated—regardless of which religion is involved. Therefore, when essential investigative activity may impact this right, the investigative activity must be conducted in a manner that avoids the actual—and the appearance of—interference with religious practice to the maximum extent possible.

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

(U) Furthermore, FBI employees may take appropriate cognizance of the role religion may play in the membership or motivation of a criminal or terrorism enterprise. If, for example, affiliation with a certain religious institution or a specific religious sect is a known requirement for inclusion in a violent organization that is the subject of an investigation, then whether a person of interest is a member of that institution or sect is a rational and permissible consideration. Similarly, if investigative experience and reliable intelligence reveal that members of a terrorist or criminal organization are known to commonly possess or exhibit a combination of religion-based characteristics or practices (e.g., group leaders state that acts of terrorism are based in religious doctrine), it is rational and lawful to consider such a combination in gathering intelligence about the group—even if any one of these, by itself, would constitute an impermissible consideration. By contrast, solely because prior subjects of an investigation of a particular group were members of a certain religion and they claimed a religious motivation for their acts of crime or terrorism, other members' mere affiliation with that religion, by itself, is

not a basis to assess or investigate—absent a known and direct connection to the threat under Assessment or investigation. Finally, the absence of a particular religious affiliation can be used to eliminate certain individuals from further investigative consideration in those scenarios where religious affiliation is relevant.

4.2.3 *(U) FREEDOM OF THE PRESS*[9]

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

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

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

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

A) (U) Is appropriately authorized;

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

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

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

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

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

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

(U) The right to petition the government for redress of grievances is so linked to peaceful assembly and association that it is included in this discussion. A distinction between the two is that an individual may exercise the right to petition the government by himself whereas assembly necessarily involves others. The right to petition the government includes writing letters to Congress, carrying a placard outside city hall that delivers a political message, recruiting others to one's cause, and lobbying Congress or an executive agency for a particular result.

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

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

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

A) (U) Undercover participation in group activities:

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

C) (U) Properly authorized electronic surveillance;

D) (U) Recruitment and operation of sources;

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

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

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

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

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

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

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

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

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

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

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

4.3 (U) EQUAL PROTECTION UNDER THE LAW

4.3.1 *(U) INTRODUCTION*

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

(U) Specifically, federal government employees are prohibited from engaging in invidious discrimination against individuals on the basis of race, ethnicity, gender, national origin, religion, disability, sexual orientation, or gender identity. This principle is further reflected and implemented for federal law enforcement in the United States Department of Justice's *Guidance for Federal Law Enforcement Agencies Regarding the Use of Race, Ethnicity, Gender, National Origin, Religion, Sexual Orientation, or Gender Identity* (May 2023) (hereinafter "DOJ's 2023 Guidance on Use of Race, etc.") and the Department of Justice's *Guidance on Interactions with Members of the Public with Disabilities in Traditional Law Enforcement Program Activities*.

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

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

4.3.2 *(U) POLICY PRINCIPLES*

(U) In May 2023, the Department of Justice issued the DOJ's 2023 Guidance on Use of Race, etc. which superseded the Department's 2014 "Guidance Regarding the Use of Race by Federal Law Enforcement Agencies."

(U) The DOJ's 2023 Guidance applies to Federal law enforcement officers performing Federal law enforcement activities, including those related to national security and intelligence, and defines not only the circumstances in which Federal law enforcement officers may take into account a person's race and ethnicity but also when gender, national origin, religion, sexual orientation, or gender identity may be taken into account. This Guidance also applies to state and local law enforcement officers while participating in Federal law enforcement task forces.

(U) The DOJ's 2023 Guidance on Use of Race, etc. provides two standards in combination which will guide Federal law enforcement and task force officers in the appropriate use of race, ethnicity, gender, national origin, religion, sexual orientation, or gender identity in law enforcement or intelligence activities:

A) (U) In making routine or spontaneous law enforcement decisions, such as ordinary traffic stops, Federal law enforcement or task force officers may not use race, ethnicity, gender, national origin, religion, sexual orientation, or gender identity to any degree, except that

officers may rely on the listed characteristics in a specific suspect description. This prohibition applies even where the use of a listed characteristic might otherwise be lawful.

B) (U) In conducting all activities other than routine or spontaneous law enforcement activities, Federal law enforcement or task force officers may consider race, ethnicity, gender, national origin, religion, sexual orientation, or gender identity only to the extent that there is trustworthy information, relevant to the locality or time frame, that links persons possessing a particular listed characteristic to an identified criminal incident, scheme, or organization, a threat to national or homeland security, a violation of Federal immigration law, or an authorized intelligence activity. In order to rely on a listed characteristic, federal law enforcement or task force officers must also reasonably believe that the law enforcement, security, or intelligence activity to be undertaken is merited under the totality of the circumstances, such as any temporal exigency and the nature of any potential harm to be averted. This standard applies even where the use of a listed characteristic might otherwise be lawful.

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

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

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

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

(U) On January 6, 2017, the Department of Justice (DOJ) issued the Department of Justice's *Guidance on Interactions with Members of the Public with Disabilities in Traditional Law Enforcement Programs and Activities*. Agents must not unlawfully discriminate against any person with a disability and must treat persons with disabilities with professionalism and respect. DOJ is responsible, under Executive Order 12250, for coordinating implementation of Section 504 of the Rehabilitation Act of 1973 with respect to both federally assisted and federally

conducted programs and activities. As the DOJ's guidance reiterated, it is important that FBI's programs and activities be a model of compliance.

4.3.3 *(U) Guidance on the Use of Race, Ethnicity, Gender, National Origin, Religion, Sexual Orientation, or Gender Identity in Assessments and Predicated Investigations*

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

4.3.3.1 (U) Individual Race, Ethnicity, Gender, National Origin, Religion, Sexual Orientation, or Gender Identity as a Factor

(U) The *DOJ's 2023 Guidance on Use of Race, etc.* permits the consideration of race, ethnicity, gender, national origin, religion, sexual orientation, or gender identity information based on specific reporting—such as from an eyewitness. As a general rule, race, ethnicity, gender, national origin, religion, sexual orientation, or gender identity as an identifying feature of a suspected perpetrator, subject, and in some cases, a victim, is relevant if it is based on reliable evidence or information—not conjecture or stereotyped assumptions. In addition, the DOJ's 2023 Guidance on Use of Race, etc. permits consideration of such personal characteristics in other investigative or collection scenarios if it is relevant to an identified criminal incident, scheme, or organization. These examples illustrate:

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

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

4.3.3.2 (U) Community Race, Ethnicity, Gender, National Origin, Religion, Sexual Orientation, or Gender Identity as a Factor

4.3.3.2.1 *(U) Collecting and Analyzing Demographics*

(U) The and FBI policy permit the FBI to identify locations of concentrated ethnic communities in the field office's domain, if these locations will reasonably aid the analysis of potential threats and vulnerabilities to national and homeland security or an authorized intelligence activity, e.g., assist domain awareness for the purpose of performing intelligence analysis. If, for example, intelligence reporting reveals that members of certain terrorist organizations live and operate primarily within a certain concentrated community of the same ethnicity, the location of that community is clearly valuable—and properly collectible—data.

Similarly, the locations of ethnic-oriented businesses and other facilities may be collected if their locations will reasonably contribute to an awareness of potential threats and vulnerabilities, and intelligence collection opportunities. Also, members of some communities may be potential victims of civil rights crimes and, for this reason, community location may aid enforcement of civil rights laws. Information about such communities should not be collected, however, unless the communities are sufficiently concentrated and established so as to provide a reasonable potential for intelligence collection that would support FBI mission programs (e.g., where identified terrorist subjects from certain countries may relocate to blend in and avoid detection).

4.3.3.2.2 *(U) GEO-MAPPING ETHNIC/RACIAL DEMOGRAPHICS*

(U) As a general rule, if information about community demographics may be collected, it may be "mapped." Sophisticated computer geo-mapping technology visually depicts lawfully collected information and can assist in showing relationships among disparate data. By itself, mapping raises no separate concerns about racial or ethnic profiling, assuming the underlying information that is mapped was properly collected. It may be used broadly - e.g., for domain awareness of all relevant demographics in the field office's area of responsibility or to track crime trends – or narrowly to identify specific communities or areas of interest to inform a specific Assessment or investigation. In each case, the relevance of the ethnic or racial information mapped to the authorized purpose of the Assessment or investigation must be clearly demonstrated and documented.

4.3.3.2.3 *(U) GENERAL ETHNIC/RACIAL BEHAVIOR*

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

4.3.3.2.4 *(U) SPECIFIC AND RELEVANT ETHNIC BEHAVIOR*

(U) On the other hand, knowing the behavioral and life style characteristics of known individuals who are criminals or who pose a threat to national security may logically aid in the detection and prevention of crime and threats to the national security within the community and beyond. Focused behavioral characteristics reasonably believed to be associated with a particular criminal or terrorist element of an ethnic community (not with the community as a whole) may be collected and retained. For example, if it is known through intelligence analysis or otherwise that individuals associated with an ethnic-based terrorist or criminal group conduct their finances by certain methods, travel in a certain manner, work in certain jobs, or come from a certain part of their home country that has established links to terrorism, those are relevant factors to consider when investigating the group or assessing whether it may have a presence within a community. It is recognized that the "fit" between specific behavioral characteristics and a terrorist or criminal group is unlikely to be perfect—

that is, there will be members of the group who do not exhibit the behavioral criteria as well as persons who exhibit the behaviors who are not members of the group. Nevertheless, in order to maximize FBI mission relevance and to minimize the appearance of racial or ethnic profiling, the criteria used to identify members of the group within the larger ethnic community to which they belong must be as focused and as narrow as intelligence reporting and other circumstances permit. If intelligence reporting is insufficiently exact so that it is reasonable to believe that the criteria will include an unreasonable number of people who are not involved, then it would be inappropriate to use the behaviors, standing alone, as the basis for FBI activity.

4.3.3.2.5 *(U) EXPLOITIVE ETHNIC BEHAVIOR*

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

4.4 (U) LEAST INTRUSIVE METHOD

4.4.1 *(U) OVERVIEW*

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

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

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

4.4.2 *(U) General Approach to Least Intrusive Method Concept*

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

A) (U) Gather information that is relevant to the Assessment or predicated investigation;

B) (U) Acquire the information within the time frame required by the Assessment or predicated investigation;

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

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

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

4.4.3 *(U) Determining Intrusiveness*

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

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

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

B) (U) ***Scope of the information sought:*** Collecting information regarding an isolated event—such as a certain phone number called on a specific date or a single financial transaction—is less intrusive or invasive of an individual's privacy than collecting a complete communications or financial "profile." Similarly, a complete credit history is a more intrusive view into an individual's life than a few isolated credit charges. In some cases, of course, a complete financial and credit profile is exactly what the investigation requires (for example, investigations of terrorist financing or money laundering). If so, FBI employees should not hesitate to use appropriate legal process to obtain such information if the predicate requirements are satisfied. Operational security—such as source protection—may also dictate seeking a wider scope of information than is absolutely necessary for the purpose of protecting

a specific target or source. When doing so, however, the concept of least intrusive method still applies. The FBI may obtain more data than strictly needed, but it should obtain no more data than is needed to accomplish the investigative or operational security purpose.

C) (U) ***Scope of the use of the method:*** Using a method in a manner that captures a greater picture of an individual's or a group's activities are more intrusive than using the same method or a different one that is focused in time and location to a specific objective. For example, it is less intrusive to use a tracking device to verify point-to-point travel than it is to use the same device to track an individual's movements over a sustained period of time. Sustained tracking on public highways would be just as lawful but more intrusive because it captures a greater portion of an individual's daily movements. Similarly, surveillance by closed circuit television that checks a discrete location within a discrete time frame is less intrusive than 24/7 coverage of a wider area. For another example, a computer intrusion device that captures only host computer identification information is far less intrusive than one that captures file content.

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

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

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

4.4.4 *(U) STANDARD FOR BALANCING INTRUSION AND INVESTIGATIVE REQUIREMENTS*

(U) Once an appropriate method and its deployment have been determined, reviewing and approving authorities should balance the level of intrusion against investigative requirements. This balancing test is particularly important when the information sought involves clearly established constitutional, statutory, or evidentiary rights or sensitive circumstances (such as obtaining information from religious or academic institutions or public fora where First Amendment rights are being exercised), but should be applied in all circumstances to ensure that the least intrusive method if reasonable based upon the circumstances of the investigation is being utilized.

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

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

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

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

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

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

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

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

(U) Another consideration to be balanced is operational security: if a less intrusive but reasonable method were selected, would the subject detect its use and alter his activities—including his means of communication—to thwart the success of the operation? Operational

security—particularly in national security investigations—should not be undervalued and may, by itself, justify covert tactics which, under other circumstances, would not be the least intrusive.

4.4.5 *(U) CONCLUSION*

(U) The foregoing guidance is offered to assist FBI employees in navigating the often unclear course to select the least intrusive investigative method that effectively accomplishes the operational objective at hand. In the final analysis, choosing the method that most appropriately balances the impact on privacy and civil liberties with operational needs, is a matter of judgment, based on training and experience. Pursuant to the AGG-Dom, other applicable laws and policies, and this guidance, FBI employees may use any lawful method allowed, even if intrusive, where the intrusiveness is warranted by the threat to the national security or to potential victims of crime and/or the strength of the information indicating the existence of that threat.

5 (U) ASSESSMENTS

5.1 (U) ASSESSMENT PURPOSE AND SCOPE

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

(U) More broadly, detecting and interrupting criminal activities at their early stages, and preventing crimes from occurring in the first place, is preferable to allowing criminal plots to come to fruition. Hence, Assessments may also be undertaken proactively with such purposes as detecting criminal activities; obtaining information on individuals, groups, or organizations of possible investigative interest, either because they may be involved in criminal or national security-threatening activities or because they may be targeted for attack or victimization in such activities; [redacted] b7E

(U//~~FOUO~~) *Note:* In the DIOG, the word "assessment" has two distinct meanings. The *AGG-Dom* authorizes as an investigative activity an "Assessment," which requires an authorized purpose, as discussed in this section of the DIOG. The US Intelligence Community (USIC), however, also uses the word "assessment" to describe written intelligence products, as discussed in DIOG subsections 15.2.3 and 15.6.1.2.

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

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

sought and the proposed means to obtain that information on the other. An FBI employee must be able to explain the authorized purpose and the clearly defined objective(s) and the reason the particular investigative methods were used to conduct the Assessment. FBI employees who conduct Assessments are responsible for ensuring that Assessments are not pursued for frivolous or improper purposes and are not based solely on First Amendment rights or on the race, ethnicity, gender, national origin, religion, disability, sexual orientation, or gender identity of the subject of the Assessment, or a combination of only such factors (*AGG-Dom*, Part II).

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

5.1.1 *(U) SITUATIONAL EXAMPLES*

(U) The following examples offer fact patterns similar to those that FBI employees may encounter. In some examples, the response to the scenario demonstrates the delicate balance between pursuing legitimate investigative goals without infringing upon the exercise of constitutionally protected activities. These examples are not exhaustive and may not be illustrative of all applicable factors. FBI employees who are unsure if an Assessment can be opened or if an Assessment could implicate privacy or civil liberties concerns must seek guidance from a supervisor, chief division counsel (CDC), associate division counsel (ADC), or the Office of the General Counsel (OGC).

5.1.1.1 (U) EXAMPLE A

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

b7E

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

5.1.1.2 **(U) EXAMPLE B**

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

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

5.1.1.3 **(U) EXAMPLE C**

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

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

5.1.1.4 **(U) EXAMPLE D**

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

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

(U//~~FOUO~~)

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

5.1.1.1 (U) EXAMPLE E

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

b7E

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

5.1.1.2 (U) EXAMPLE F

b7E

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

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

5.1.1.3 (U) EXAMPLE G

b7E

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

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

5.2 (U) CIVIL LIBERTIES AND PRIVACY

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

(U) Even when an authorized purpose is present, an Assessment could create the appearance that it is directed at or activated by constitutionally protected activity, race, ethnicity, gender, national origin, religion, disability, sexual orientation, or gender identity—particularly under

circumstances where the link to an authorized FBI mission is not readily apparent. In these situations, it is vitally important that the authorized purpose and the clearly defined objective(s), as well as the use of any investigative methods, are well documented.

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

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

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

(U) By emphasizing the use of the least intrusive means to obtain information, intelligence, or evidence, FBI employees can effectively execute their duties while mitigating the potential negative impact on the privacy and civil liberties and the damage to the reputation of all people encompassed within the investigation or Assessment, including targets, witnesses, and victims. This principle is not intended to discourage FBI employees from seeking relevant and necessary intelligence, information, or evidence, but rather is intended to encourage FBI employees to choose the least intrusive—but still reasonable based upon the circumstances of the investigation—means from the available options to obtain the information (*AGG-Dom*, Part I.C.2).

5.3 (U) COMPLAINT PROCESSING

5.3.1 *(U) OVERVIEW*

(U//~~FOUO~~) The purpose of this subsection is to provide clarity on investigative activities that are permitted prior to opening an Assessment or a predicated investigation. (See DIOG Sections 6 & 7.)[10]

[10] (U//~~FOUO~~) In some circumstances, Guardian incidents may also lead to the opening of an enterprise investigation (see DIOG Section 8) or a positive foreign intelligence investigation (see DIOG Section 9).

(U//~~FOUO~~) The *AGG-Dom* combines the concept of evaluating national security threats with that of conducting prompt and extremely limited checking of leads, and refers to this as an "Assessment." Under the *AGG-Dom*, all the investigative activity described in DIOG Section 5 requires an authorized purpose.

(U//~~FOUO~~) The basis for processing a complaint, tip, observation, or information (hereafter referred to generally as "complaints" or "complaint processing"), including the use of the permitted investigative methods, cannot be arbitrary or groundless speculation. Additionally, the rationale for processing a complaint cannot be based solely on the exercise of First Amendment protected activities or on the race, ethnicity, gender, national origin, religion, disability, sexual orientation, or gender identity of the subject or a combination of only these factors.

(U//~~FOUO~~) Complaints are managed using the Guardian application (e.g., information either imported from eGuardian[11] or natively entered into Guardian by an employee). These are known as "Guardian incidents," and are processed by FBI employees to expeditiously determine if the information provides justification to open an Assessment or sufficient predication to open a predicated investigation. This complaint processing activity spans the drafting of the Guardian incident through serialization of a completed Guardian incident into Sentinel.[12]

(U//~~FOUO~~) Processing complaints related to potential or ongoing criminal activity or threats to national security, using "relatively non-intrusive" investigative methods, enables the FBI to avoid the need to proceed to more formal levels of investigative activity, if the results indicate that further action is not warranted. (*AGG-Dom*, Part II and Part IIA). To assist in evaluating this incoming information, FBI employees are authorized to use specific limited investigative methods, as detailed in DIOG subsection 5.3.9.

(U//~~FOUO~~) With the benefit of these methods, an FBI employee may be able to answer the following question when evaluating the complaint: does the complaint appear to represent a credible basis to open an Assessment, with an authorized purpose and clearly defined objective(s), or to open a predicated investigation consistent with the standards set forth in the DIOG?

(U//~~FOUO~~) Upon receipt of the complaint, or while engaged in complaint processing activity, if the information collected or obtained meets the standard for opening an Assessment or a predicated investigation, and the employee intends to continue pursuing the matter, an Assessment or a predicated investigation should be opened and assigned. Any records obtained must be treated in accordance with DIOG subsection 5.3.8.

5.3.2 *(U) COMPLAINT PROCESSING CATEGORIES*

(U//~~FOUO~~) There are three categories of precedence for complaint processing, which apply regardless of investigative program:

[11] (U) Some Guardian incidents are entered into the "eGuardian" system, which then creates a Guardian incident.
[12] (U//~~FOUO~~) A supervisor reviews the draft Guardian incident submitted by an employee and determines its disposition or next investigative steps, if warranted.

A) (U//~~FOUO~~) **Threat to Life (TTL) processing:** processing that includes a credible threat of harm or violence that could reasonably result in death or serious bodily injury. (See DIOG subsection 5.3.3.1 for additional information.)

B) (U//~~FOUO~~) **Time Sensitive processing:** processing involving an imminent or ongoing threat of (1) sexual abuse, physical abuse, or exploitation of a child or (2) abuse against the elderly and otherwise vulnerable individuals. (See also DIOG subsection 5.3.3.2 for additional information and definitions for time sensitive processing.)

C) (U//~~FOUO~~) **Routine processing:** processing that does not meet the criteria outlined in category A or B.

5.3.3 *(U) INTAKE OF COMPLAINTS*

(U//~~FOUO~~) The FBI regularly receives complaints with potential investigative value through a variety of methods, including the National Threat Operations Center (NTOC), "walk-ins" to FOs, contact with the public, field observations of suspicious activity, and referrals from other government agencies (OGA). This information is documented as a draft Guardian incident.

(U//~~FOUO~~) When employees undertake investigative activities authorized prior to opening an Assessment or predicated investigation, they must have a reason that is tied to an authorized FBI criminal or national security purpose to undertake these activities. If, while engaged in such activities, the information collected or obtained meets the standard for opening an Assessment or a predicated investigation, and the employee intends to continue pursuing the matter, an Assessment or a predicated investigation must be opened, and any records obtained must be treated in accordance with DIOG subsection 5.12.

5.3.3.1 (U) THREAT TO LIFE COMPLAINTS

(U//~~FOUO~~) The FBI regularly receives a broad array of complaints regarding acts of violence. **Within the context of the DIOG, a "threat to life" means a credible threat of harm or violence that could reasonably result in death or serious bodily injury.** Pursuant to DIOG subsection 14.7, the FBI has a responsibility to notify persons of credible threats to their life or threats that may result in serious bodily injury.

(U//~~FOUO~~) Whenever sufficient information is received to process a Guardian incident as a TTL, the receiving employee must take immediate action to mitigate the threat to protect life or public safety. The initial focus must be on conducting relevant investigative steps to corroborate and mitigate threat activity and notifying appropriate supervisors and response teams. Administrative reporting and documentation requirements, as set out in this subsection can be held in abeyance while the active threat mitigation steps are undertaken.

(U//~~FOUO~~) Each FO must have at least one **TTL Guardian designee**[13] appointed by the FO head. This designee is responsible for overseeing the FO's responses to and adjudications of TTL Guardian incidents. The TTL Guardian designee(s) may be [redacted] b7E

[redacted]

[13] (U) [redacted]

b7E

5.3.3.2 (U) TIME SENSITIVE COMPLAINTS

(U//~~FOUO~~) The FBI regularly receives information involving imminent or ongoing (1) sexual or physical abuse of a child, or (2) abuse of the elderly or an otherwise vulnerable individual. The latter is defined as the willful affliction of physical or psychological harm to an elderly or otherwise vulnerable individual. Within the context of this subsection, "imminent or ongoing" means that, based on all available information, and in the FBI employee's professional judgement, a reasonable likelihood exists that a child, the elderly, or otherwise vulnerable individual will be physically victimized. Time Sensitive Guardian incidents must be addressed as an immediate priority.

(U//~~FOUO~~) Whenever sufficient information exists involving a Time Sensitive Guardian incident, FBI employees must take immediate action to prevent injury to a victim. Effective law enforcement action to mitigate a threat should never be delayed solely to comply with administrative requirements contained in DIOG subsection 5.3.

(U//~~FOUO~~) Whenever Time Sensitive Guardian incidents fall outside of the FBI's primary investigative jurisdiction, FBI employees must promptly disseminate the information to other law enforcement agencies, in accordance with DIOG subsection 14.4.2. For policy on reporting suspected child abuse, refer to DIOG subsection 14.8 (new). For policy on reporting suspected abuse of the elderly or otherwise vulnerable individuals, refer to DIOG subsection 14.9 (new).

5.3.3.3 (U) ROUTINE COMPLAINTS

(U//~~FOUO~~) The FBI regularly receives complaints with potential investigative value through a variety of methods, including NTOC, walk-ins to FOs, contact with the public, field observations of suspicious activity, and referrals from OGAs. Typically, the complaints involve information on potential or ongoing criminal activity or national security threats. These complaints are documented as draft routine Guardian incidents.

(U//~~FOUO~~) Routine complaints do not involve TTL or Time Sensitive information.

5.3.4 *(U) COMPLAINTS PROCESSED BY THE NATIONAL THREAT OPERATIONS CENTER*

(U//~~FOUO~~) NTOC personnel (including threat intake examiners [TIE] and SSAs) receive complaints from the public through telephone and online intake methods prior to routing the complaint for further evaluation. NTOC personnel must determine if there is an authorized purpose that warrants investigative activity (see DIOG subsection 5.1) before using any investigative methods (see DIOG subsection 5.3.9). Using established standard operating procedures and methodology that must adhere to DIOG standards and requirements, NTOC personnel log tips and complaints into an NTOC-specific workflow that feeds into the Guardian application.

(U//~~FOUO~~) In accordance with its internal procedures and workflow, routine Guardian incidents are documented and reviewed by NTOC supervisors, then routed to the appropriate FO for further evaluation and action, as deemed appropriate.

5.3.4.1 (U//~~FOUO~~) NTOC PROCESSING OF TTL AND TIME SENSITIVE COMPLAINTS AND TIPS

(U//~~FOUO~~) As soon as possible, NTOC personnel must telephonically contact the applicable FO's operations center to notify them of the inbound processing of a complaint and provide an oral synopsis of the TTL or Time Sensitive incident, including the rationale for elevating the incident reporting. Then, NTOC personnel must document in the Guardian incident:

1) (U)
2) (U)
3) (U)

b7E

(U//~~FOUO~~) After routing the Guardian incident to the FO, NTOC personnel must also send an email to the FO's operations center (via the unclassified network [UNet]) with the specific TTL or Time Sensitive information (to the extent possible in an unclassified manner). Refer to the *Records and Information Management Policy Guide* (1223PG) regarding the requirement to import nontransitory record emails into a record keeping system (i.e., Sentinel) within 20 calendar days after the original creation or transmission date.

5.3.5 *(U) COMPLAINTS PROCESSED BY FIELD OFFICES*[14]

(U//~~FOUO~~) FO employees may receive complaints with potential investigative value by various means (e.g., walk-in complaints, phone calls, CHS reporting, referral from an OGA, or contact with citizens in public settings) and may be assigned a Guardian incident for processing by a supervisor. Regardless of the source, upon receipt, an FBI employee assesses the information to determine if there is an authorized purpose that warrants investigative activity. If the information provided in the complaint meets the standard for opening a predicated investigation (e.g., PI or Full investigation), the employee may do so in accordance with the standards set out in DIOG Sections 6–9, as applicable.

(U//~~FOUO~~) If an authorized purpose exists, but information received is not sufficient to open an Assessment or predicated investigation, the employee must determine whether use of any permitted investigative methods will assist in evaluating the complaint. (See DIOG subsection 5.3.6.1.) Supervisory approval is not required to draft a Guardian incident and submit it to a supervisor for evaluation and whatever action is deemed appropriate.

[14] (U//~~FOUO~~) The FO intake and processing differs slightly from NTOC to account for field-related activities such as information provided by the public while engaged in other investigative activities, or the observation of suspicious activity by an agent while on duty.

5.3.5.1 (U//~~FOUO~~) FIELD OFFICE TIME FRAME FOR COMPLETING AND SUBMITTING A GUARDIAN INCIDENT

(U//~~FOUO~~) Upon determining there is an authorized purpose that warrants investigative activity, the receiving employee must act on the information, in accordance with the following standards, based upon the category of precedence:

A. (U//~~FOUO~~) **TTL and Time Sensitive processing:** Upon receipt of information, a FO employee must immediately [redacted] draft a Guardian incident within the relevant investigative program, must orally notify the FO operations center about the Guardian incident, and must submit the Guardian incident to a relevant supervisor.

B. (U//~~FOUO~~) **Routine processing:** A FO employee must complete drafting the Guardian incident involving criminal, cyber, or counterintelligence matters no more than [redacted] **days** from receiving the complaint with potential investigative value, and submit the form to the supervisor for evaluation and assignment, as appropriate. For a Guardian incident involving counterterrorism or WMDD matters, the employee must complete drafting the Guardian incident no more than [redacted] from receiving a complaint with potential investigative value, and submit the form to the supervisor for evaluation and assignment, as appropriate.[15] b7E

(U//~~FOUO~~) See DIOG subsection 5.3.5.2 for the employee time frame for processing the Guardian incident whenever the employee is assigned the Guardian incident by a supervisor (i.e., the Guardian incident has already been drafted and submitted to the supervisor for evaluation and assignment, and it has been assigned to an employee).

5.3.5.2 (U) FIELD OFFICE TIME FRAME FOR PROCESSING A GUARDIAN INCIDENT

(U//~~FOUO~~) The applicable time frame and procedures for processing a supervisory assigned Guardian incident in a FO are determined by the investigative program and category of precedence, as described below:

A. (U//~~FOUO~~) **TTL and Time Sensitive processing:** All investigative programs must adhere to the following:

- (U//~~FOUO~~) The assigned employee is required to immediately commence the activities described in DIOG subsection 5.3.9, (an employee taking and documenting the initial complaint may also perform this activity for timeliness purposes), and conduct any other appropriate investigative action. At a minimum, the assigned employee must complete the database checks described in DIOG subsection 5.3.10 no more than [redacted] after being assigned the Guardian incident for processing. b7E
- (U//~~FOUO~~) If an initial processing is not "converted" into an Assessment or predicated investigation (see DIOG subsection 5.3.6.2) or closed as "Information Only" (see DIOG subsection 5.3.6.3) no more than [redacted] after it is assigned, an SSA must review the assigned employee's progress and determine a disposition. This review must

[15] (U) See also the [redacted] b7E

be repeated every five business days thereafter until the initial processing is "converted" or closed.

B. (U//~~FOUO~~) **Routine processing:** For criminal, cyber, and counterintelligence related complaints, the assigned employee is required to complete the complaint processing activities described in DIOG subsection 5.3.10 no more than [redacted] from being assigned the Guardian incident for processing, unless an extension is granted. Refer to DIOG subsection 5.3.7 for extensions beyond [redacted] For counterterrorism and WMDD related complaints, an assigned employee is required to begin the complaint processing activities described in DIOG subsection 5.3.9 no more than [redacted] from being assigned the Guardian incident for processing.[16] b7E

5.3.6 *(U) SUPERVISORY EVALUATION OF A COMPLAINT OR GUARDIAN INCIDENT*

(U//~~FOUO~~) Regardless of how the complaint is initiated, a FO supervisor (or designee) (e.g., Guardian coordinator or co-coordinator per DIOG subsection 5.3.3.1) must review the Guardian incident, and determine if the complaint has an authorized purpose and warrants further investigative steps or not. Based upon this determination, the supervisor may choose an option to:

- (U) Assign to an FBI employee for processing. (See DIOG subsection 5.3.6.1.) An authorized purpose must exist whenever using investigative methods permitted prior to opening an Assessment (See DIOG subsection 5.3.9.)
- (U) Convert the Guardian incident to an Assessment or predicated investigation. (See DIOG subsection 5.3.6.2.)
- (U) Close–by referring to OGA partners for further action (see DIOG subsection 5.3.6.3).
- (U) Close–if no investigative activity is warranted at this time (see DIOG subsection 5.3.6.4).
- (U) Close–The information received is solely based on activities that are protected by the First Amendment or on race, ethnicity, gender, national origin, religion, disability, sexual orientation, or gender identity of the subject, or a combination of only such factors (see DIOG subsection 5.3.6.5.).

(U//~~FOUO~~) See DIOG subsection 5.3.6.6 for additional guidance on closing Guardian incidents.

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

5.3.6.1 (U) OPTION 1: ASSIGN THE COMPLAINT OR GUARDIAN INCIDENT FOR PROCESSING

(U//F~~OUO~~) Based upon the intake method and substance of the complaint information, permitted investigative methods may, or may not, have been undertaken by the employee who drafted the submitted Guardian incident. Based upon this circumstance, and evaluation of the complaint information[17], a supervisor must assign an employee to conduct the complaint processing activities described in DIOG subsection 5.3.9.

(U//~~FOUO~~) After completing the processing, the assigned FBI employee must submit the results to the supervisor (or Guardian designee per DIOG subsection 5.3.3.1) with a recommendation to either convert to an Assessment or predicated investigation or close the Guardian incident. Additional processing of the information may also be sought.

5.3.6.2 (U) OPTION 2: CONVERT THE COMPLAINT OR GUARDIAN INCIDENT TO AN ASSESSMENT OR PREDICATED INVESTIGATION

(U//F~~OUO~~) A supervisor may determine that the information in a complaint is sufficient to meet the standard for opening of an Assessment[18] or a predicated investigation.

(U) The supervisor may serialize to:

- (U//~~FOUO~~) A new Assessment file, when further investigative activity is warranted, and the FBI employee articulates an authorized purpose and clearly defined objective(s) to open an Assessment.
- (U//~~FOUO~~) An open Assessment file, when further investigative activity is warranted, and the information is consistent with and advances the authorized purpose and clearly defined objective(s) of an ongoing Assessment.
- (U//~~FOUO~~) A new predicated investigation file, when further investigative activity is warranted, there is sufficient predication to open an investigation, and the FBI employee obtains the requisite supervisory approval(s) to open an investigation.
- (U//~~FOUO~~) An open predicated investigation file, when further investigative activity is warranted and the information is related to and advances an ongoing investigation.

5.3.6.3 (U) OPTION 3: CLOSE THE COMPLAINT OR GUARDIAN INCIDENT AS "INFORMATION ONLY" - REFER TO OTHER GOVERNMENT AGENCY

(U) When it is determined that the information received is credible concerning serious criminal activity not within the FBI's investigative jurisdiction, the supervisor must promptly transmit the information or refer the complainant to a law enforcement agency having jurisdiction, unless an exemption exists for sharing the information. (See DIOG subsection 14.4.2.) In this circumstance, the Guardian incident (converted to an FD-71a when serialized into Sentinel) must

[17] (U) The Guardian application refers to this evaluation as "pre-Assessment" activity.
[18] (U//F~~OUO~~ b7E

be placed into the appropriate case file classification's zero file. An FD-999 may also be required when information is disseminated to another agency. (See DIOG subsection 12.6.)

(U//~~FOUO~~) Specific procedures for the required dissemination of information related to TTL and suspected abuse are located in the following subsections:

- (U) Threat to Life: See DIOG subsection 14.7.
- (U) Suspected child abuse: See DIOG subsection 14.8.
- (U) Suspected abuse of the elderly or otherwise vulnerable individuals: See DIOG subsection 14.9.

(U) See DIOG subsection 5.12.1, when disseminating personally identifiable information (PII) contained in a complaint or Guardian incident. If PII from a closed complaint is disseminated outside the FBI (according to authorized dissemination guidelines and procedures and consistent with the Privacy Act of 1974), it must be accompanied by the required annotation, as set out in DIOG subsection 5.12.1.

(U) The supervisor may serialize to:

- (U//~~FOUO~~) A closed Assessment file, when the Guardian incident is to be closed (FD-71a in Sentinel) as "Information Only" and no further investigative activity is warranted, but the information is related to the authorized purpose and clearly defined objective(s) of a previously closed Assessment.
- (U//~~FOUO~~) A closed predicated investigation file, when the Guardian incident is to be closed (FD-71a in Sentinel) as "Information Only" and no further investigative activity is warranted, but the information is relevant to the closed predicated investigation.

5.3.6.4 (U) OPTION 4: CLOSE THE COMPLAINT OR GUARDIAN INCIDENT – NO INVESTIGATIVE ACTIVITY WARRANTED AT THIS TIME

(U) The information received cannot be rationally tied to a particular crime or threatened crime; conduct constituting a threat to national security; an individual, group, or organization that may be involved in criminal or national security threatening conduct; or a topical matter of foreign intelligence interest.

(U) Although the FBI has broad investigative jurisdiction, there are myriad reasons why a submitted tip or complaint may not warrant investigative activity (e.g., a tip containing insufficient detail or a complaint lacking a federal nexus). In these circumstances, the initial FO reviewer may opt to close the complaint outright. The supervisor must annotate the Guardian incident accordingly by including a caveat that the individual or group was identified as part of the initial processing of a complaint received, but no information was developed at that time to warrant investigation.

(U) The supervisor may serialize to:

- (U//~~FOUO~~) A zero file, when the initial processing Guardian (converted to an FD-71a in Sentinel) is to be closed as "Information Only," and no further investigative activity is warranted.

- (U//~~FOUO~~) An unaddressed work file, when the information has potential investigative value, but there are insufficient human resources to adequately address it. In this circumstance, the supervisor must annotate the handling of the Guardian incident accordingly.

5.3.6.5 (U) Option 5: Close the Complaint or Guardian Incident - The Information Received is Based Solely on Activities that are Protected by the First Amendment or on Race, Ethnicity, Gender, National Origin, Religion, Disability, Sexual Orientation, or Gender Identity of the Subject, or a Combination of Only Such Factors.

(U) The complaint received is based solely on the basis of activities that are protected by the First Amendment or on race, ethnicity, gender, national origin, religion, disability, sexual orientation, or gender identity of the subject, or a combination of only such factors. The supervisor must annotate the Guardian incident accordingly by including a caveat that the individual or group was identified as part of the initial processing of a complaint received, but no information was developed at that time that warranted further investigation. In such a circumstance, the Guardian incident (converted to an FD-71a) and any retained record associated with it must be treated in accordance with the *Handling of Privacy Act Records Maintained in Violation of the Privacy Act's Provision Concerning First Amendment Activity Policy Directive* (1270D).

5.3.6.6 (U//~~FOUO~~) Additional Supervisory Requirements for a Closing Complaint or Guardian Incident

(U//~~FOUO~~) **Closing a TTL or a Time Sensitive Guardian incident:** Closing a TTL or Time Sensitive tip or complaint requires SSA approval. SSAs must review the Guardian incident to ensure that the reasons for closing are clearly documented and any relevant information was properly disseminated pursuant to DIOG subsection 14.7[19] (for TTL complaints) or 14.8 (for Time Sensitive complaints involving suspected child abuse).

(U//~~FOUO~~) Additionally, no more than [redacted] from the TTL or Time Sensitive Guardian incident's closing date, an [redacted] must review the Guardian to document concurrence with the SSA's determination to close the Guardian incident and that all of the reasons for the closure are properly documented. If the [redacted] b7E

[redacted]

[19] (U//~~FOUO~~) Even when a partner agency is investigating the matter and has not (and will not) request FBI assistance, the requirements of subsection 14.7 to notify the intended victim still apply.

(U//~~FOUO~~) **Closing a Routine Guardian incident:** Closing a Routine complaint requires SSA approval. SSAs must review the Guardian incident to ensure that the reasons for closing are clearly documented [redacted] b7E

(U//~~FOUO~~) FBI supervisors are only permitted to place a closed complaint into an open (i.e., pending or pending inactive) investigative file when it is related to and advances an ongoing Type 1 & 2 or 3 Assessment or predicated investigation. A closed complaint cannot be placed into an open Type 4–6 Assessment file.

5.3.6.7 (U//~~FOUO~~) TIME FRAME FOR SUPERVISORY EVALUATION OF A SUBMITTED GUARDIAN INCIDENT

(U//~~FOUO~~) The applicable time frame and procedures for a supervisor to evaluate the submitted Guardian incident are determined by the investigative program and category of complaint processing (e.g., TTL, Time Sensitive, and Routine).

A. (U//~~FOUO~~) **TTL and Time Sensitive processing:** The responsible SSA must evaluate and assign the Guardian incident for processing. The assigned employee is required to **immediately** commence the processing activities described in DIOG subsection 5.3.9. At a minimum, the assigned employee must complete the database checks described in DIOG subsection 5.3.10 no more than [redacted] after being assigned the initial processing. b7E

   (U//~~FOUO~~) **TTL and Time Sensitive** Guardian incidents are assigned to an FBI employee for processing pursuant to DIOG subsection 5.3.6.

B. (U//~~FOUO~~) **Routine processing:** A FO supervisor must complete the Guardian review involving criminal, cyber, or counterintelligence matters, no more than [redacted] from receiving the submitted Guardian incident. For a Guardian involving counterterrorism or WMDD matters, the supervisor must complete the review no more than [redacted] from receiving the submitted Guardian.

(U) Consistent with DIOG Section 14, FBI employees are responsible for properly disseminating certain information as soon as practicable. Specific procedures for the required dissemination of information related to TTL and suspected abuse are located in the following subsections:

- (U) Threat to Life: See DIOG subsection 14.7.
- (U) Suspected child abuse: See DIOG subsection 14.8.
- (U) Suspected abuse of the elderly or otherwise vulnerable individuals: See DIOG subsection 14.9.

5.3.7 *(U//~~FOUO~~) ROUTINE GUARDIAN INCIDENT JUSTIFICATION REVIEWS (CRIMINAL, CYBER, AND COUNTERINTELLIGENCE)*

(U//~~FOUO~~) Pursuant to DIOG subsection 5.3.5.2 FBI employees are required to complete Guardian incident processing activities no more than [redacted] from being assigned a **Routine** Guardian incident for processing in the criminal, cyber, or counterintelligence b7E

programs. If a routine Guardian incident has not been converted to an Assessment or predicated investigation, or closed, pursuant to DIOG subsection 5.3.6 by the end of this [redacted] period, a supervisor must review the Guardian incident and the investigative steps undertaken with the assigned FBI employee to determine an appropriate disposition. A supervisor must repeat this review of the Guardian incident at the end of each subsequen[redacted] period, until the incident is converted or closed. (See DIOG subsection 5.3.6.) This justification review process only applies to routine Guardian incidents in the criminal, cyber, or counterintelligence programs. b7E

(U//~~FOUO~~) This Guardian justification review must be completed and documented [redacted] after the end of the [redacted] and should cover the following [responses to the justification review questions below are documented in the appropriate field provided in the Guardian incident]:

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

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

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

(U//~~FOUO~~) Supervisors should confirm that the initial processing is not based solely on activity that is protected by the First Amendment or on the race, ethnicity, gender, national origin, religion, disability, sexual orientation, or gender identity of an individual, group, or organization (or a combination of only those factors). b7E

(U//~~FOUO~~) Is it reasonably likely that, if given more time to complete the activities authorized during initial processing, the FBI employee will be able to establish an appropriate basis to open an Assessment, with an authorized purpose and clearly defined objective(s), or to open a predicated investigation consistent with the standards set forth in the DIOG?

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

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

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

(U//~~FOUO~~) If additional time is necessary to determine if the Guardian incident should be closed as "Information Only" or "converted" into an Assessment or predicated investigation, a supervisor may approve [redacted] extension in the Guardian incident. Additional

extensions, routed to the approving official by the Guardian application, require the following approvals:

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

b7E

(U//~~FOUO~~)

5.3.8 *(U) Documentation of Investigative Methods Authorized Prior to Opening an Assessment or Predicated Investigation*

(U//~~FOUO~~) FBI employees are permitted to retain records checks and other information collected while processing a complaint received using the investigative methods permitted in DIOG subsection 5.3.9. This collection or record retention is permitted if, in the judgement of the FBI employee, there is a law enforcement, national security, intelligence, or public safety purpose to do so. Indexing of the information is mandatory.

(U//F~~OUO~~) All pending investigative files and unaddressed work files are subject to file reviews pursuant to DIOG subsection 3.5.4.

(U//~~FOUO~~) When documenting investigative activities authorized during the complaint processing, FBI employees must create a complete and accurate record by documenting information as provided by the reporting party or as reflected in the accessed record. Any characterizations of individuals, groups, or activities must be properly attributed to the reporting party (or accessed record) and not to the FBI (e.g.,

b7E

(U) For policy on information or evidence obtained prior to opening an Assessment, in Assessments and predicated investigations, see DIOG subsection 18.4.

5.3.9 *(U) Investigative Methods Authorized During the Processing of Complaints (i.e., Investigative Activities Permitted Prior to Opening an Assessment or Predicated Investigation)*

(U//~~FOUO~~) When processing a complaint, an FBI employee is permitted to use only the following investigative methods. These investigative methods focus on access to historical records or data in the possession of governmental agencies, publicly accessible information, or information voluntarily provided. As such, their use aligns with the principle of utilizing the least intrusive method available, based upon the circumstances, to achieve an investigative objective:

5.3.9.1 **(U) PUBLIC INFORMATION**

(U//~~FOUO~~) See DIOG subsection 18.5.1.

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

5.3.9.2 **(U) RECORDS OR INFORMATION - FBI AND DOJ**

(U//~~FOUO~~) See DIOG subsection 18.5.2.

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

(U//~~FOUO~~) See DIOG subsection 18.5.3.1.

5.3.9.4 **(U) ONLINE SERVICES AND RESOURCES**

(U//~~FOUO~~) See DIOG subsection 18.5.4 and DIOG Appendix L, Section 3

5.3.9.5 **(U) CLARIFYING INTERVIEW**

(U//~~FOUO~~) Conduct a voluntary clarifying interview of the complainant or the person who initially furnished the information. A clarifying interview is limited to the sole purpose of clarifying or eliminating confusion in the original allegation or information provided. It is not intended to be an interview as described in 18.5.6. A clarifying interview should be documented [redacted] b7E

(U//~~FOUO~~) Whenever feasible, all interviews conducted in response to a TTL Guardian incident must be conducted in person.

5.3.9.6 **(U) INFORMATION VOLUNTARILY PROVIDED BY GOVERNMENTAL OR PRIVATE ENTITIES**

(U//~~FOUO~~) See DIOG subsection 18.5.7.

NOTE: (U//~~FOUO~~) Activities described in DIOG subsections 5.3.9.1–5.3.9.4 and 5.3.9.6 may also be proactively undertaken without prior supervisory approval (i.e., not in response to a specific complaint), as long as the FBI employee conducting the queries has an authorized purpose to do so (i.e., a reason tied to an authorized FBI criminal or national security purpose for undertaking the activity). For example, independent of a specific complaint, an FBI employee may query FBI databases and publicly available information on the internet to process observations or to support an intelligence product. Refer to DIOG subsection 15.2.3 for additional policy on intelligence analysis and planning. Policy on online activities authorized prior to opening an Assessment or predicated investigation is located in DIOG Appendix L.

[20] (U//~~FOUO~~) [redacted] The clarifying interview must be limited to the initial complaint or specific topic initially discussed. b7E

5.3.10 *(U//~~FOUO~~) REQUIRED RECORDS CHECKS FOR ALL INITIAL PROCESSING*

(U//~~FOUO~~) Whenever a Guardian incident is assigned for processing, the assigned employee must query all of the following databases using all known selectors and identifiers:

A) (U//~~FOUO~~)
B) (U//~~FOUO~~)
C) (U//~~FOUO~~)
D) (U//~~FOUO~~)
E) (U//~~FOUO~~)
F) (U//~~FOUO~~)

b7E

(U//~~FOUO~~) Based upon information obtained from these databases, FBI employees may determine that additional database checks are appropriate and necessary, including queries of:

A) (U//~~FOUO~~)
B) (U//~~FOUO~~)
C) (U//~~FOUO~~)
D) (U//~~FOUO~~)
E) (U//~~FOUO~~)
F) (U//~~FOUO~~)
G) (U//~~FOUO~~)
H) (U//~~FOUO~~)
I) (U//~~FOUO~~)
J) (U//~~FOUO~~)

(U//~~FOUO~~)

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

b7E

b7E

5.3.11 *(U) CONVERT, TRANSFER, OR RECATEGORIZE A GUARDIAN INCIDENT DURING THE PROCESSING PHASE*

(U//~~FOUO~~) Initial determinations during the processing of complaints may change as FBI employees develop additional information. For example, a complaint assigned to an FBI employee for processing may be quickly "converted" to a Type 1 & 2 Assessment, if the FBI employee has sufficient information to establish an authorized purpose and clearly defined objective(s).

(U//~~FOUO~~) When the initial processing of complaints are transferred within or between FOs, the time frames described in DIOG subsections, 5.3.5.1, 5.3.5.2, and 5.3.6.7 do not reset.

(U//F~~OUO~~) If an FBI employee has reason to believe that a TTL complaint is improperly categorized (i.e., there is no credible threat of harm or violence that could reasonably result in death or serious bodily injury), the employee must obtain approval from the TTL Guardian designee (see DIOG subsection 5.3.3.1) to recategorize the Guardian incident as Routine. Additionally, if a duty agent, Guardian squad supervisor, or other applicable SSA assesses that initial processing of a complaint is assigned to an incorrect AOR, he or she must immediately transfer the Guardian incident to the correct FO (or legal attaché office) and then make positive contact with a representative in that office to confirm receipt. Documentation of the positive contact must be made in the Guardian application.

(U//F~~OUO~~) Similarly, if an FBI employee has reason to believe that a Time Sensitive Guardian incident is improperly categorized (i.e., the complaint does not include information regarding an [1] sexual abuse, physical abuse or exploitation of a child or [2] abuse against the elderly and otherwise vulnerable individuals), he or she must obtain supervisory approval to recategorize the Guardian incident as Routine.

(U//F~~OUO~~)

b7E

5.3.12 *(U) SITUATIONAL COMPLAINT EXAMPLES*

(U) The following examples demonstrate the delicate balance between pursuing legitimate investigative goals without infringing upon the exercise of constitutionally protected rights. They are not exhaustive and may not be illustrative of all applicable factors. FBI employees who are unsure if Guardian incident processing implicates privacy and civil liberties concerns must seek guidance from a supervisor, a CDC, an ADC, or the OGC.

[22] (U//~~FOUO~~

b7E

5.3.12.1 **(U) EXAMPLE A**

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

b7E

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

5.3.12.2 **(U) EXAMPLE B**

b7E

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

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

5.3.12.3 **(U) EXAMPLE C:**

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

b7E

b7E

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

5.4 (U) FIVE TYPES OF ASSESSMENTS (*AGG-DOM*, PART II.A.3.)

5.4.1 *(U) ASSESSMENT TYPES*

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

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

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

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

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

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

5.5 (U) STANDARDS FOR OPENING OR APPROVING AN ASSESSMENT

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

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

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

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

5.6 (U) POSITION EQUIVALENTS, EFFECTIVE DATE, DURATION, DOCUMENTATION, APPROVAL, NOTICE, FILE REVIEW, AND RESPONSIBLE ENTITY

5.6.1 *(U) FIELD OFFICE AND FBIHQ POSITION EQUIVALENTS*

(U//~~FOUO~~) FBIHQ and FBI FOs have the authority to conduct all Assessment activities, as authorized in DIOG subsection 5.4. Position equivalents for FO and FBIHQ personnel when FBIHQ opens, conducts, or closes an Assessment are specified in DIOG Section 3.5.1.

5.6.2 *(U) EFFECTIVE DATE OF ASSESSMENTS*

(U//~~FOUO~~) The effective date of an Assessment (for record keeping purposes) is the date the final approval authority approves the Guardian FD-71a (Type 1 & 2) or the EC used to open the Assessments (Types 3–6) in Sentinel. Documenting the effective date of an Assessment is important for many reasons, including establishing time frames for justification and file reviews, and extensions. The effective date for Assessments occurs when:

A) (U//~~FOUO~~) **For Type 1 & 2 Assessments:** the SSA approves the Guardian incident's conversion to "Open" in Guardian.

(U//~~FOUO~~) *Note*: Per DIOG subsection 5.6.3.1.3, agents or TFOs do not need to obtain supervisory approval for engaging in the use of investigative methods permitted prior to the opening of a Type 1 & 2 Assessment. Once the Guardian is converted to the Open status, the change is transmitted to Sentinel.

B) (U//~~FOUO~~) **For Type 3–6 Assessments:** the SSA, supervisory intelligence analyst (SIA), and for Type 6 Assessments, the HUMINT Program Management Unit (HPMU) unit chief (UC) approves the opening "Create Case Request" in Sentinel as a Type 3–6 Assessment.

C) (U//~~FOUO~~) **For Type 1 & 2 Sensitive Investigative Matters (SIM) Assessments:**

1. (U//~~FOUO~~) ***Field Office:*** the SAC approves the Guardian incident's conversion to Open in Guardian. (See DIOG subsection 5.7 and Section 10.)
2. (U//~~FOUO~~) ***FBIHQ:*** the deputy director (DD) approves the Guardian incident's conversion to Open in Guardian. (See DIOG subsection 5.7 and Section 10.)

D) **For Type 3 - 6 SIM Assessments:**

1. (U//~~FOUO~~) ***Field Office***: The SAC (and for Type 6 Assessments the Directorate of Intelligence [DI] HUMINT Operations Section [HOS] section chief [SC])

approves Guardian incident's conversion to Open as Type 3-6 Assessment. (See DIOG subsection 5.7 and Section 10.)

2. (U//~~FOUO~~) ***FBIHQ***: The relevant FBIHQ SC approved the Guardian incident's conversion to Open as a Type 3–6 Assessment

5.6.3 *(U) ASSESSMENT TYPES*

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

(U//~~FOUO~~) In all types of Assessments, investigative leads (either "Action Required" or "Information Only") may be set by a Sentinel Lead Request form, EC, or the Guardian application. See DIOG Appendix J for additional information involving leads.

5.6.3.1 (U) TYPE 1 & 2 ASSESSMENTS

(U) **Type 1 & 2 Assessment defined:** Seek information, proactively or in response to investigative leads, relating to activities—or the involvement or role of individuals, groups, or organizations in those activities—constituting violations of federal criminal law or threats to national security (i.e., the prompt checking of leads on individuals, activity, groups or organizations) (*AGG-Dom*, Part II.A.3.a.i and ii).

(U//~~FOUO~~) Within the Guardian application, FBI employees may apply two categories of higher precedence to Type 1 & 2 Assessments, as appropriate:

A. (U//~~FOUO~~) **TTL,** for Type 1 & 2 Assessments involving a credible threat of harm or violence that could reasonably result in the death or serious bodily injury of an individual.

B. (U//~~FOUO~~) **Time Sensitive,** for Type 1 & 2 Assessments involving an imminent or ongoing threat of (1) sexual abuse, physical abuse or exploitation of a child or (2) abuse against the elderly and otherwise vulnerable individuals.

(U//~~FOUO~~) A Guardian incident marked as "TTL" or "Time Sensitive" retains that category label upon conversion to an open Type 1 & 2 Assessment, unless that category label is removed pursuant to the recategorization process described in DIOG subsection 5.3.11. Whenever requirements for a TTL Type 1 & 2 Assessment or Time Sensitive Type 1 & 2 Assessment differ from a routine Type 1 & 2 Assessment, those differences are specifically set out in the relevant subsections below. For more detailed information on TTL reporting and documentation, beyond Type 1 & 2 Assessments, refer to DIOG subsections 5.3.3 and 14.7.

(U//~~FOUO~~) See DIOG subsection 5.11 for intelligence collection (i.e., incidental collection) and documentation requirements. All incidental collection must be documented in the [redacted] b7E
[redacted] additionally, the appropriate operational squad must be notified of the information to determine whether an Assessment or a predicated investigation is already open, or should be opened, based upon the alleged threat activity.

(U//~~FOUO~~) Conducting a Type 1 & 2 Assessment from FBIHQ has additional separate requirements, refer to DIOG subsection 5.6.3.1.4.

5.6.3.1.1 ***(U) DURATION***

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

5.6.3.1.2 ***(U) DOCUMENTATION***

(U//~~FOUO~~) [redacted] FD-71a.

(U//~~FOUO~~) FBI employees must also document in the Guardian application [redacted] b7E

[redacted] in the Guardian application requires SSA approval before being closed and serialized as an FD-71a [redacted]

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

(U//~~FOUO~~) *Note:* Investigative activity must not be conducted[23] out of a control file.

(U//~~FOUO~~) Indexing of the information used to create the initial Guardian FD-71a is mandatory.

5.6.3.1.3 ***(U) APPROVAL TO OPEN***

(U//~~FOUO~~) An agent or TFO may engage in Type 1 & 2 Assessment activity without prior supervisory approval. However, all Type 1 & 2 Assessment activity [redacted] the Guardian application, [redacted] b7E

[redacted] See DIOG subsection 5.3.5.1 for drafting a Guardian incident.

(U//~~FOUO~~) The agent or TFO and the SSA must apply the standards for opening a Type 1 & 2 Assessment contained in DIOG subsection 5.5. Additional approval requirements apply to SIMs, as described below in DIOG subsection 5.6.3.1.4.

5.6.3.1.4 ***(U) SENSITIVE INVESTIGATIVE MATTERS***

(U//~~FOUO~~) **Opening requirements for Type 1 & 2 SIM Assessments:**

(U//~~FOUO~~) ***Opened by an FO:*** As soon as practicable, but not more than five business days after determining that a Type 1 & 2 Assessment involves a SIM, the matter must be reviewed by the CDC and approved by the SAC. If the Assessment involves Presidential or congressional candidates or campaigns, refer to DIOG subsection 5.6.3.1.4.1 for additional requirements. The term "sensitive investigative matter" is defined in DIOG subsection 5.7.1 and Section 10. The documentation in the Guardian application [redacted] b7E

[redacted]

[23] (U) Investigative methods may only be conducted out of investigative files. Additionally, certain investigative methods are not permitted in Assessments, or for use prior to opening an Assessment or predicated investigation.

b7E

(U//~~FOUO~~) ***Opened by FBIHQ:*** For the rare circumstances in which FBIHQ-led Type 1 & 2 SIM Assessments are deemed appropriate, prior consultation with the ADIC(s) or SAC(s) of all affected FOs, OGC review, and DD (nondelegable) approval are required. The documentation in the Guardian application

(U//~~FOUO~~) If a SIM arises after an FBIHQ-led Type 1 & 2 Assessment has already been opened, ongoing and previously approved investigative activity may continue; however, before initiating or beginning additional investigative activity, the FBIHQ section with oversight must consult with the affected ADIC(s) or SAC(s), obtain OGC review, and obtain DD (nondelegable) approval to continue the investigation. These steps must be completed as soon as practicable, but not more than five business days after the SIM arises.

5.6.3.1.4.1 (U) Additional Rules Regarding Presidential and Congressional Candidates and Campaigns

(U) The following additional rules apply to certain Type 1 & 2 Assessments.

- (U//~~FOUO~~) Regarding a declared candidate for President or Vice President of the United States, a Presidential campaign, or a senior Presidential campaign staff member or advisor[24], the opening of the Assessment. Under no circumstances are FBI personnel permitted to open a Type 1 & 2 Assessment prior to b7E
- (U//~~FOUO~~) Regarding a declared candidate for the US Senate or the US House of Representatives or his or her campaign, the appropriate the opening of an FBIHQ Assessment. Under no circumstances are FBI personnel permitted to open a Type 1 & 2 Assessment
- (U//~~FOUO~~) Regarding any investigation into activities related to illegal contributions to, donations to, or expenditures on behalf of a Presidential or US congressional campaign by foreign nationals, the opening of a FO Assessment, or the appropriate the opening of an FBIHQ Assessment or

[24] (U) This includes any person who has been publicly announced by a campaign as a staffer or a member of an official campaign advisory committee or group.

(U//~~FOUO~~) If any of the above matters arise after the opening of a Type 1 & 2 Assessment, FBI personnel may continue investigative activity but must begin conducting required notifications and consultations and begin seeking required approvals within five business days.

5.6.3.1.5 *(U) UNDISCLOSED PARTICIPATION (UDP)*

(U//~~FOUO~~) b7E

(See DIOG Section 16.)

5.6.3.1.6 *(U) NOTICE*

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

(U//~~FOUO~~) However, if the Assessment has additional approval requirements because it involves a Presidential or congressional candidate or campaign (see DIOG subsection 5.6.3.1.4.1), the case manager, in coordination with the FBIHQ operational unit, must provide written notification to the assistant Attorney(s) General (AAG) and the US attorney(s) with jurisdiction over the matter.

(U//~~FOUO~~) Employees should check b7E

5.6.3.1.7 *(U) JUSTIFICATION REVIEW*

(U//~~FOUO~~) In accordance with DIOG subsection 3.5.4.6, SSAs must conduct justification reviews for Type 1 & 2 Assessments every 30 calendar days. At the end of each 30 calendar day period, the agent or TFO and the supervisor have **up to ten calendar days** to complete all aspects of the justification review and to document the review. Justification reviews may be documented in either Guardian or Sentinel. (See DIOG subsection 3.5.4.6.)

(U//~~FOUO~~) b7E

(U) Refer to DIOG subsection 3.5.4 for complete requirements and justification review standards.

5.6.3.1.8 *(U) RESPONSIBLE ENTITY*

(U//~~FOUO~~) A Type 1 & 2 Assessment may be conducted by a FO investigative squad or by an FBIHQ operational division. Only agents and TFOs can be assigned as case managers for Type 1 & 2 Assessments. Pursuant to DIOG subsection 3.4.2.3, IAs and professional investigative staff may not be assigned as case managers or co-case managers for Type 1 & 2 Assessments.

5.6.3.1.9 ***(U) TYPE 1 & 2 ASSESSMENT CLOSING***

(U//~~FOUO~~) Closing a Type 1 & 2 Assessment requires supervisory approval, as described below. Supervisors must review the investigative actions documented in the Guardian application (or the associated Sentinel case file) to ensure that it contains sufficient details of the investigation and the basis on which the decision was made to close the Type 1 & 2 Assessment [redacted] b7E

A) (U//~~FOUO~~) **Closing When Opened by an FO:** Closing a Type 1 & 2 Assessment opened by an FO requires approval from the SSA with oversight.

(U//~~FOUO~~) **Closing For TTL and Time Sensitive**: The closure of a TTL or Time Sensitive Type 1 & 2 Assessment requires [redacted] b7E
[redacted] the Assessment should therefore be closed. Within [redacted] days of the assigned case manager submitting a TTL or Time Sensitive Assessment for closure, [redacted]

B) (U//~~FOUO~~) **Closing When Opened by FBIHQ:** Closing a Type 1 & 2 Assessment opened by FBIHQ requires [redacted]

(U//~~FOUO~~) **Closing For TTL and Time Sensitive**: The closure of a TTL or Time Sensitive Type 1 & 2 Assessment when opened at FBIHQ requires the same procedures as outlined above for FO closings. [redacted]

C) (U//~~FOUO~~) **Closing When SIM Opened by an FO:** Closing a Type 1 & 2 Assessment opened by an FO involving a SIM requires [redacted] If the Type 1 & 2 Assessment involves a Presidential or congressional candidate or campaign (see DIOG subsection 5.6.3.1.4.1), the same level of approval required to open the Assessment is also required to close the investigation (e.g., [redacted] b7E

D) (U//~~FOUO~~) **Closing When SIM Opened by FBIHQ:** Closing a Type 1 & 2 Assessment opened by FBIHQ involving a SIM requires [redacted] If the Type 1 & 2 Assessment involves a Presidential or congressional candidate or campaign (see DIOG subsection 5.6.3.1.4.1), the same level of approval required to open the Assessment is also required to close the investigation (e.g., i[redacted]

(U//~~FOUO~~) Refer to DIOG subsections 5.12.1 and 5.12.1.1 for additional guidance on closing Type 1 & 2 Assessments.

5.6.3.1.10 *(U) EXAMPLES AND SCENARIOS OF TYPE 1 & 2 ASSESSMENTS*

5.6.3.1.10.1 (U) EXAMPLE 1

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

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

b7E

(U//~~FOUO~~) The agent or TFO can proactively conduct basic record checks and online searches If the agent or TFO determines no further investigation is required to open an Assessment (or predicated investigation) after conducting these queries, he or she should refer to DIOG subsection 5.3.8 for documentation requirements.

(U//~~FOUO~~)

and complete a Guardian FD-71a.

5.6.3.1.10.2 (U) EXAMPLE 2

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

b7E

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

b7E

5.6.3.2 **(U) TYPE 3 ASSESSMENTS**

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

(U//~~FOUO~~) Type 3 Assessments may be used to analyze or determine whether particular national security or criminal threats exist within the AOR and whether there are victims or targets within the AOR who are vulnerable to any such actual or potential threats. The authorized purpose and clearly defined objective(s) of a Type 3 Assessment must be based on or related to actual or potential federal criminal or national security targets, threats, or vulnerabilities. While no particular factual predication is required, the basis of the Assessment cannot be arbitrary or groundless speculation, nor can the Assessment be based solely on the exercise of First Amendment protected rights, or on race, ethnicity, gender, national origin, religion, disability, sexual orientation, or gender identity, or a combination of only such factors.

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

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

(U//~~FOUO~~) Investigative or Assessment activity utilized in the development of an intelligence product in support of special events (such as a Joint Threat Assessment [JTA], Joint Special Event Threat Assessment [JSETA], or a Special Events Threat Assessment [SETA]) must be authorized from and documented to a DIOG approved investigative or open Assessment case file. For example, if CHS tasking, data mining, or a collection emphasis or action message is required to develop an intelligence product in support of a special event, a Type 3 Assessment, maintained in the must be open to authorize Assessment activities and to produce the intelligence product. b7E

(U//~~FOUO~~) Intelligence products produced in support of special events (i.e., JTA, JSETA, and SETA) derived solely from information that already exists in systems of records from within the FBI or the Intelligence Community does not require separate DIOG authorization to produce. Opening a Type 3 Assessment in support of special events does not eliminate the

requirement to use the [redacted] as a non-investigative file for administrative and logistical functions related to the FBI's support of a special event. (See the *Special Events Management Policy Guide* [0666PG].) b7E

(U//~~FOUO~~) Documenting the use and results of investigative methods authorized prior to opening an Assessment, during an Assessment, and in a predicated investigation cannot be serialized or otherwise maintained in [redacted] This does not preclude the inclusion of investigative and Assessment activity and results from such activity in [redacted] in the context of how the investigative or Assessment activity directly impacts special event planning, coordination, and resource allocation. If these non-investigative documents discuss investigative or assessment activities, these documents must appropriately cite the DIOG open Assessment or predicated investigative case file number that authorizes the Assessment or investigative activity. Additionally, the [redacted] is subject to the periodic file review requirements described in DIOG subsection 3.5.4. b7E

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

(U//~~FOUO~~) See DIOG subsection 5.11 for intelligence collection, (i.e., incidental collection) and documentation requirements. All incidental collection must be documented in the 815 FO file. Additionally, the appropriate operational squad must be notified of the information to determine whether an Assessment or a predicated investigation is already open, or should be opened, based upon the alleged threat activity.

5.6.3.2.1 *(U) DURATION*

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

5.6.3.2.2 *(U) DOCUMENTATION*

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

[redacted]

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

[redacted]

b7E

(U//~~FOUO~~)

(U//~~FOUO~~)

(U//F~~OUO~~) Investigative Activity must not be conducted[25] out of a control file.

5.6.3.2.3 ***(U) APPROVAL***

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

5.6.3.2.4 ***(U) SENSITIVE INVESTIGATIVE MATTERS (SIM)***

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

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

(U//~~FOUO~~) As specified in FBIHQ divisions' PGs, there may be agreements (e.g., memoranda of understanding or treaties) that require additional coordination and approval prior to conducting certain activities.

5.6.3.2.5 ***(U) UNDISCLOSED PARTICIPATION (UDP)***

(U//~~FOUO~~) If the Assessment involves UDP, additional levels of approval may be required. (See DIOG Section 16.)

5.6.3.2.6 ***(U) NOTICE***

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

[25] (U) Investigative methods may only be conducted out of investigative files.

5.6.3.2.7 ***(U) FILE REVIEW***

(U//~~FOUO~~) A Type 3 Assessment requires a file review in accordance with DIOG subsection 3.5.4.

5.6.3.2.8 ***(U) RESPONSIBLE ENTITY***

(U//~~FOUO~~) A Type 3 Assessment may be opened by FO IPs, the DI, a DI sponsored entity, FO investigative squads, and FBIHQ operational divisions. The nature of the Assessment dictates the file classification into which the Type 3 Assessment is opened. Assessments conducted by the DI or FO IPs must be opened in the appropriate [redacted] b7E [redacted] All other Type 3 Assessments must be opened in the appropriate investigative file classification. If the responsibility for an FO IP opened Type 3 Assessment is transferred to an operational squad, the [redacted] must be changed to an appropriate investigative file classification.

5.6.3.2.9 ***(U) AUTHORIZED INVESTIGATIVE METHODS IN TYPE 3 ASSESSMENTS***

(U//~~FOUO~~) In addition to the investigative methods permitted during an Assessment listed in DIOG subsection 18.5, a Type 3 Assessment [redacted] b7E [redacted]

5.6.3.2.10 ***(U) TYPE 3 ASSESSMENT CLOSING***

(U//~~FOUO~~) The closing EC must be approved by the supervisor responsible for the investigation. If it is a SIM investigation, the closing EC must also be approved by the SAC.

(U//~~FOUO~~) Refer to DIOG subsections 5.12.1 and 5.12.1.2 for guidance on documentation requirements when closing a Type 3 Assessment.

5.6.3.2.11 ***(U) EXAMPLES OF TYPE 3 ASSESSMENTS***

5.6.3.2.11.1 **(U) EXAMPLE 1**

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

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

5.6.3.2.11.2 **(U) EXAMPLE 2**

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

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

5.6.3.2.11.3 **(U) EXAMPLE 3**

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

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

5.6.3.2.11.4 **(U) EXAMPLE 4**

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

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

b7E

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

5.6.3.2.11.5 **(U) EXAMPLE 5**

b7E

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

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

5.6.3.3 **(U) TYPE 4 ASSESSMENTS**

(U) Type 4 Assessment defined: Obtain and retain information to inform or facilitate intelligence analysis and planning (*AGG-Dom*, Part II.A.3.d and Part IV).

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

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

(U//~~FOUO~~) Whenever a Type 4 Assessment identifies and begins to focus on specific individual(s), group(s), or organization(s), whose activities may constitute a violation of federal criminal law or a threat to national security, a separate Type 1 & 2 Assessment or a predicated investigation must be opened. Similarly, if a Type 4 Assessment identifies a particular national security or criminal threat within the AOR, or identifies victims or targets

within an AOR who are vulnerable to any actual or potential threat, a separate Type 3 Assessment or predicated investigation must be opened.

(U//~~FOUO~~) A Type 4 Assessment may not be used for the purpose of collecting PFI, although such intelligence may be incidentally collected. PFI can only be intentionally collected pursuant to DIOG subsection 5.6.3.5 (Type 6 Assessment) and Section 9.

(U//~~FOUO~~) See DIOG subsection 5.11 for intelligence collection (i.e., incidental collection) and documentation requirements. All incidental collection must be documented in the FBIHQ or FO 815 file. Additionally, the appropriate operational squad must be notified of the information to determine whether an Assessment or a predicated investigation is already open, or should be opened, based upon the alleged threat activity.

5.6.3.3.1 *(U) DURATION*

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

5.6.3.3.2 *(U) DOCUMENTATION*

(U//~~FOUO~~) b7E

(U//~~FOUO~~)

(U//~~FOUO~~) This type of Assessment must be documented in the appropriate

(U//~~FOUO~~) *Note:* Investigative activity must not be conducted[26] out of a control file.

5.6.3.3.3 *(U) APPROVAL*

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

5.6.3.3.4 *(U) SENSITIVE INVESTIGATIVE MATTERS (SIM)*

(U//~~FOUO~~) If the Assessment involves a sensitive investigative matter (SIM), the CDC must review and the SAC must approve the Assessment prior to opening. If a SIM arises after the

[26] (U) Investigative methods may only be conducted out of investigative files.

opening of a Type 4 Assessment, Assessment activity may continue, but the matter must be documented in an EC reviewed by the CDC and approved by the SAC as soon as practicable, but not more than five business days after the SIM arises. The term "sensitive investigative matter" is defined in DIOG subsection 5.7 and Section 10.

5.6.3.3.5 *(U) NOTICE*

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

5.6.3.3.6 *(U) FILE REVIEW*

(U//~~FOUO~~) A Type 4 Assessment requires a file review in accordance with DIOG subsection 3.5.4.

5.6.3.3.7 *(U) RESPONSIBLE ENTITY*

(U//~~FOUO~~) A Type 4 Assessment may only be opened and managed by the domain management coordinator or an intelligence analyst performing domain analysis functions within the operational divisions.

5.6.3.3.8 *(U) TYPE 4 ASSESSMENT CLOSING*

(U//~~FOUO~~) The closing EC must be approved by the supervisor responsible for the investigation. If it is a SIM investigation, the closing EC must also be approved by the SAC.

(U//~~FOUO~~) Refer to DIOG subsections 5.12.1 and 5.12.1.2 for guidance on documentation requirements when closing a Type 4 Assessment.

5.6.3.3.9 *(U) EXAMPLES OF TYPE 4 ASSESSMENTS*

5.6.3.3.9.1 (U) EXAMPLE 1

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

b7E

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

5.6.3.3.9.2 (U) EXAMPLE 2

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

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

b7E

5.6.3.3.9.3 **(U) EXAMPLE 3**

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

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

5.6.3.3.9.4 **(U) EXAMPLE 4**

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

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

5.6.3.4 **(U) TYPE 5 ASSESSMENTS**

(U) Type 5 Assessment defined: Seek information to identify potential human sources, assess their suitability, credibility, or value of individuals as human sources (*AGG-Dom*, Part II.A.3.c).

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

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

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

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

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

(U//~~FOUO~~ b7E

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

5.6.3.4.1 *(U) PHASES OF TYPE 5 ASSESSMENTS*

5.6.3.4.1.1 (U//~~FOUO~~) IDENTIFICATION PHASE

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

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

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

(U//~~FOUO~~) If necessary, after a CHS identification plan has been approved, and a group of individuals who potentially have placement and access to the relevant information have been identified, the SA or IA may, with authorization set forth in DIOG subsection 5.6.3.4.3.1, use additional characteristics to narrow the group of individuals to those most likely to have the desired placement and access. An intelligence product may be produced during the Identification Phase describing the results of, or analysis generated during, the Identification Phase. The product may be based upon analysis of the group's characteristics or search criteria that may yield insight into previously unknown similarities, activities, or patterns of conduct. If any additional investigative methods are sought that will focus on an individual, then an Evaluation Phase must be opened. Any product produced must be documented in the Assessment's INTELPRODS subfile, and approved and disseminated in accordance with the procedures outlined in the *IPPG*.

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

5.6.3.4.1.2 (U//~~FOUO~~) EVALUATION PHASE

(U//~~FOUO~~) This phase may be used by an SA assigned to either a HUMINT or investigative squad or by an IA assigned to a FO or FBIHQ to evaluate a known individual believed to have placement and access, so that the individual, if successfully recruited, can provide the FBI with information of value. The goal of this phase of a Type 5 Assessment is to gather information, through the use of the investigative methods set forth in DIOG subsection 5.6.3.4.8, regarding background, authenticity, and suitability of a particular PCHS (specific named individual). An IA who develops information during this phase that indicates a PCHS is worthy of recruitment should prepare a [redacted] b7E for use by an SA on the appropriate HUMINT or investigative squad to recruit the individual. The SIP, or any other intelligence product, must be documented in the Assessment's INTELPRODS subfile. *Note:* A [redacted] may be prepared by other FBI employees assigned to the Evaluation Phase of a Type 5 Assessment as case participants. However, the Assessment's assigned case manager(s) remains responsible for the content of the [redacted]. If information developed during this phase indicates the individual should not be recruited as a CHS, the Type 5 Assessment must be closed.

5.6.3.4.1.3 (U//~~FOUO~~) RECRUITMENT PHASE

(U//~~FOUO~~) This phase may only be used by an SA assigned to a HUMINT or investigative squad. The goal of this phase of a Type 5 Assessment is to recruit the PCHS to become an operational CHS, and therefore, the Recruitment Phase may focus only on a specific named individual. Information from a [redacted] or other information or intelligence b7E available to the SA may be used during the recruitment phase. If the recruitment is successful, the Type 5 Assessment must be closed (see DIOG subsection 5.6.3.4.9) and the individual opened as a CHS in Delta. The Type 5 Assessment must also be closed if

the recruitment is not successful, either because the individual declines to become a CHS or a determination is made not to continue the recruitment.

5.6.3.4.2 ***(U) DURATION***

(U//~~FOUO~~) The effective date of a Type 5 Assessment is the date the highest level of authority required approves the opening EC. A Type 5 Assessment may continue for as long as necessary to achieve its authorized purpose and clearly defined objective(s), as set forth in the three phases above, or when it is determined that the individual named subject cannot or should not be recruited as a CHS.

5.6.3.4.3 ***(U) DOCUMENTATION***

5.6.3.4.3.1 **(U//~~FOUO~~) IDENTIFICATION PHASE**

(U//~~FOUO~~)

b7E

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

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

b7E

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

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

b7E

b7E

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

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

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

b7E

5.6.3.4.3.2 **(U//~~FOUO~~) EVALUATION/RECRUITMENT PHASES**

(U//~~FOUO~~) A Type 5 Assessment opened to evaluate or recruit a specific person as a CHS must be opened with an EC using the appropriate b7E

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

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

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

5.6.3.4.4 ***(U) APPROVAL***

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

5.6.3.4.4.1 **(U//~~FOUO~~) SENSITIVE POTENTIAL CHSS AND GROUPS**

(U//~~FOUO~~) CDC review and SAC approval is required before a Type 5 Assessment may be opened on a sensitive PCHS or if, during the Identification Phase, a sensitive characteristic is at least one aspect being used to identify individuals with potential placement and access to information of interest. If it is determined after opening a Type 5 Assessment that a PCHS is sensitive or that a sensitive characteristic must be added to the PCHS identification plan, the Assessment activity may continue, but the matter must be documented in an EC, reviewed by the CDC, and approved by the SAC as soon as practicable, but not more than five business days of this determination. Additionally, if the Type 5 Assessment involves a sensitive PCHS (Evaluation and Recruitment Phases), or during the Identification Phase, a sensitive characteristic is an aspect being used to identify individuals, the EC must contain the words "Sensitive PCHS" or "Sensitive Characteristic" (as part of an identification plan). Conversely, if a matter that has been designated as a sensitive PCHS or as having a sensitive characteristic, no longer remains as such, due to a change in the facts and circumstances of the Assessment, this change of designation must be made to the file in the case title. A sensitive PCHS or sensitive characteristic (as part of an identification plan) is defined as follows:

A) (U//~~FOUO~~) A domestic public official (other than a member of the US Congress or White House staff, which requires higher approval authority). (See the *Confidential Human Source Policy Guide* (1212PG) (CHSPG) [redacted] b7E

B) (U//~~FOUO~~) A domestic political candidate.

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

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

E) (U//~~FOUO~~) A member of the news media.

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

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

(U//~~FOUO~~) For additional information regarding sensitive PCHSs, see the *CHSPG*, Part 2; DIOG subsection 10.1.4; and *DIOG Appendix G - Classified Provisions* [redacted]

5.6.3.4.5 ***(U) NOTICE***

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

5.6.3.4.6 ***(U) FILE REVIEW***

(U//~~FOUO~~) The frequency of a supervisory file review must be in accordance with DIOG subsection 3.5.4.7. See the *CHSPG* [links to a ~~SECRET//NOFORN~~ document] for Type 5 file review procedures.

(U//~~FOUO~~) The Type 5 Assessment file review must be documented in Sentinel. Because Type 5 Assessments are confidential, the Sentinel file review must not reveal information that could identify the PCHS.

5.6.3.4.7 ***(U) RESPONSIBLE ENTITY***

(U//~~FOUO~~) A Type 5 Assessment without a specific named individual may be opened by SAs on HUMINT or investigative squads or at FBIHQ or by IAs assigned to a FO or FBIHQ. A Type 5 Assessment on specific named individual may be opened by SAs on HUMINT or investigative squads and by IAs (Evaluation Phase only) assigned to the FO HUMINT or investigative squads or at FBIHQ.

5.6.3.4.8 ***(U) AUTHORIZED INVESTIGATIVE METHODS IN TYPE 5 ASSESSMENTS***

(U//~~FOUO~~) Only the following investigative methods may be used in a Type 5 Assessment, whether in the Identification, Evaluation, or Recruitment phase. All of these investigative methods may be used by SAs. IAs and professional investigative staff members (PIS) may only use investigative methods (A) through (F).

A) (U//~~FOUO~~) Public information.

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

C) (U//~~FOUO~~) Records or information–other federal, state, local, tribal, or foreign government agencies.

D) (U//~~FOUO~~) Online services and resources.

E) (U//F~~OUO~~) Information voluntarily provided by governmental or private entities.

F) (U//F~~OUO~~) Use of an alias with false identification (AFID) or the covert approach is only permitted for use during approved activity in a Type 5 Assessment. (See the note below and the *CHSPG* [redacted] b7E

G) (U//~~FOUO~~) CHS use and recruitment.

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

I) (U//F~~OUO~~) Physical surveillance (not requiring a court order).

J) (U//~~FOUO~~) Polygraph examinations (See *CHSPG*).

K) (U//~~FOUO~~) Trash covers (searches that do not require a warrant or court order). (*Note*: SSA approval and consultation with CDC or OGC is required prior to use of this method. See DIOG subsection 18.6.12.5.)

(U//~~FOUO~~) *Note:* Consent searches are authorized in Assessments.[27]

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

(U//~~FOUO~~) In addition, as specified in FBIHQ divisions' PGs, there may be agreements (e.g., memoranda of understanding) that require additional coordination and approval prior to conducting certain activities.

(U//~~FOUO~~) If DIOG Section 18 requires documentation of the request or the approval to use an authorized investigative method, the request and approval must be documented with an EC.

(U//~~FOUO~~) *Note:* The covert approach, which may be authorized in an approved Type 5 Assessment, pursuant to the procedures detailed in the *CHSPG* [links to a ~~SECRET//NOFORN~~ document], is not an undercover activity subject to the provisions of DIOG subsection 18.6.13. The distinction between the covert approach and undercover activity lies in the authorized purpose of the Type 5 Assessment, which is to seek information to identify, evaluate, and recruit an individual as a CHS, not to seek information relevant to federal crimes or national security threats. (See also *DIOG Appendix G – Classified Provisions* [links to a ~~SECRET//NOFORN~~ document].)

(U//~~FOUO~~) Additionally, in the course of a predicated investigation, an agent cannot utilize undercover activity (up to five times pursuant to UCO guidelines), with the specific purpose to identify, evaluate, or recruit a PCHS. The agent must

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

b7E

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

5.6.3.4.9 *(U) CLOSING TYPE 5 ASSESSMENTS*

(U//~~FOUO~~) A Type 5 Assessment must be closed under the following circumstances:

A) (U//~~FOUO~~) In a Type 5 Assessment opened without a specific named individual, it is determined that the characteristics and search criteria used to identify individuals with placement and access to needed information have not succeeded

[27] (U//~~FOUO~~) The DOJ has opined that consent searches are authorized in Assessments, as well as in predicated investigations.

in identifying such individuals, or the FBI no longer has a need for a CHS with the specified placement and access. Additionally, the closing EC must document the factual basis for closing the Assessment.

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

C) (U//~~FOUO~~) In a Type 5 Assessment opened on a specific named individual, it is determined that the PCHS is not a suitable candidate for further evaluation and recruitment efforts. Additionally, the closing EC must document the factual basis for closing the Assessment.

D) (U//~~FOUO~~) In a Type 5 Assessment opened on a specific named individual, SA recruitment efforts are successful and the PCHS has been opened as a CHS in Delta. Do not include the S number in the closing EC. Once the successfully recruited PCHS' Delta file is opened, all documents and records in the Type 5 Assessment must be maintained in the CHS' open Delta file.

E) (U//~~FOUO~~) In a Type 5 Assessment opened on a specific named individual, SA efforts to recruit the PCHS have been unsuccessful, or it is determined that further recruitment efforts are not likely to be successful. Additionally, the closing EC must document the factual basis for closing the Assessment.

(U) Refer to DIOG subsection 5.12.1.3 for guidance on properly marking a closed Type 5 Assessment that contains personal information.

5.6.3.4.9.1 (U) CLOSING APPROVAL FOR TYPE 5 ASSESSMENTS

(U//~~FOUO~~) Type 5 Assessments must be closed, via EC, with SSA approval, if it was opened by an SA. Type 5 Assessments must be closed with SIA and SSA approval, if it was opened by an IA.

5.6.3.4.10 *(U) EXAMPLES OF TYPE 5 ASSESSMENTS*

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

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

b7E

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

b7E

b7E

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

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

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

b7E

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

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

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

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

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

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

5.6.3.5 (U) TYPE 6 ASSESSMENTS

(U) Type 6 Assessment defined: Seek information, proactively or in response to investigative leads, relating to matters of foreign intelligence interest responsive to foreign intelligence requirements. (*AGG-Dom*, Part II.A.3.a.iii).

(U//~~FOUO~~) A Type 6 Assessment is designed to allow the FBI to determine whether the circumstances within a FO's territory would enable the office to conduct a Full Investigation to collect information responsive to a PFI requirement. PFI requirements are described in DIOG subsection 9.1. A Type 6 Assessment focuses on a FO's capability to collect on those PFI requirements. While no particular factual predication is required, the basis of the

Assessment cannot be arbitrary or groundless speculation, nor can the Assessment be based solely on the exercise of First Amendment protected rights or on race, ethnicity, gender, national origin, religion, disability, sexual orientation, or gender identity, or a combination of only those factors.

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

(U//~~FOUO~~) FBI employees must prioritize collection in response to FBI National Collection Requirements, before attempting to collect against a PFI collection requirement. The *IPG* furnishes guidance on the prioritization of collection.

(U//~~FOUO~~) See DIOG subsection 5.11 for intelligence collection (i.e., incidental collection) and documentation requirements. All incidental collection must be documented in the FBIHQ or FO 815 file. Additionally, the appropriate operational squad must be notified of the information to determine whether an Assessment or a predicated investigation is already open, or should be opened, based upon the alleged threat activity.

5.6.3.5.1 *(U) DURATION*

(U//~~FOUO~~) There are no time limitations on the duration of a Type 6 Assessment. The effective date of the Assessment is the date on which the DI HOS HPMU, UC approves the EC. (See DIOG subsection 5.6.2.) A Type 6 Assessment may continue for as long as necessary to achieve its authorized purpose and clearly defined objective(s). Although a Type 6 Assessment is not limited in duration, when the authorized purpose and clearly defined objective(s) have been met, the Assessment must be closed or converted to a Full Investigation with an EC approved by the FO SSA and the HPMU UC. When closing a Type 6 Assessment that is designated as a SIM, the SAC and the HOS SC must approve the closing EC.

5.6.3.5.2 *(U) DOCUMENTATION*

(U//~~FOUO~~) A Type 6 Assessment must be opened by EC, using the appropriate [redacted] The opening EC must identify the authorized purpose and the clearly defined objective(s) of the Assessment. If additional objectives arise during the course of the Assessment, they must also be documented in an EC and approved by the FO SSA. [redacted] b7E

(U//~~FOUO~~) *Note:* Investigative activity must not be conducted[28] out of a control file.

5.6.3.5.3 *(U) APPROVAL*

(U//~~FOUO~~) All Type 6 Assessments must be opened by EC and approved in advance by an SSA and the HPMU UC. A Type 6 Assessment must be approved in accordance with the

[28] (U) Investigative methods may only be conducted out of investigative files.

standards provided in DIOG subsection 5.5. Notwithstanding any other provision in the DIOG, a Type 6 Assessment cannot be opened on oral approval.

5.6.3.5.4 ***(U) SENSITIVE INVESTIGATIVE MATTERS (SIM)***

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

5.6.3.5.5 ***(U) NOTICE***

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

5.6.3.5.6 ***(U) FILE REVIEW***

(U//~~FOUO~~) A Type 6 Assessment requires a file review in accordance with DIOG subsection 3.5.4.

5.6.3.5.7 ***(U) RESPONSIBLE ENTITY***

(U//~~FOUO~~) A Type 6 Assessment may only be opened and conducted by the FO IP and the DI. (See the *IPPG* for further details.) Under the management of the FIG, FO investigative squads or FBIHQ divisions may support the collection of information in a Type 6 Assessment.

5.6.3.5.8 ***(U) TYPE 6 ASSESSMENT CLOSING***

(U//~~FOUO~~) The closing EC must be approved by the supervisor responsible for the investigation and the HPMU UC. If it is a SIM investigation, the closing EC must also be approved by the SAC and the DI SC.

(U//~~FOUO~~) See DIOG subsections 5.12.1 and 5.12.1.2 for guidance on documentation requirements when closing a Type 6 Assessment.

5.6.3.5.9 ***(U) EXAMPLES/SCENARIOS OF TYPE 6 ASSESSMENTS***

5.6.3.5.9.1 **(U) EXAMPLE 1**

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

b7E

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

b7E

5.6.3.5.9.2 **(U) EXAMPLE 2**

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

b7E

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

5.7 (U) SENSITIVE INVESTIGATIVE MATTERS (SIM) IN ASSESSMENTS AND SENSITIVE POTENTIAL CHS OR SENSITIVE CHARACTERISTIC DESIGNATIONS IN TYPE 5 ASSESSMENTS

(U//~~FOUO~~)

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

b7E

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

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

5.7.1 *(U) SIM CATEGORIES IN ASSESSMENTS*

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

b7E

[redacted] b7E

[redacted] If a Type 1 & 2 Assessment involves Presidential or congressional candidates or campaigns, refer to DIOG subsections 5.6.3.1.4.1, 5.6.3.1.6, and 5.6.3.1.9 for additional requirements.

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

5.7.2 *(U) ACADEMIC NEXUS IN ASSESSMENTS*

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

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

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

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

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

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

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

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

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

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

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

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

5.9 (U) AUTHORIZED INVESTIGATIVE METHODS IN ASSESSMENTS

5.9.1 *(U) TYPE 1 & 2, TYPE 3, TYPE 4, AND TYPE 6 ASSESSMENTS*

(U//~~FOUO~~) A complete discussion of these investigative methods, including approval requirements, is contained in DIOG Section 18. The use or dissemination of information obtained by the use of the below methods must comply with the *AGG-Dom* and DIOG Section 14. Only the following investigative methods are authorized in Type 1 &2, Type 3, Type 4, and Type 6 Assessments:

A) (U) Public information (DIOG subsection 18.5.1).

B) (U) Records or information—FBI and DOJ (DIOG subsection 18.5.2).

C) (U) Records or information—other federal, state, local, tribal, or foreign government agency (DIOG subsection 18.5.3.1).

D) (U) Online services and resources (DIOG subsection 18.5.4).

E) (U) CHS use and recruitment (DIOG subsection 18.5.5).

F) (U) Interview or request information from the public or private entities (DIOG subsection 18.5.6).
(U//FOUO) Whenever feasible, all interviews conducted in response to a TTL Guardian incident must be conducted in person.

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

H) (U) Physical surveillance (not requiring a court order) (DIOG subsection 18.5.8).

I) (U) Grand jury subpoenas—to providers of electronic communication services **(only available in a Type 1 & 2 Assessment)** (DIOG subsection 18.5.9).

(U//~~FOUO~~) *Note:* consent searches are authorized in Assessments. [redacted] b7E
[redacted] are also authorized in Assessments (see DIOG subsection 18.6.8.5).

5.9.2 *(U) TYPE 5 ASSESSMENTS*

(U//~~FOUO~~) In addition to the investigative methods listed in DIOG subsection 5.9.1, in a Type 5 Assessments only, an employee may also use the following investigative methods:

A) (U) Use of AFID or covert approach is only permitted for use during approved activity in a Type 5 Assessment. (See the *CHSPG* [links to a ~~SECRET//NOFORN~~ document].)

B) (U) Polygraph examinations (see the *CHSPG*).

C) (U) Trash covers (searches that do not require a warrant or court order). (See DIOG subsection 18.6.12.) (*Note*: SSA approval and consultation with the CDC or OGC is required prior to use of this method.)

5.10 (U) Other Investigative Methods Not Authorized During Assessments

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

5.11 (U) Intelligence Collection (i.e., Incidental Collection)

(U//F~~OUO~~) Incidental collection is information derived during the course of a pending investigation, Assessment, or a Collection Emphasis Message (CEM) that is responsive to a PFI, FBI, or IC collection requirement, but is not related to the topic, purpose, or objective(s), of that specific investigation, Assessment, or CEM.

(U//~~FOUO~~) Incidentally collected information, responsive to the above-mentioned collection requirements, may also be derived from

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

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

b7E

(U//~~FOUO~~)

Additionally, the appropriate operational squad must be notified of the information to determine whether an Assessment or a predicated investigation is already open, or should be opened, based upon the alleged threat activity.

(U//~~FOUO~~)

5.12 (U) RETENTION AND DISSEMINATION OF PRIVACY ACT RECORDS

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

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

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

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

(U) Information obtained during the processing of complaints/Guardian incidents, or during an Assessment, that has insufficient value to justify further investigative activity may contain personal information, such as when records retained in a Guardian incident or an Assessment specifically identify an individual or group whose possible involvement in criminal or national security-threatening activity was checked out while processing the complaint/Guardian incident or through the Assessment. Therefore, whenever the Guardian incident or Assessment turns up no sufficient basis to justify further investigation of the individual or group, then the records must be annotated with the caveats listed in DIOG subsections 5.12.1.1 through 5.12.1.3.

(U) Extreme care should be taken when disseminating personally identifiable information collected during an Assessment that does not lead to sufficient facts to open a predicated

investigation. If personal information from the Assessment is disseminated outside the FBI, according to authorized dissemination guidelines and procedures, it must be accompanied by the required annotation that the Assessment involving this individual or group did not warrant further investigation by the FBI at the time the Assessment was closed.

5.12.1.1 (U) Type 1 & 2 Assessments and Processing Complaints or Guardian Incidents

(U//~~FOUO~~) [redacted] b7E
[redacted] in the Guardian FD-71a. Moreover, any FBI employee who shares information outside the FBI from such a closed Guardian incident or Assessment file must ensure that the following caveat is included in the dissemination:

> (U) "This person [or group] was identified during an Assessment [or "while processing a complaint" for Guardian incidents], but no information was developed at that time that warranted further investigation of the person [or group]."

5.12.1.2 (U) Type 3, 4, and 6 Assessments

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

> (U) "This person [or group] was identified during an Assessment, but no information was developed at that time that warranted further investigation of the person [or group]." b7E

5.12.1.3 (U) Type 5 Assessments

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

A) (U//~~FOUO~~) Type 5 Assessments [redacted]

(U) [redacted]

B) (U//~~FOUO~~) All other Type 5 Assessments:

(U) [redacted]

(U//~~FOUO~~) Any dissemination from a closed Type 5 Assessment must be conducted in accordance with dissemination guidance on CHS closed files provided in the *CHSPG* [links to a ~~SECRET//NOFORN~~ document].

5.13 (U) Assessment File Records Management and Retention

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

b7E

the Guardian FD-71a

Records must be retained according to National Archives and Records Administration (NARA) approved disposition authorities. Consult the IMD Help Desk for assistance.

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

must be approved by the SSA or SIA and serialized to the file. If additional objectives arise during the Assessment, they must be documented in an EC, approved by the SSA or if appropriate, an SIA, and serialized to the file. Assessment classification files must be retained according to NARA-approved disposition authorities.

5.13.1 *(U) PENDING INACTIVE STATUS*

(U//~~FOUO~~) b7E

5.14 (U) OTHER PROGRAM SPECIFIC INVESTIGATION REQUIREMENTS

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

This Page is Intentionally Blank.

6 (U) PRELIMINARY INVESTIGATIONS

6.1 (U) OVERVIEW

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

6.2 (U) PURPOSE AND SCOPE

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

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

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

6.3 (U) CIVIL LIBERTIES AND PRIVACY

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

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

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

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

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

6.4 (U) LEGAL AUTHORITY

6.4.1 *(U) CRIMINAL INVESTIGATIONS*

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

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

6.4.2 *(U) THREATS TO THE NATIONAL SECURITY*

(U) The FBI has authority to investigate threats to the national security pursuant to executive orders, Attorney General authorities, and various statutory sources. (See Appendix B: Executive Order (EO) 12333; 50 U.S.C. §§ 3001 et seq.; 50 U.S.C. §§ 1801 et seq.)

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

6.5 (U) PREDICATION

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

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

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

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

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

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

(U) *NOTE*: See *DIOG Appendix G - Classified Provisions* [links to ~~SECRET//NOFORN~~ document] for additional circumstances warranting a Preliminary Investigation.

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

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

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

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

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

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

6.7 (U) OPENING DOCUMENTATION, APPROVAL, EFFECTIVE DATE, NOTICE, EXTENSION, PENDING INACTIVE STATUS, CONVERSION, AND FILE REVIEW

6.7.1 *(U) OPENING DOCUMENTATION*

(U//~~FOUO~~) The predication to open a Preliminary Investigation must be documented in the opening Electronic Communication (EC). Indexing of the information in the opening document

is mandatory. Division PGs may also require the use of other specific forms to supplement the opening. The appropriate approving authority may grant oral authority to open a Preliminary Investigation if the standards for opening or approving a Preliminary Investigation are met. Should oral authorization to conduct a Preliminary Investigation be granted, an EC setting forth the predicating facts, as well as the identity of the authorizing supervisor and date of oral authorization, must be documented to the supervisor who granted the oral authorization, as soon as practicable, but not more than five (5) business days after granting oral authorization.

(U//~~FOUO~~) b7E

(U//~~FOUO~~) *Note:* Investigative activity must not be conducted[29] out of a control file.

6.7.1.1 **(U) APPROVAL/EFFECTIVE DATE/NOTICE**

(U//~~FOUO~~) The effective date of the Preliminary Investigation is the date the final approval authority (e.g., Supervisory Special Agent (SSA) or Special Agent-in-Charge (SAC)) approves the opening EC. If the Preliminary Investigation is opened on oral authority, the date on which the oral authority was granted is the effective date. See DIOG subsection 3.5.2.2. Adding another subject after opening the Preliminary Investigation does not change the original effective date or the extension date.

A) (U//~~FOUO~~) ***Opened By a Field Office:*** The opening of a Preliminary Investigation by the field office requires prior approval of the SSA b7E

B) (U//~~FOUO~~) ***Opened By FBIHQ:*** The opening of a Preliminary Investigation by FBIHQ requires prior approval of the Unit Chief (UC)

C) (U//~~FOUO~~) ***Sensitive Investigative Matters (SIM):*** The opening of a Preliminary Investigation (PI) involving a SIM:

1) (U//~~FOUO~~) ***SIM Opened by a Field Office:*** requires prior chief division counsel (CDC) review and SAC approval, and written notification via EC to the appropriate FBIHQ operational unit with program responsibility within 15 calendar days of the opening b7E

See *DIOG Appendix G, "Classified Provisions,"* for additional notice requirements. See If the Preliminary Investigation involves presidential or congressional candidates or campaigns, refer to DIOG subsection 6.7.1.2 for additional requirements.

(U//~~FOUO~~) in writing (by letterhead memorandum [LHM] or similar documentation), as soon as practicable,

[29] (U) Investigative methods may only be conducted out of investigative files.

[redacted] after the investigation was opened, [redacted] b7E
[redacted] in its written notice and LHM (or similar documentation) to the responsible FBIHQ operational unit. Upon receiving this notice from the field office, the FBIHQ operational unit must notify the responsible DOJ division, in writing (by LHM or similar documentation), as soon as practicable, [redacted] after the investigation was opened. If the Preliminary Investigation involves presidential or congressional candidates or campaigns, refer to DIOG subsection 6.7.1.2 for additional requirements.

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

(U//~~FOUO~~) If a SIM arises after the opening of a Preliminary Investigation, investigative activity may continue, but the matter must be reviewed by the CDC and approved by the SAC as soon as practicable, but not more than five business days thereafter to continue the investigation. Written notice must be furnished to the responsible FBIHQ operational unit and to the responsible USAO or DOJ division, if applicable. [redacted]

2) (U//~~FOUO~~) ***SIM Opened by FBIHQ:*** For the rare circumstances in which FBIHQ-led PIs involving SIMs are deemed appropriate, prior consultation with the ADIC(s) or SAC(s) of all affected FOs, OGC review, and DD (nondelegable) approval are required [redacted] b7E
[redacted] If the PI involves presidential or congressional candidates or campaigns, refer to DIOG subsection 6.7.1.2 for additional requirements.

(U//~~FOUO~~) The FBIHQ section must also notify the responsible USAO, in writing (by LHM or similar documentation), as soon as practicable [redacted] b7E after the investigation was opened. If the FBIHQ section does not intend to provide notice to the USAO, the FBIHQ section must state the circumstances for not notifying the USAO in its written notice and LHM (or similar documentation) to the responsible DOJ division and the appropriate field office(s), as soon as practicable, but no later than 30 calendar days after the investigation was opened. If the PI involves presidential or congressional candidates or campaigns, refer to DIOG subsection 6.7.1.2 for additional requirements.

(U//~~FOUO~~) b7E

(U//F~~OUO~~) If a SIM arises once a PI has already been opened, ongoing and previously approved investigative activity may continue; however, before initiating or beginning additional investigative activity, the FBIHQ section with oversight must consult with the affected ADIC(s) or SAC(s), obtain OGC review, and obtain DD (nondelegable) approval to continue the investigation. These steps must be completed as soon as practicable, but not more than five business days after the SIM arises. b7E

D) (U//~~FOUO~~) ***FBIHQ Disapproves Opening:*** The Executive Assistant Director (EAD) for the National Security Branch must notify the Deputy Attorney General if FBIHQ disapproves a field office's opening of a Preliminary Investigation relating to a threat to the national security on the ground that the predication for the investigation is insufficient, and the EAD for the National Security Branch is responsible for establishing a system that will allow for the prompt retrieval of such denials. (AGG-Dom, Part II.B.5.d)

6.7.1.2 (U) Additional Requirements for Presidential and Congressional Candidates and Campaigns

(U) In addition to the above SIM notification and approval requirements, the following requirements apply to certain predicated investigations.

(U) Notifications:

(U) All investigations regarding a declared candidate for president or vice president of the United States; a presidential campaign; a senior presidential campaign staff member or advisor[30]; a declared candidate for the US Senate or the US House of Representatives or his or her campaign; or illegal contributions, donations, or expenditures by foreign nationals to a presidential or congressional campaign require written notification to and consultation with the assistant Attorney General(s) (AAG) and US attorney(s) with

[30] (U) This includes any person who has been publicly announced by a campaign as a staffer or a member of an official campaign advisory committee or group.

jurisdiction over the matter. The written notification may be [redacted] b7E

(U) Approvals:

- (U//~~FOUO~~) Regarding a declared candidate for president or vice president of the United States, a presidential campaign, or a senior presidential campaign staff member or advisor; the FBI Director and the AG must approve the opening of the investigation. Under no circumstances are FBI personnel permitted to open an investigation prior to obtaining approval from the Director and AG. The Director's and AG's approval must be documented in writing to the investigative file (e.g. [redacted] b7E
- (U//~~FOUO~~) Regarding a declared candidate for the US Senate or the US House of Representatives or his or her campaign; the [redacted] the opening of an FBIHQ investigation. Under no circumstances are FBI personnel permitted to open an investigation [redacted] b7E
- (U//~~FOUO~~) Regarding any investigation into activities related to illegal contributions, donations, or expenditures by foreign nationals to a presidential or congressional campaign; the [redacted] the opening of an FBIHQ investigation [redacted] b7E

(U//~~FOUO~~) If any of the above matters arise after the opening of an investigation, FBI personnel may continue investigative activity but must initiate required notifications and consultations, and begin seeking required approvals within five business days of the determination that the additional requirements apply.

6.7.2 *(U) EXTENSION*

(U//~~FOUO~~) A Preliminary Investigation must be closed via EC within six months of its opening but may be extended for an additional six months by the SAC (or final approval authority for FBIHQ-led SIM - see DIOG subsection 6.7.1.1.C.2). FBIHQ division PGs may require written notification of this six-month extension. Extensions of Preliminary Investigations beyond one year are discouraged and, in addition to being approved by the SAC (or final approval authority for FBIHQ-led SIM - see DIOG subsection 6.7.1.1.C.2), must be approved, in writing, by the appropriate FBIHQ operational Section Chief for one additional six-month period on a showing of "good cause." The PI extension must be reviewed per the standards of DIOG subsection 6.7.2.1. (AGG-Dom, Part II.B.4.a.ii).

6.7.2.1 (U) GOOD CAUSE

(U//~~FOUO~~) The following factors must be used to determine whether "good cause" exists to extend the Preliminary Investigation beyond one year:

A) (U//~~FOUO~~) Whether logical investigative steps have yielded information that tends to inculpate or exculpate the subject;

B) (U//~~FOUO~~) The progress that has been made toward determining whether a Full Investigation should be opened or the Preliminary Investigation should be closed;

C) (U//~~FOUO~~) Whether, based on the planned course of investigation for the following six months, it is reasonably likely that information will be obtained that will lead to predication for a Full Investigation, thereby warranting an extension for another six months, or will lead to exculpatory information, thereby warranting closing the Preliminary Investigation; and

D) (U//~~FOUO~~) Whether adequate predication has been developed to justify opening a Full Investigation or whether sufficient information has been developed that justifies closing the Preliminary Investigation.

6.7.3 *(U) PENDING INACTIVE STATUS*

(U//~~FOUO~~) b7E

6.7.4 *(U) CONVERSION TO FULL INVESTIGATION*

(U//~~FOUO~~) When converting a Preliminary Investigation to a Full Investigation, see DIOG Section 7 for approval and notification requirements.

6.7.5 *(U) FILE REVIEW*

(U//~~FOUO~~) Supervisory file reviews must be conducted at least once every 90 days in accordance with DIOG Section 3.5.4. File reviews for probationary FBI employees must be conducted at least every 60 days.

6.8 (U) STANDARDS FOR OPENING OR APPROVING THE USE OF AN AUTHORIZED INVESTIGATIVE METHOD IN PRELIMINARY INVESTIGATIONS

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

A) (U//~~FOUO~~) The use of the particular investigative method is likely to further the authorized purpose of the Preliminary Investigation;

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

C) (U//~~FOUO~~) The method to be used is an appropriate use of personnel and financial resources.

6.9 (U) AUTHORIZED INVESTIGATIVE METHODS IN PRELIMINARY INVESTIGATIONS

(U) All lawful methods may be used in a Preliminary Investigation, except for mail opening, physical search requiring a Federal Rules of Criminal Procedure (FCRP) Rule 41 search warrant or a Foreign Intelligence Surveillance Act (FISA) order, electronic surveillance requiring a judicial order or warrant (Title III or FISA), or Title VII FISA requests. Authorized methods include, but are not limited to, those listed below. Some of the methods listed are subject to special restrictions or review or approval requirements. (AGG-Dom, Part V.4.A)

(U//~~FOUO~~) A complete discussion of these investigative methods, including approval requirements, is contained in Section 18. The use or dissemination of information obtained by the use of the below methods must comply with the AGG-Dom and DIOG Section 14. The following investigative methods are authorized to be used in Preliminary Investigations:

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

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

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

D) (U) Online services and resources. (See subsection 18.5.4)

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

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

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

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

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

(U//~~FOUO~~) See the classified provisions in Appendix G for additional information.

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

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

L) (U) Administrative subpoenas. (See subsection 18.6.4)

M)(U) Grand jury subpoenas. (See subsection 18.6.5)

N) (U) National Security Letters. (See subsection 18.6.6)

O) (U) FISA Order for business records. (See subsection 18.6.7)

P) (U) Stored wire and electronic communications and transactional records. (See subsection 18.6.8)[31]

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

R) (U) Mail covers. (See subsection 18.6.10)

S) (U) Polygraph examinations. (See subsection 18.6.11)

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

U) (U) Undercover operations. (See subsection 18.6.13)

(U) See *DIOG Appendix G - Classified Provisions* [links to ~~SECRET//NOFORN document~~] for additional information.

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

6.10 (U) SENSITIVE INVESTIGATIVE MATTERS (SIM) IN PRELIMINARY INVESTIGATIONS

(U//~~FOUO~~) [redacted] DIOG Section 10 contains the required approval authority and factors for consideration when determining whether to conduct or approve a Preliminary Investigation involving a SIM. b7E

6.10.1 *(U) SIM CATEGORIES IN PRELIMINARY INVESTIGATIONS*

(U//~~FOUO~~) A SIM is an investigative matter involving the activities of a domestic public official or domestic political candidate (involving corruption or a threat to the national security), religious or domestic political organization or individual prominent in such an organization, or news media, an academic nexus, or any other matter which, in the judgment of the official authorizing an investigation, should be brought to the attention of FBIHQ and other DOJ officials. (AGG-Dom, Part VII.N.) As a matter of FBI policy, "judgment" means that the decision of the authorizing official is discretionary. [redacted] b7E

If the Preliminary Investigation involves presidential or congressional candidates or campaigns, refer to DIOG subsection 6.7.1.2 for additional requirements.

6.10.2 *(U) ACADEMIC NEXUS IN PRELIMINARY INVESTIGATIONS*

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

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

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

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

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

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

(U//~~FOUO~~) Incidental collection is information derived during the course of a pending investigation, Assessment, or a CEM that is responsive to a PFI, FBI, or IC collection requirement, but is not related to the topic, purpose or objective(s), of that specific investigation, Assessment, or CEM.

(U//~~FOUO~~) Incidentally collected information, responsive to the above-mentioned collection requirements, may also be derived from [redacted] b7E

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

(U//~~FOUO~~) Example 2: [redacted] b7E

(U//~~FOUO~~) [redacted] Additionally, the appropriate operational squad must be notified of the information to determine whether an Assessment or a predicated investigation is already open, or should be opened, based upon the alleged threat activity.

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

6.12 (U) Standards for Approving the Closing of a Preliminary Investigation

6.12.1 *(U) Standards*

(U//~~FOUO~~) At the conclusion of a Preliminary Investigation, each of the following items must be documented in the closing communication (EC and/or LHM):

A) (U//~~FOUO~~) A summary of the results of the investigation;

B) (U//~~FOUO~~) Whether all logical and reasonable investigation was completed;

C) (U//~~FOUO~~) Whether all investigative methods/techniques initiated have been completed and/or discontinued;

D) (U//~~FOUO~~) Whether all leads set have been completed and/or discontinued;

E) (U//~~FOUO~~) Whether all evidence has been returned, destroyed or retained in accordance with evidence policy; and

F) (U//~~FOUO~~) A summary statement of the basis on which the Preliminary Investigation will be closed, and a selection of the appropriate closing status:

1) (U//F~~OUO~~) C-4: Administrative Closing, which includes:

a) (U//~~FOUO~~) No further investigation is warranted because logical investigation and/or leads have been exhausted, and the investigation to date did not identify a criminal violation or a priority threat to the national security

b) (U//F~~OUO~~) Investigation assigned a new file number

c) (U//F~~OUO~~) Investigation consolidated into a new file number or an existing file number, or

d) (U//~~FOUO~~) Unaddressed Work investigation file closed because no investigation or no further investigation will be conducted

2) (U//~~FOUO~~) C-5: USA Declination Closing, which includes:

a) (U//~~FOUO~~) The USAO declined prosecution – individual matter declination

b) (U//~~FOUO~~) The USAO declined prosecution – blanket declination

3) (U//F~~OUO~~) C-6: Other Closing, which includes:

a) (U//F~~OUO~~) National security investigation has been completed

b) (U//~~FOUO~~) Prosecution became non-viable for national security reasons

c) (U//~~FOUO~~) Any other reason to close

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

6.12.2 *(U) APPROVAL REQUIREMENTS TO CLOSE*

(U//~~FOUO~~) The appropriate closing supervisor described below must review and approve the closing communication (as described in subsection 6.12.1) to ensure it contains the above required information and sufficient details of the investigation on which to base the decision to close the Preliminary Investigation. The appropriate closing supervisors are:

A) (U//~~FOUO~~) **Opened by a Field Office:** Closing a Preliminary Investigation opened by a field office requires approval from the SSA [redacted] b7E
Notification to the FBIHQ operational unit may be required by division PGs.

B) (U//~~FOUO~~) **Opened by FBIHQ:** Closing a Preliminary Investigation opened by FBIHQ requires approval from the UC and notification to any appropriate field office.

C) (U//~~FOUO~~) **SIM Opened by a Field Office:** Closing a Preliminary Investigation opened by a field office involving a SIM requires approval from the SAC, written notification to the FBIHQ operational unit and section. If the Preliminary Investigation involves presidential or congressional candidates or campaigns (see DIOG subsection 6.7.1.2), the same level of

approval required to open the investigation is also required to close the investigation, (e.g. if DD approval is required to open the investigation, then the DD must also approve the closure).

D) (U//~~FOUO~~) **SIM Opened by FBIHQ:** Closing a PI opened by FBIHQ involving a SIM requires notification to the ADIC(s) or SAC(s) of all affected FOs, OGC review, and approval from the DD (nondelegable). If the PI involves presidential or congressional candidates or campaigns (see DIOG subsection 6.7.1.2), the same level of approval required to open the investigation is also required to close the investigation, (e.g. if DD approval is required to open the investigation, then the DD must also approve the closure).

6.13 (U) OTHER PROGRAM-SPECIFIC INVESTIGATIVE REQUIREMENTS

(U//~~FOUO~~) To facilitate compliance with investigative program specific requirements, the FBI employee should consult the relevant division's PG.

This Page is Intentionally Blank.

7 (U) FULL INVESTIGATIONS

7.1 (U) OVERVIEW

(U//~~FOUO~~) The *AGG-Dom* authorizes a second level of investigative activity—predicated investigations. Predicated investigations that concern federal crimes or threats to the national security are subdivided into Preliminary Investigations (PI) and Full Investigations (Full). A Full Investigation may be opened if there is an "articulable factual basis" of possible criminal or national threat activity, as discussed in greater detail in Section 7.5, below. There are three types of Full Investigations: (i) single and multi-subject; (ii) Enterprise; and (iii) positive foreign intelligence collection.

7.2 (U) PURPOSE AND SCOPE

(U) A Full Investigation may be opened to detect, obtain information about, or prevent or protect against federal crimes or threats to the national security or to collect foreign intelligence.

(U) The purposes for conducting Full Investigations include such matters as:

A) (U) determining whether a federal crime is being planned, prepared for, occurring or has occurred;

B) (U) identifying, locating, and apprehending the perpetrators;

C) (U) obtaining evidence for prosecution;

D) (U) identifying threats to the national security;

E) (U) investigating an enterprise (as defined in DIOG Section 8); or

F) (U) collecting positive foreign intelligence (PFI) (as defined in DIOG Section 9).

(U) The investigation of threats to the national security can be investigated under the FBI's criminal investigation authority or its authority to investigate threats to the national security. As with criminal investigations, detecting and solving crimes, gathering evidence and arresting and prosecuting the perpetrators are frequently the objectives of investigations relating to threats to the national security. These investigations also serve important purposes outside the ambit of normal criminal investigations, however, by providing the basis for decisions concerning other measures needed to protect the national security.

(U//~~FOUO~~) A Full Investigation solely for the collection of positive foreign intelligence extends the sphere of the FBI's information gathering activities beyond federal crimes and threats to the national security and permits the FBI to seek information regarding a broader range of matters relating to foreign powers, organizations, or persons that may be of interest to the conduct of the United States' foreign affairs. (See DIOG Section 9)

7.3 (U) CIVIL LIBERTIES AND PRIVACY

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

(U) No investigative activity, including Full Investigations, may be taken solely on the basis of rights that are protected by the First Amendment or on the race, ethnicity, gender, national origin, religion, disability, sexual orientation, or gender identity of the subject, or a combination of only those factors. Full Investigations of individuals, groups or organizations must focus on activities related to the threats or crimes being investigated, not solely on First Amendment rights or on the race, ethnicity, gender, national origin, religion, disability, sexual orientation, or gender identity of the subject. In this context, it is particularly important clearly to identify and document the law enforcement or national security basis of the Full Investigation.

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

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

(U) By emphasizing the use of the least intrusive means to obtain intelligence or evidence, FBI employees can effectively execute their duties while mitigating the potential negative impact on the privacy and civil liberties of all people encompassed within the investigation, including targets, witnesses, and victims. This principle is not intended to discourage FBI employees from seeking relevant and necessary intelligence, information, or evidence, but rather is intended to encourage FBI employees to choose the least intrusive—but still reasonable based upon the circumstances of the investigation—from the available options to obtain the intelligence, information or evidence. (See DIOG Section 4)

7.4 (U) LEGAL AUTHORITY

7.4.1 *(U) CRIMINAL INVESTIGATIONS*

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

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

7.4.2 *(U) THREATS TO THE NATIONAL SECURITY*

(U) The FBI has authority to investigate threats to the national security pursuant to executive orders, Attorney General authorities, and various statutory sources. (See E.O. 12333; 50 U.S.C. §§ 3001 et seq.; 50 U.S.C. §§ 1801 et seq.)

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

7.4.3 *(U) FOREIGN INTELLIGENCE COLLECTION*

(U) The FBI authority to collect foreign intelligence derives from a mixture of administrative and statutory sources. (See E.O. 12333; 50 U.S.C. §§ 3001 et seq.; 50 U.S.C. §§ 1801 et seq.; 28 U.S.C. § 532 note (incorporates the Intelligence Reform and Terrorism Protection Act, P.L. 108-458 §§ 2001-2003).

(U) "Foreign Intelligence" is defined as information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations or foreign persons, or international terrorists. (AGG-Dom, Part VII.E)

7.5 (U) PREDICATION

(U) A Full Investigation may be opened if there is an "articulable factual basis" that reasonably indicates one of the following circumstances exists:

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

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

C) (U) The investigation may obtain foreign intelligence that is responsive to a PFI requirement, as defined in DIOG Section 7.4.3, above.

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

A) (U//~~FOUO~~) corroborated information from an intelligence agency states that an individual is a member of a terrorist group;

B) (U//~~FOUO~~) an analyst discovers on a blog a threat to a specific home builder and additional information connecting the blogger to a known terrorist group; and

C) (U//~~FOUO~~) FBI DI has posted an authorized PFI requirement for collection.

(U) *NOTE:* See *DIOG Appendix G - Classified Provisions* [links to ~~SECRET//NOFORN~~ documents] for additional circumstances warranting a Full Investigation.

7.6 (U) STANDARDS FOR OPENING OR APPROVING A FULL INVESTIGATION

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

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

B) (U//~~FOUO~~) The Full Investigation is not based solely on the exercise of First Amendment rights or on the race, ethnicity, gender, national origin, religion, disability, sexual orientation, or gender identity of the subject or a combination of only such factors; and

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

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

7.7 (U) OPENING DOCUMENTATION, APPROVAL, EFFECTIVE DATE, NOTICE, PENDING INACTIVE STATUS, FILE REVIEW, AND LETTER HEAD MEMORANDUM

7.7.1 *(U) OPENING DOCUMENTATION*

(U//~~FOUO~~) The predication to open a Full Investigation must be documented in the opening EC. Indexing of the information in the opening document is mandatory. Division PGs may also require the use of other specific forms to supplement the opening. The appropriate approving authority may grant oral authority to open a Full Investigation if the standards for opening or approving a Full Investigation are met. Should oral authorization to conduct a Full Investigation be granted, an EC setting forth the predicating facts, as well as the identity of the authorizing supervisor and date of oral authorization, must be documented to the supervisor who granted the oral authorization, as soon as practicable, but not more than five (5) business days after granting the authorization.

(U//~~FOUO~~) b7E

(U//~~FOUO~~) *Note:* Investigative activity must not be conducted[32] out of a control file.

7.7.1.1 (U) APPROVAL/EFFECTIVE DATE/NOTICE

(U//~~FOUO~~) The effective date of a Full Investigation is the date the final approval authority (e.g., SSA or SAC) approves the EC. If the Full Investigation is opened on oral authority, the effective date of the Full Investigation is the date on which the oral authority was granted. See DIOG subsection 3.5.2.2.

A) (U//~~FOUO~~) ***Opened By a Field Office:*** The opening of a Full Investigation for circumstances described in subsections 7.5.A and 7.5.B (i.e., for any reason other than to collect intelligence that is responsive to a PFI requirement) by a field office requires prior approval by the SSA. The opening of a Full Investigation on a United States person (USPER) relating to a threat to national security for circumstances described in subsections 7.5.A and 7.5.B (i.e., for any reason other than to collect intelligence that is responsive to a PFI requirement) requires

[32] (U) Investigative methods may only be conducted out of investigative files.

written notification within 15 calendar days of the opening to the responsible FBIHQ operational unit. The responsible FBIHQ NSB unit must notify DOJ NSD (by letterhead memorandum [LHM] or similar documentation) as soon as practicable, but in all events within 30 calendar days after the investigation is opened or the subject is determined to be an USPER. If the subject of the investigation is a non-USPER and later becomes or is determined to be an USPER, the notice provisions in this subsection to DOJ NSD also apply.

B) (U//~~FOUO~~) ***Opened By FBIHQ:*** The opening of a Full Investigation by FBIHQ for circumstances described in Sections 7.5.A and 7.5.B (i.e., for any reason other than to collect intelligence that is responsive to a PFI requirement) requires prior approval of the UC with written notification within 15 calendar days of the opening to any appropriate field office. The opening of a Full Investigation by FBIHQ of an USPER relating to a threat to the national security for circumstances described in Sections 7.5.A and 7.5.B (i.e., for any reason other than to collect intelligence that is responsive to a PFI requirement) also requires notice to DOJ NSD (by LHM or similar documentation) as soon as practicable, but in all events within 30 days after the investigation is opened or the subject is determined to be an USPER. If the subject of the investigation is a non-USPER and later becomes or is determined to be an USPER, the notice provisions in this subsection to the field office and DOJ also apply.

C) (U//~~FOUO~~) ***Sensitive Investigative Matters (SIM):*** The opening of a Full Investigation involving a sensitive investigative matter:

1) (U//~~FOUO~~) ***SIM Opened by a Field Office:*** requires prior chief division counsel (CDC) review, SAC approval, and written notification via EC, to the FBIHQ operational unit with program responsibility within 15 calendar days of the opening [redacted] b7E

[redacted]

See *DIOG Appendix G, "Classified Provisions"* for additional notice requirements. See [redacted] for details concerning notice in counterintelligence and espionage investigations. If the Full Investigation involves presidential or congressional candidates or campaigns, refer to DIOG subsection 7.7.1.2 for additional requirements.

(U//~~FOUO~~) The field office must also notify the US Attorney's Office (USAO), in writing (by letterhead memorandum [LHM] or similar documentation), as soon as practicable [redacted] b7E after the investigation was opened. If the field office does not intend to provide notice to the USAO, the field office must state the circumstances for not notifying the USAO in its written notice and LHM (or similar documentation) to the responsible FBIHQ operational unit. Upon receiving this notice the from the field office, the FBIHQ operational unit must notify DOJ in writing (by LHM or similar documentation), as soon as practicable [redacted] after the investigation was opened. If the Full Investigation involves presidential or congressional candidates or campaigns, refer to DIOG subsection 7.7.1.2 for additional requirements.

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

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

[redacted] Written notice must be furnished to the responsible FBIHQ operational unit and to the responsible USAO or DOJ division, if applicable. [redacted]

2)

2. (U//~~FOUO~~) ***SIM Opened By FBIHQ:*** For the rare circumstances in which FBIHQ-led Full Investigations involving SIMs are deemed appropriate, prior consultation with the ADIC(s) or SAC(s) of all affected FOs, OGC review, and DD (nondelegable) approval are required. b7E

[redacted] If the Full Investigation involves presidential or congressional candidates or campaigns, refer to DIOG subsection 7.7.1.2 for additional requirements.

(U//~~FOUO~~) The FBIHQ section must also notify the responsible USAO, in writing (by LHM or similar documentation), as soon as practicable, but no later than 30 calendar days after the investigation was opened. If the FBIHQ section does not intend to provide notice to the USAO, the FBIHQ section must state the circumstances for not notifying the USAO in its written notice and LHM or similar documentation to the responsible DOJ division and the appropriate field office(s), as soon as practicable, but no later than 30 calendar days after the investigation was opened. If the Full Investigation involves presidential or congressional candidates or campaigns, refer to DIOG subsection 7.7.1.2 for additional requirements. (U//~~FOUO~~) [redacted] b7E

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

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

[redacted] b7E

D) (U//~~FOUO~~) ***Positive Foreign Intelligence Full Investigation:*** The opening of a Full Investigation in order to collect positive foreign intelligence for circumstances described in Section 7.5.C above must be approved as provided in DIOG Section 9. Additionally, written notification to FBIHQ Domain, Collection, HUMINT Operations Section (HOS) SC and DOJ NSD is required as soon as practicable but no later than 30 calendar days after opening the investigation.

E) (U//~~FOUO~~) ***FBIHQ Disapproves Opening:*** The EAD for the National Security Branch (NSB) must notify the Deputy Attorney General if FBIHQ disapproves a field office's opening of a Full Investigation relating to a threat to the national security on the ground that the predication for the investigation is insufficient, and the EAD for the NSB is responsible for establishing a system that will allow for the prompt retrieval of such denials. (AGG-Dom, Part II.B.5.d)

7.7.1.2 ADDITIONAL REQUIREMENTS FOR PRESIDENTIAL AND CONGRESSIONAL CANDIDATES AND CAMPAIGNS

(U) In addition to the above SIM notification and approval requirements, the following requirements apply to certain predicated investigations.

(U) Notifications:

(U) All investigations regarding a declared candidate for president or vice president of the United States; a presidential campaign; a senior presidential campaign staff member or advisor[33]; a declared candidate for the US Senate or the US House of Representatives or his or her campaign; or illegal contributions, donations, or expenditures by foreign nationals to a presidential or congressional campaign require written notification to and consultation with the AAG(s) and US attorney(s) with jurisdiction over the matter. The written notification may [redacted] b7E

(U) Approvals:

- (U//~~FOUO~~) Regarding a declared candidate for president or vice president of the United States, a presidential campaign, or a senior presidential campaign staff member or advisor; the FBI Director and the AG must approve the opening of the

[33] (U) This includes any person who has been publicly announced by a campaign as a staffer or a member of an official campaign advisory committee or group.

investigation. Under no circumstances are FBI personnel permitted to open an investigation prior to obtaining approval from the Director and AG. The Director's and AG's approval must be documented in writing to the investigative file (e.g. [redacted] b7E

- (U//~~FOUO~~) Regarding a declared candidate for the US Senate or the US House of Representatives or his or her campaign; the [redacted] the opening of an FBIHQ investigation. Under no circumstances are FBI personnel permitted to open an investigation [redacted]

- (U//~~FOUO~~) Regarding any investigation into activities related to illegal contributions, donations, or expenditures by foreign nationals to a presidential or congressional campaign; [redacted] the opening of a field office investigation, or [redacted] the opening of an FBIHQ investigation [redacted] b7E

(U//~~FOUO~~) If any of the above matters arise after the opening of an investigation, FBI personnel may continue investigative activity but must initiate required notifications and consultations, and begin seeking required approvals within five business days of the determination that the additional requirements apply.

7.7.2 *(U) Pending Inactive Status*

(U//~~FOUO~~) A Full Investigation may be placed in "pending inactive" status once all logical investigation has been completed and only prosecutive action or other disposition remains to be reported. [redacted] b7E

Examples of Full Investigations that may be placed in "pending inactive" status would include, but not be limited to: criminal investigations pending an appeal; fugitive investigations, when all logical investigation has been conducted and the subject is still in fugitive status; parental kidnapping investigations, when the parent who kidnapped the child is residing in a foreign country and the local authorities will not or cannot extradite the subject back to the United States.

7.7.3 *(U) File Review*

(U//~~FOUO~~) Supervisory file reviews must be conducted at least once every 90 days in accordance with DIOG Section 3.5.4. File reviews for probationary FBI employees must be conducted at least every 60 days.

7.7.4 *(U) Annual Letterhead Memorandum*

(U//~~FOUO~~) Annual letterhead memoranda regarding the status of Full Investigations are not required by the AGG-Dom; however, the FBIHQ operational divisions may require such reports in their PGs. See foreign intelligence collection in Section 9 for annual reporting requirements to FBIHQ HOS and DOJ.

7.8 (U) STANDARDS FOR OPENING OR APPROVING THE USE OF AN AUTHORIZED INVESTIGATIVE METHOD IN FULL INVESTIGATIONS

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

A) (U//~~FOUO~~) The use of the particular investigative method is likely to further the authorized purpose of the Full Investigation;

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

C) (U//~~FOUO~~) If the Full Investigation is for collecting positive foreign intelligence, the FBI is operating openly and consensually with a USPER, to the extent practicable; and

D) (U//~~FOUO~~) The method to be used is an appropriate use of personnel and financial resources.

7.9 (U) AUTHORIZED INVESTIGATIVE METHODS IN FULL INVESTIGATIONS

(U) All lawful methods may be used in a Full Investigation, unless the investigation is to collect foreign intelligence. A complete discussion of these investigative methods, including approval requirements, is contained in Section 18. The use or dissemination of information obtained by the use of these methods must comply with the AGG-Dom and DIOG Section 14. The following investigative methods are authorized to be used in all Full Investigations, other than investigations to collect foreign intelligence:

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

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

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

D) (U) Online services and resources. (Subsection 18.5.4)

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

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

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

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

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

(U//FOUO) See the classified provisions in Appendix G for additional information.

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

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

L) (U) Administrative subpoenas. (Subsection 18.6.4)

M)(U) Grand jury subpoenas. (Subsection 18.6.5)

N) (U) National Security Letters. (Subsection 18.6.6)

O) (U) FISA Order for business records. (Subsection 18.6.7).

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

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

R) (U) Mail covers. (Subsection 18.6.10)

S) (U) Polygraph examinations. (Subsection 18.6.11)

T) (U) Trash Covers (Searches that do not require a warrant or court order). (Subsection 18.6.12)

U) (U) Undercover Operations (Subsection 18.6.13)

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

W)(U) Electronic surveillance – Title III. (Subsection 18.7.2)

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

(U) See *DIOG Appendix G - Classified Provisions* [links to ~~SECRET//NOFORN~~ document] for additional information.

7.10 (U) SENSITIVE INVESTIGATIVE MATTERS (SIM) IN FULL INVESTIGATIONS

(U//~~FOUO~~) [redacted] DIOG Section 10 contains the required approval authority and factors to be considered when determining whether to conduct or approve a Full Investigation involving a SIM.

7.10.1 *(U) SIM CATEGORIES IN FULL INVESTIGATIONS*

(U//~~FOUO~~) A SIM is an investigative matter involving the activities of a domestic public official or domestic political candidate (involving corruption or a threat to the national security), religious or domestic political organization or individual prominent in such an organization, or news media, an academic nexus, or any other matter which, in the judgment of the official authorizing an investigation, should be brought to the attention of FBIHQ and other DOJ officials. (AGG-Dom, Part VII.N). As a matter of FBI policy, "judgment" means that the decision of the authorizing official is discretionary. DIOG Section 10 and the DIOG Appendix G – Classified Provisions define [redacted] If the Full Investigation involves presidential or congressional candidates or campaigns, refer to DIOG subsection 7.7.1.2 for additional requirements. b7E

7.10.2 *(U) ACADEMIC NEXUS IN FULL INVESTIGATIONS*

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

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

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

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

(U//~~FOUO~~)

b7E

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

(U//~~FOUO~~) Incidental collection is information derived during the course of a pending investigation, Assessment, or a CEM that is responsive to a PFI, FBI, or IC collection requirement, but is not related to the topic, purpose or objective(s), of that specific investigation, Assessment, or CEM.

(U//~~FOUO~~) Incidentally collected information, responsive to the above-mentioned collection requirements, may also be derived from

b7E

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

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

b7E

(U//~~FOUO~~)

Additionally, the appropriate operational squad must be notified of the information to determine whether an Assessment or a predicated investigation is already open, or should be opened, based upon the alleged threat activity.

(U//~~FOUO~~)

b7E

(U) Because the authority to collect positive foreign intelligence enables the FBI to obtain information pertinent to the United States' conduct of its foreign affairs, even if that information is not related to criminal activity or threats to the national security, the information gathered may concern lawful activities. Accordingly, the FBI must operate openly and consensually with an USPER to the extent practicable when collecting positive foreign intelligence that does not concern criminal activities or threats to the national security.

7.12 (U) STANDARDS FOR APPROVING THE CLOSING OF A FULL INVESTIGATION

7.12.1 *(U) STANDARDS*

(U//~~FOUO~~) At the conclusion of a Full Investigation, each of the following items must be documented in the closing communication (EC and/or LHM):

A) (U//~~FOUO~~) A summary of the results of the investigation:

B) (U//~~FOUO~~) Whether sufficient personnel and financial resources were expended on the investigation, or an explanation/justification for not expending sufficient resources:

C) (U//~~FOUO~~) Whether logical and reasonable investigation was completed:

D) (U//~~FOUO~~) Whether all investigative methods/techniques initiated have been completed and/or discontinued:

E) (U//~~FOUO~~) Whether all leads set have been completed and/or discontinued:

F) (U//~~FOUO~~) Whether all evidence has been returned, destroyed or retained in accordance with evidence policy: and

G) (U//~~FOUO~~) A summary statement of the reason the Full Investigation will be closed, and selection of the appropriate closing status:

1) (U//~~FOUO~~) C-4: Administrative Closing, which includes:

a) (U//~~FOUO~~) No further investigation is warranted because logical investigation and/or leads have been exhausted, and the investigation to date did not identify a criminal violation or a priority threat to the national security

b) (U//~~FOUO~~) Investigation assigned a new file number

c) (U//~~FOUO~~) Investigation consolidated into a new file number or an existing file number

d) (U//~~FOUO~~) Unaddressed Work investigation file closed because no investigation or no further investigation will be conducted

2) (U//~~FOUO~~) C-5: USA Declination Closing, which includes:

a) (U//~~FOUO~~) The USAO declined prosecution – individual matter declination

b) (U//~~FOUO~~) The USAO declined prosecution – blanket declination

3) (U//~~FOUO~~) C-6: Other Closing, which includes:

a) (U//~~FOUO~~) Final prosecution or final prosecutive action has been completed

b) (U//~~FOUO~~) National security investigation has been completed

c) (U//~~FOUO~~) Prosecution became non-viable for national security reasons

d) (U//~~FOUO~~) A federal grand jury returned a "No True Bill"

e) (U//~~FOUO~~) A nolle prosequi has been entered with the court

f) (U//~~FOUO~~) any other reason for closing

7.12.2 *(U) APPROVAL REQUIREMENTS TO CLOSE*

(U//~~FOUO~~) The appropriate closing supervisor described below must review and approve the closing communication (as described in Section 7.12.1) to ensure it contains the above-required information and sufficient details of the investigation on which to base the decision to close the Full Investigation. Although there is no duration limit for a Full Investigation, the investigation must be closed upon all investigative activity being exhausted. The appropriate closing supervisors are:

A) (U//~~FOUO~~) ***Opened by a Field Office:*** Closing a Full Investigation opened by a field office requires approval from the SSA. Closing a Full Investigation involving espionage or an espionage related matter, requires the concurrence of the FBIHQ Counterespionage section chief. Notification to the FBIHQ operational unit may be required by division PGs.

B) (U//~~FOUO~~) ***Opened by FBIHQ:*** Closing a Full Investigation opened by FBIHQ requires approval from the UC and notification to the appropriate field office.

C) (U//~~FOUO~~) ***SIM Opened by a Field Office:*** Closing a Full Investigation opened by a field office involving a SIM requires approval from the SAC, written notification to the FBIHQ operational unit and section. If the Full Investigation involves presidential or congressional candidates or campaigns (see DIOG subsection 7.7.1.2), the same level of approval required to open the investigation is also required to close the investigation, (e.g. if DD approval is required to open the investigation, then the DD must also approve the closure).

D) (U//~~FOUO~~) ***SIM Opened by FBIHQ:*** Closing a Full Investigation opened by FBIHQ involving a SIM requires notification to the ADIC(s) or SAC(s) of all affected FOs, OGC review, and approval from the DD (nondelegable). If the Full Investigation involves presidential or congressional candidates or campaigns (see DIOG subsection 7.7.1.2), the same level of approval required to open the investigation is also required to close the investigation, (e.g. if DD approval is required to open the investigation, then the DD must also approve the closure).

E) (U//~~FOUO~~) ***Positive Foreign Intelligence:*** (See DIOG Section 9)

7.13 (U) OTHER PROGRAM SPECIFIC INVESTIGATIVE REQUIREMENTS

(U//~~FOUO~~) To facilitate compliance with investigative program-specific requirements, the FBI employee should consult the relevant division's PG to ascertain any program-specific requirements.

This Page is Intentionally Blank.

8 (U) ENTERPRISE INVESTIGATIONS (EI)

8.1 (U) OVERVIEW

(U) An Enterprise Investigation (EI) may only be opened and operated as a Full Investigation and is subject to the same requirements that apply to a Full Investigation as described in DIOG Section 7, although there are additional approval requirements that affect Enterprise Investigations. An Enterprise Investigation focuses on a group or organization that may be involved in the most serious criminal or national security threats to the public, as described in Section 8.5 below. An Enterprise Investigation cannot be conducted as Preliminary Investigation or an Assessment, nor may they be conducted for the sole purpose of collecting positive foreign intelligence (PFI). See Section 8.2, below, regarding Preliminary Investigations and Assessments.

8.2 (U) PURPOSE, SCOPE AND DEFINITIONS

(U) **Enterprise defined:** An enterprise is a group of persons associated together for a common purpose of engaging in a course of conduct. The term "enterprise" includes any partnership, corporation, association, or other legal entity, and any union or group of individuals associated in fact, although not a legal entity.

(U) **Associated in fact defined:** The term "associated in fact" means the persons have an ongoing organization, formal or informal, and that the persons function together as a continuing unit.

(U) **Purpose/Scope:** The purpose of an Enterprise Investigation is to examine the structure, scope, and nature of the group or organization including: its relationship, if any, to a foreign power; the identity and relationship of its members, employees, or other persons who may be acting in furtherance of its objectives; its finances and resources; its geographical dimensions; its past and future activities and goals; and its capacity for harm. (*AGG-Dom*, Part II.C.2)

(U//~~FOUO~~) Although an Enterprise Investigation may not be conducted as a Preliminary Investigation, a Preliminary Investigation may be used to determine whether a group or organization is a criminal or terrorist enterprise if the FBI has "information or an allegation" that an activity constituting a federal crime or a threat to the national security has or may have occurred, is or may be occurring, or will or may occur, and the investigation may obtain information relating to the activity of the group or organization in such activity. An Assessment may also be opened to determine whether a group or organization is involved in activities constituting violations of federal criminal law or threats to the national security.

8.3 (U) CIVIL LIBERTIES AND PRIVACY

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

(U) No investigative activity, including an Enterprise Investigation, may be taken solely on the basis of rights that are protected by the First Amendment or on the race, ethnicity, gender, national origin, religion, disability, sexual orientation, or gender identity of the subject or a combination of only those factors. An Enterprise Investigation of groups and organizations must focus on activities related to the threats or crimes being investigated, not solely on First Amendment rights or on the race, ethnicity, gender, national origin, religion, disability, sexual orientation, or gender identity of the members of the group or organization. In this context, it is particularly important clearly to identify and document the law enforcement or national security basis of the Enterprise Investigation.

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

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

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

8.4 (U) PREDICATION

(U) A Full Investigation of a group or organization may be opened as an Enterprise Investigation if there is an articulable factual basis for the investigation that reasonably indicates the group or organization may have engaged, or may be engaged in, or may have or may be engaged in planning or preparation or provision of support for: (AGG-Dom, Part II.C.1)

A) (U) **Racketeering Activity:**

(U) A pattern of racketeering activity as defined in 18 U.S.C. § 1961(5) - (92 and 305A matters may be opened as Enterprise Investigations-Racketeering Activity (EI/RA));

B) (U) **International Terrorism:**

(U) International terrorism, as defined in AGG-Dom, Part VII.J – (415 and 466 matters may be opened as Enterprise Investigations);

C) (U) **Other National Security Threats,** as listed in AGG-Dom, Part VII.S [redacted] b7E

[redacted]

D) (U) **Domestic Terrorism:**

1) (U) Domestic terrorism as defined in 18 U.S.C. § 2331(5) involving a violation of federal criminal law – (100 matters may be opened as Enterprise Investigations);
2) (U) Furthering political or social goals wholly or in part through activities that involve force or violence and a violation of federal criminal law – (100 matters may be opened as Enterprise Investigations); or
3) (U) An offense described in 18 U.S.C. § 2332b(g)(5)(B) or 18 U.S.C. § 43 – (100 matters may be opened as Enterprise Investigations).

(U) The "articulable factual basis" for opening an Enterprise Investigation is met with the identification of a group whose statements made in furtherance of its objectives or its conduct demonstrate a purpose of committing crimes or securing the commission of crimes by others. The group's activities and statements of its members may be considered in combination to comprise the "articulable factual basis," even if the statements alone or activities alone would not warrant such a determination.

(U) *Note:* Enterprise Investigations were designed, among other things, to combine and replace the traditional "Racketeering Enterprise Investigations" (92 classification) and "Terrorism Enterprise Investigations" (100 classification). An Enterprise Investigation is only authorized to be opened on the most serious criminal or national security threats. The term Enterprise Investigation as used in the DIOG should not be confused with other usages of the word "enterprise," such as criminal Enterprise Investigations (e.g., 281 classification, 245 classification, etc.), which are not Enterprise Investigations as defined in DIOG Section 8. See DIOG Sections 8.4 and 8.5.

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

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

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

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

8.5 (U) STANDARDS FOR OPENING OR APPROVING AN ENTERPRISE INVESTIGATION

(U//~~FOUO~~) Before opening or approving the conduct of an Enterprise Investigation, an FBI employee or approving official must determine whether:

A) (U//~~FOUO~~) Adequate predication exists for opening an Enterprise Investigation;

B) (U//~~FOUO~~) The Enterprise Investigation is not based solely on the exercise of First Amendment rights or on the race, ethnicity, gender, national origin, religion, disability, sexual orientation, or gender identity of the subject or a combination of only such factors; and

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

(U//~~FOUO~~) In addition to the above, the FBIHQ SC reviewing the EI opening request, must also consider whether the request involves an organization or group involved in the most serious violations of federal crime or threats to national security, whether the field office requesting to open the EI is the logical Office of Origin (OO) to oversee the investigation, what impact, if any, opening the EI may have on other field offices, and whether the FBIHQ Section is best positioned to support the OO's investigative strategy and provide deconfliction guidance among affected field offices or operational programs, as appropriate.

(U//~~FOUO~~) A predicated investigation, including an Enterprise Investigation, cannot be opened solely based on an FBI collection requirement.

8.6 (U) OPENING DOCUMENTATION, EFFECTIVE DATE, APPROVAL, NOTICE, AND FILE REVIEW

8.6.1 *(U) OPENING DOCUMENTATION*

(U//~~FOUO~~) The predication to open an Enterprise Investigation must be documented in the opening electronic communication (EC). Indexing of the information in the opening document is mandatory.

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

[redacted] Additional approval requirements apply to SIMs, as described below.

(U//~~FOUO~~) The appropriate approving authority (Section Chief) may grant oral authority to open an Enterprise Investigation if the standards for opening or approving an Enterprise Investigation are met. Should oral authorization to conduct an Enterprise Investigation be granted, an EC setting forth the predicating facts, as well as the identity of the approving official(s) (i.e., SC), and the date of oral authorization must be documented to the approving official(s) who granted the oral authorization as soon as practicable, but not more than five (5) business days after granting oral authorization.

(U//~~FOUO~~) *Note:* Investigative activity must not be conducted[34] out of a control file.

8.6.2 *(U) EFFECTIVE DATE*

(U//~~FOUO~~) The effective date of the Enterprise Investigation is the date the final approval authority (i.e., SC) approves the EC. If the Enterprise Investigation is opened on oral authority, the date on which the oral approval authority was granted is the effective date. See DIOG Section 3.5.2.2.

[34] (U) Investigative methods may only be conducted out of investigative files.

8.6.3 *(U) APPROVAL REQUIREMENTS FOR OPENING AN ENTERPRISE INVESTIGATION (EI)*

8.6.3.1 (U) EI OPENED BY A FIELD OFFICE

(U//~~FOUO~~) The opening of an Enterprise Investigation by an FBI field office requires the prior approval of the appropriate FBIHQ SC, as well as written notification to the United States Attorney's Office (USAO) and the Department of Justice (DOJ) as specified in section 8.6.4.

8.6.3.2 (U) ENTERPRISE INVESTIGATIONS OPENED BY FBIHQ

(U//~~FOUO~~) The opening of an EI by an FBIHQ division requires the prior approval of the appropriate FBIHQ SC, as well as written notification to the appropriate FO(s), the USAO, and DOJ, as specified in subsection 8.6.4. Additional approval requirements apply to SIMs, as described below.

8.6.3.3 (U) NOTICE REQUIREMENTS TO DOJ

(U//~~FOUO~~) FBIHQ division PGs may require specific facts to be included in a field office request to open an Enterprise Investigation. At a minimum, the request must include whether the Enterprise Investigation is a SIM.

(U//~~FOUO~~) The responsible FBIHQ section must notify the DOJ NSD or the Organized Crime and Racketeering Section (OCRS) of the opening of an Enterprise Investigation by a field office or by FBIHQ, as soon as practicable but no later than 30 calendar days after the opening of the investigation.

(U//~~FOUO~~) For Enterprise Investigations that involve groups of persons engaged in international terrorism, other national security threat, or domestic terrorism the responsible DOJ component for the purpose of notification and reports is the NSD. For Enterprise Investigations that involve groups of persons engaged in racketeering activity, the responsible DOJ component is the OCRS of the Criminal Division. (AGG-Dom, Part II.C.3)

(U) The assistant Attorney General for national security or the chief of the OCRS, as appropriate, may at any time request the FBI to provide a report on the status of an Enterprise Investigation, and the FBI will provide such reports as requested. (AGG-Dom, Part II C.3.d)

8.6.3.4 (U) ADDITIONAL REQUIREMENTS FOR PRESIDENTIAL AND CONGRESSIONAL CANDIDATES AND CAMPAIGNS

(U) In addition to the above SIM notification and approval requirements, the following requirements apply to certain predicated investigations.

(U) Notifications:

(U) All investigations regarding a declared candidate for president or vice president of the United States; a presidential campaign; a senior presidential campaign staff member or

advisor[35]; a declared candidate for the US Senate or the US House of Representatives or his or her campaign; or illegal contributions, donations, or expenditures by foreign nationals to a presidential or congressional campaign require written notification to and consultation with the AAG(s) and US attorney(s) with jurisdiction over the matter. The written notification may be in the form of an LHM or similar documentation.

(U) Approvals:

- (U//~~FOUO~~) Regarding a declared candidate for president or vice president of the United States, a presidential campaign, or a senior presidential campaign staff member or advisor; the FBI Director and the AG must approve the opening of the investigation. Under no circumstances are FBI personnel permitted to open an investigation prior to obtaining approval from the Director and AG. The Director's and AG's approval must be documented in writing to the investigative file (e.g. [redacted] b7E
- (U//~~FOUO~~) Regarding a declared candidate for the US Senate or the US House of Representatives or his or her campaign; the [redacted] the opening of an FBIHQ investigation. Under no circumstances are FBI personnel permitted to open an investigation [redacted]
- (U//~~FOUO~~) Regarding any investigation into activities related to illegal contributions, donations, or expenditures by foreign nationals to a presidential or congressional campaign; the [redacted] the opening of a field office investigation, or [redacted] the opening of an FBIHQ investigation [redacted] b7E

(U//~~FOUO~~) If any of the above matters arise after the opening of an investigation, FBI personnel may continue investigative activity but must initiate required notifications and consultations, and begin seeking required approvals within five business days of the determination that the additional requirements apply.

8.6.4 *(U) SENSITIVE INVESTIGATIVE MATTERS*

8.6.4.1 (U//~~FOUO~~) SIM OPENED BY A FIELD OFFICE

(U//~~FOUO~~) Requires prior CDC review, SAC approval, and approval from the FBIHQ [redacted] b7E

[35] (U) This includes any person who has been publicly announced by a campaign as a staffer or a member of an official campaign advisory committee or group.

If the Enterprise Investigation involves presidential or congressional candidates or campaigns, refer to DIOG subsection 8.6.3.4 for additional requirements.
(U//~~FOUO~~) The field office must also notify the USAO, in writing (by LHM or similar documentation), as soon as practicable, but no later than 30 calendar days after the investigation was opened b7E

(U//~~FOUO~~)

(U//~~FOUO~~)

(U//~~FOUO~~)

8.6.4.2 **(U//~~FOUO~~) SIM OPENED BY FBIHQ**

(U//~~FOUO~~) For the rare circumstances when FBIHQ-led EIs involving SIMs are deemed appropriate, prior consultation with the ADIC(s) or SAC(s) of all affected FOs, OGC review, and DD (nondelegable) approval are required. b7E

b7E

If the EI involves presidential or congressional candidates or campaigns, refer to DIOG subsection 8.6.3.4 for additional requirements.

(U//~~FOUO~~) The FBIHQ section must also notify the responsible DOJ division and USAO in writing (by LHM or similar documentation), as soon as practicable,

b7E

(U//~~FOUO~~)

(U//~~FOUO~~)

(U//~~FOUO~~)

b7E

8.6.5 *(U) FILE REVIEW*

(U//~~FOUO~~) Supervisory file reviews must be conducted at least once every 90 days in accordance with DIOG Section 3.5.4. File reviews for probationary agents must be conducted at least once every 60 days.

8.6.6 *(U) PENDING INACTIVE STATUS*

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

8.7 (U) AUTHORIZED INVESTIGATIVE METHODS IN AN ENTERPRISE INVESTIGATION

(U//~~FOUO~~) An Enterprise Investigation may only be opened and operated as a Full Investigation and is subject to the same requirements that apply to a Full Investigation. Therefore, the standards for opening or approving the use of investigative methods and the availability of investigative methods that may be used in an Enterprise Investigation are the same as set forth in Sections 7.8 and 7.9.

8.8 (U) SENSITIVE INVESTIGATIVE MATTERS (SIM) IN ENTERPRISE INVESTIGATIONS

(U//~~FOUO~~) [redacted] DIOG Section 10 contains the required approval authority and factors to be considered when determining whether to conduct or approve an Enterprise Investigation involving a SIM. b7E

8.8.1 *(U) SIM CATEGORIES IN ENTERPRISE INVESTIGATIONS*

(U//~~FOUO~~) A SIM is an investigative matter involving the activities of a domestic public official or domestic political candidate (involving corruption or a threat to the national security), religious or domestic political organization or individual prominent in such an organization, or news media, an academic nexus, or any other matter which, in the judgment of the official authorizing an investigation, should be brought to the attention of FBIHQ and other DOJ officials. (AGG-Dom, Part VII.N). As a matter of FBI policy, "judgment" means that the decision of the authorizing official is discretionary. DIOG Section 10 and/or the DIOG Appendix G – Classified Provisions define domestic public official, domestic political candidate, religious or domestic political organization or individual prominent in such an organization, news media, and academic nexus. If the Enterprise Investigation involves presidential or congressional candidates or campaigns, refer to DIOG subsection 8.6.3.4 for additional requirements.

8.8.2 *(U) ACADEMIC NEXUS IN ENTERPRISE INVESTIGATIONS*

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

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

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

(U//~~FOUO~~) The sensitivity related to an academic institution arises from the American tradition of "academic freedom" (e.g., an atmosphere in which students and faculty are free to express

unorthodox ideas and views and to challenge conventional thought without fear of repercussion). Academic freedom does not mean, however, that academic institutions are off limits to FBI investigators in pursuit of information or individuals of legitimate investigative interest.

(U//~~FOUO~~)

b7E

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

(U//~~FOUO~~) Incidental collection is information derived during the course of a pending investigation, Assessment, or a CEM that is responsive to a PFI, FBI, or IC collection requirement, but is not related to the topic, purpose or objective(s), of that specific investigation, assessment, or CEM.

(U//~~FOUO~~) Incidentally collected information, responsive to the above-mentioned collection requirements, may also be derived from

b7E

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

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

(U//~~FOUO~~)

b7E

(U//~~FOUO~~)

b7E

8.10 (U) STANDARDS FOR APPROVING THE CLOSING OF AN ENTERPRISE INVESTIGATION

8.10.1 *(U) STANDARDS*

(U//F~~OUO~~) At the conclusion of an Enterprise Investigation, each of the following items must be documented in the closing communication (EC and/or LHM):

A) (U//F~~OUO~~) A summary of the results of the investigation;

B) (U//F~~OUO~~) Whether logical and reasonable investigation was completed;

C) (U//F~~OUO~~) Whether all investigative methods initiated have been completed and/or discontinued;

D) (U//F~~OUO~~) Whether all leads set have been completed and/or discontinued;

E) (U//F~~OUO~~) Whether all evidence has been returned, destroyed or retained in accordance with evidence policy; and

F) (U//F~~OUO~~) A summary statement of the basis on which the Enterprise Investigation will be closed, and selection of the appropriate closing status:

1) (U//F~~OUO~~) C-4: Administrative Closing, which includes:

a) (U//F~~OUO~~) No further investigation is warranted because logical investigation and/or leads have been exhausted, and the investigation to date did not identify a criminal violation or a priority threat to the national security

b) (U//F~~OUO~~) Investigation assigned a new file number, or

c) (U//F~~OUO~~) Investigation consolidated into a new file number or an existing file number.

2) (U//F~~OUO~~) C-6: Other Closing, which includes:

a) (U//F~~OUO~~) Enterprise Investigation has been completed; or

b) (U//F~~OUO~~) Any other type of closing

8.10.2 *(U) APPROVAL REQUIREMENTS TO CLOSE*

(U//F~~OUO~~) The appropriate closing supervisor described below must review and approve the closing communication (as described in Section 8.10.1) to ensure it contains the above-required information and sufficient details of the investigation on which to base the decision to close the Enterprise Investigation. Although there is no limit on the duration of an Enterprise Investigation, the investigation must be closed upon all investigative activity being exhausted. The appropriate closing supervisors are:

A) (U//F~~OUO~~) ***Opened by a Field Office with FBIHQ SC Approval:*** Closing an Enterprise Investigation opened by a field office requires the prior approval of the appropriate FBIHQ SC.

B) (U//F~~OUO~~) ***Opened by FBIHQ:*** Closing an Enterprise Investigation opened by FBIHQ requires approval from the appropriate SC and notification to the appropriate field office.

C) (U//~~FOUO~~) ***EI Involving a SIM Opened by FBIHQ:*** Closing an EI opened by FBIHQ involving a SIM requires notification to the ADIC(s) or SAC(s) of all affected FOs, OGC review, and approval from the DD (nondelegable). If the Enterprise Investigation involves presidential or congressional candidates or campaigns (see DIOG subsection 8.6.3.4), the same level of approval required to open the investigation is also required to close the investigation, (e.g. if DD approval is required to open the investigation, then the DD must also approve the closure).

D) (U//~~FOUO~~) ***SIM Opened by FBIHQ:*** Closing an Enterprise Investigation opened by FBIHQ involving a sensitive investigative matter requires approval from the SC, and written notification to the appropriate field office. If the Enterprise Investigation involves presidential or congressional candidates or campaigns (see DIOG subsection 8.6.3.4), the same level of approval required to open the investigation is also required to close the investigation, (e.g. if DD approval is required to open the investigation, then the DD must also approve the closure).

E) (U) Other Program Specific Investigative Requirements

(U//~~FOUO~~) To facilitate compliance with investigative program-specific requirements, the FBI employee should consult the relevant division's PG to ascertain any program-specific requirements.

9 (U) FOREIGN INTELLIGENCE

9.1 (U) OVERVIEW

(U) **Foreign Intelligence defined:** Foreign intelligence is "information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorists." A "Foreign Intelligence Requirement" is a collection requirement issued under the authority of the Director of National Intelligence (DNI) and accepted by the FBI Directorate of Intelligence (DI). Additionally, the President, a United States Intelligence Community (USIC) office designated by the President, the Attorney General, Deputy Attorney General, or other designated Department of Justice (DOJ) official may levy a foreign intelligence requirement on the FBI. Foreign intelligence collection by the FBI is based upon requirements.

(U//~~FOUO~~) Foreign intelligence requirements issued by one of the parties listed above and accepted by the FBI DI will fall into one of two categories: (i) those that address national security issues that are within the FBI's core national security mission (FBI collection requirements); and (ii) information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, foreign persons, or international terrorists which are not within the FBI's core national security mission (PFI Collection Requirements).

(U//~~FOUO~~) Requirements which fall into the first category may correspond to FBI national collection requirements as defined in DIOG Section 5.12. FBI national collection requirements are addressed in properly authorized Assessments (See DIOG Section 5.6.3.5) or predicated investigations. (See the *Intelligence Program Policy Guide* (1170PG), for specific requirements.)

(U//~~FOUO~~) Requirements which fall into the second category are known as Positive Foreign Intelligence (PFI) Collection Requirements and may only be addressed under the authorities described in this section. Type 6 Assessments opened for the purpose of determining whether a field office has the ability to collect on a PFI Collection Requirement (See DIOG Section 5.6.3.5), and Full Investigations opened for the specific purpose of collecting on PFI Collection Requirements must be predicated on an established PFI Collection Requirement that has been accepted and approved by the FBIHQ Directorate of Intelligence (DI) – HUMINT Operations Section (HOS), HUMINT Program Management Unit (HPMU) Unit Chief (UC). Preliminary Investigations for the sole purpose of collecting on PFI requirements are not authorized by the *AGG-Dom*. [redacted] b7E
[redacted] A Full PFI Investigation opened for the intended purpose of collecting on PFI requirements must be approved by the HPMU UC. A Full PFI Investigation cannot be opened on oral authority.

(U//~~FOUO~~) "The general guidance of the FBI's foreign intelligence collection activities by DNI-authorized requirements does not limit the FBI's authority to conduct investigations supportable on the basis of its other authorities—to investigate federal crimes and threats to the national security—in areas in which the information sought also falls under the definition of foreign intelligence." (Attorney General's Guidelines for Domestic FBI Operations (AGG-Dom), Introduction A.3) Accordingly, the AGG-Dom authorizes the collection of foreign intelligence incidental to predicated criminal, counterintelligence, counterterrorism, cyber, and weapons of

mass destruction investigations [redacted] See DIOG Sections 5.2 and 7.5.A and B. b7E

(U//~~FOUO~~) A Full PFI Investigation can be opened based solely on a PFI Collection Requirement. The authorized purpose (the PFI Collection requirement) must exist and have been accepted by the FBI.

(U) Examples:

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

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

(U//~~FOUO~~) FBIHQ DI provides specific guidance in its *Intelligence Program Policy Guide* (1170PG) regarding FBI national collection requirements, FBI field office collection requirements, and PFI requirements.

9.2 (U) PURPOSE AND SCOPE

(U//~~FOUO~~) As stated above, foreign intelligence is "information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorists." The collection of positive foreign intelligence extends the sphere of the FBI's information-gathering activities beyond federal crimes and threats to the national security and permits the FBI to seek information regarding a broader range of matters relating to foreign powers, organizations, or persons that may be of interest to the conduct of the United States' foreign affairs. (AGG-Dom, Introduction A.3)

(U//~~FOUO~~) While employees may collect positive foreign intelligence in already opened Assessments and predicated investigations (incidental collection), this section is focused on the policies and procedures that govern opening and managing Full Investigations for the specific purpose of collecting on PFI Collection Requirements published by the DI. DIOG Section 5.6.3.5 governs opening and managing Type 6 Assessments.

9.3 (U) CIVIL LIBERTIES AND PRIVACY

(U) Because the authority to collect positive foreign intelligence pursuant to PFI Collection Requirements enables the FBI to obtain information pertinent to the United States' conduct of its foreign affairs, even if that information is not related to criminal activity or threats to the national security, the information collected may concern lawful activities. Accordingly**, the FBI must**

operate openly and consensually with an US Person (USPER), to the extent practicable, when collecting positive foreign intelligence. (AGG-Dom, Introduction A.3)

(U) The pursuit of legitimate investigative goals without infringing upon the exercise of constitutional freedoms is a challenge that the FBI meets through the application of sound judgment and discretion.

(U) No investigative activity, including the collection of positive foreign intelligence pursuant to PFI Collection Requirements, may be taken solely on the basis of rights that are protected by the First Amendment or on the race, ethnicity, gender, national origin, religion, disability, sexual orientation or gender identity of the subject or a combination of only those factors. In order to take action intentionally to collect positive foreign intelligence, an FBI employee must open a Full Investigation that is predicated on a PFI requirement.

(U) The AGG-Dom present investigators with a number of authorized investigative methods in the conduct of a Full Investigation to collect positive foreign intelligence. Considering the effect on the privacy and civil liberties of individuals and the potential to damage the reputation of individuals, some of these investigative methods are more intrusive than others. The least intrusive method if reasonable based upon the circumstances of the investigation is to be used, but the FBI must not hesitate to use any lawful method consistent with the AGG-Dom. For further explanation of the least intrusive method refer to DIOG Section 4.

(U) Moreover, when collecting positive foreign intelligence, as part of a Full Investigation predicated on a PFI requirement, the FBI must operate openly and consensually with an USPER, to the extent practicable.

(U) By emphasizing the use of the least intrusive means to collect positive foreign intelligence and by emphasizing the need to operate openly and consensually with an USPER, to the extent practicable, FBI employees can effectively execute their duties while mitigating the potential negative impact on the privacy and civil liberties of all people encountered as part of the collection. This principle is not intended to discourage FBI employees from seeking relevant and necessary positive foreign intelligence, but rather is intended to make sure FBI employees choose the least intrusive—but still reasonable based upon the circumstances of the investigation – from the available options to obtain the information.

(U) The Privacy Act may not exempt from disclosure information the FBI collects during Positive Foreign Intelligence Assessments and investigations to qualified U.S. citizens or lawfully admitted permanent residents when personally identifying information about such persons resides in those files. FBI employees should therefore be particularly vigilant about properly classifying any such information and avoiding unnecessary references to, and the documentation of, identifying information about U.S. citizens and lawfully admitted permanent residents in Positive Foreign Intelligence files.

9.4 (U) LEGAL AUTHORITY

(U) The FBI's legal authority to collect positive foreign intelligence derives from a mixture of administrative and statutory sources. (See E.O. 12333; 50 U.S.C. §§ 3001 et seq.; 50 U.S.C. §§ 1801 et seq.; 28 U.S.C. § 532 note [incorporates the Intelligence Reform and Terrorism Protection Act, P.L. 108-458 §§ 2001-2003]). In collecting positive foreign intelligence, the FBI will be guided by collection requirements issued under the authority of the DNI, including the National Intelligence Priorities Framework and the National Human Intelligence (HUMINT)

Collection Directives, or any successor directives issued under the authority of the DNI and accepted by FBIHQ DI (PFI Collection Requirements).

9.4.1 *(U) FULL INVESTIGATION ACTIVITIES*

(U//~~FOUO)~~ As discussed in Section 7 of the DIOG, the AGG-Dom cites three predication circumstances warranting a Full Investigation, one of which specifically applies to the collection of positive foreign intelligence: "The Full Investigation may obtain foreign intelligence that is responsive to a [positive] foreign intelligence requirement."

(U//~~FOUO) A~~ PFI investigation may only be commenced if the Office of the DNI has levied a foreign intelligence collection requirement on the FBI and the DI has accepted the requirement as one to which the FBI will endeavor to respond to as part of its PFI Program (i.e., PFI Collection Requirements). The FBI is authorized to open a Full Investigation to collect on a USIC intelligence requirement only if it has been accepted and designated by FBIHQ DI as a PFI Collection Requirement.

9.5 (U) GENERAL REQUIREMENTS AND FBIHQ STANDARDS FOR APPROVING THE OPENING OF POSITIVE FOREIGN INTELLIGENCE INVESTIGATIONS

9.5.1 *(U) GENERAL REQUIREMENTS AND PROGRAM RESPONSIBILITIES*

(U//~~FOUO~~) The HOS is responsible for promulgating FBI policy and oversight of the Foreign Intelligence Collection Program (FICP). HOS, HPMU will provide notice to the DOJ NSD upon the opening of a positive foreign intelligence Full Investigation. To ensure that all positive foreign intelligence collection is focused on authorized PFI Collection Requirements, only HPMU may approve the opening of a Full Investigation [redacted] Field offices must request, by EC to the appropriate HPMU Unit Chief (UC) approval to open Full Investigations to collect on PFI Collection Requirements. b7E

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

(U//~~FOUO~~) *Note:* Investigative activity must not be conducted[36] out of a control file.

9.5.2 *(U) STANDARDS FOR OPENING A FULL INVESTIGATION TO COLLECT POSITIVE FOREIGN INTELLIGENCE*

(U//~~FOUO)~~ Before opening or approving a Full Investigation for the purpose of collecting PFI, the approving official must determine whether:

A) (U//~~FOUO) T~~he FBI DI has established an PFI Collection Requirement for opening a Full Investigation;

B) (U//~~FOUO) T~~he Full Investigation is not based solely on the exercise of First Amendment rights or on the race, ethnicity, gender, national origin, religion, disability, sexual orientation, or gender identity of the subject or a combination of only such factors; and

[36] (U) Investigative methods may only be conducted out of investigative files.

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

9.6 (U) OPENING DOCUMENTATION, APPROVAL, EFFECTIVE DATE, AND FILE REVIEW

9.6.1 *(U) OPENING BY A FIELD OFFICE WITH FBIHQ HPMU UC APPROVAL OR OPENING BY FBIHQ*

(U//~~FOUO~~) The predication for a Full PFI Investigation must be documented in the opening electronic communication (EC). Indexing of the information in the opening document is mandatory. A Full PFI Investigation may not be opened on oral authority.

9.6.1.1 (U) APPROVAL TO OPEN A FULL PFI INVESTIGATION

(U//~~FOUO~~) **Opened by a Field Office or Opened by FBIHQ:** HPMU UC will approve the opening of a Full Investigation based on PFI Collection Requirements.

9.6.1.1.1 *(U) EFFECTIVE DATE*

(U//~~FOUO~~) **Opened by a Field Office or Opened by FBIHQ:** The effective date of the Full Investigation is the date the HPMU UC approves the EC by electronic signature/date generated by Sentinel.

9.6.1.2 (U) APPROVAL TO OPEN A FULL PFI INVESTIGATION INVOLVING A SENSITIVE INVESTIGATIVE MATTER (SIM)

(U//~~FOUO~~) The opening of a Full PFI Investigation involving a SIM:

9.6.1.2.1 *(U//~~FOUO~~) SIM FULL PFI INVESTIGATION OPENED BY A FIELD OFFICE*

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

[redacted] If the Full PFI Investigation involves presidential or congressional candidates or campaigns, refer to DIOG subsection 9.6.1.2.4 for additional requirements.

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

9.6.1.2.2 ***(U) SIM FULL PFI INVESTIGATION OPENED BY FBIHQ***

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

[redacted] If the Full PFI Investigation involves presidential or congressional candidates or campaigns, refer to DIOG subsection 9.6.1.2.4 for additional requirements.

(U//~~FOUO~~) The HOS must also notify DOJ/NSD, in writing (by LHM or similar documentation), as soon as practicable, but no later than 30 calendar days after the investigation was opened. [redacted] b7E

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

9.6.1.2.3 ***(U) EFFECTIVE DATE***

(U//~~FOUO~~) **Opened by a Field Office or Opened by FBIHQ:** The effective date of the Full Investigation involving a SIM is the date the HOS SC approves the EC by electronic signature/date generated by Sentinel.

9.6.1.2.4 ***(U) ADDITIONAL REQUIREMENTS FOR PRESIDENTIAL AND CONGRESSIONAL CANDIDATES AND CAMPAIGNS***

(U) In addition to the above SIM notification and approval requirements, the following requirements apply to certain predicated investigations.

(U) Notifications:

(U) All investigations regarding a declared candidate for president or vice president of the United States; a presidential campaign; a senior presidential campaign staff member or advisor[37]; a declared candidate for the US Senate or the US House of Representatives or his or her campaign; or illegal contributions, donations, or expenditures by foreign nationals to a presidential or congressional campaign require written notification to and consultation with the AAG(s) and US attorney(s) with jurisdiction over the matter. The written notification may be [redacted] b7E

(U) Approvals:

- (U//~~FOUO~~) Regarding a declared candidate for president or vice president of the United States, a presidential campaign, or a senior presidential campaign staff member or advisor; the FBI Director and the AG must approve the opening of the investigation.

[37] (U) This includes any person who has been publicly announced by a campaign as a staffer or a member of an official campaign advisory committee or group.

Under no circumstances are FBI personnel permitted to open an investigation prior to obtaining approval from the Director and AG. The Director's and AG's approval must be documented in writing to the investigative file (e.g [redacted] b7E

- (U//~~FOUO~~) Regarding a declared candidate for the US Senate or the US House of Representatives or his or her campaign; the [redacted] the opening of an FBIHQ investigation. Under no circumstances are FBI personnel permitted to open an investigation [redacted]

- (U//~~FOUO~~) Regarding any investigation into activities related to illegal contributions, donations, or expenditures by foreign nationals to a presidential or congressional campaign; the [redacted] the opening of a field office investigation, or the [redacted] the opening of an FBIHQ investigation [redacted] b7E

(U//~~FOUO~~) If any of the above matters arise after the opening of an investigation, FBI personnel may continue investigative activity but must initiate required notifications and consultations, and begin seeking required approvals within five business days of the determination that the additional requirements apply

9.6.2 *(U) PENDING INACTIVE STATUS*

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

9.6.3 *(U) NOTICE TO DOJ*

9.6.3.1 (U) FOR A FULL PFI INVESTIGATION

(U//~~FOUO~~) Notice to DOJ is required when a Full Investigation to collect information responsive to a foreign intelligence requirement is opened. Notice must be forwarded from HOS/HPMU to the DOJ NSD as soon as practicable but no later than 30 calendar days after the opening of the investigation. (AGG-Dom, Part II.B.5) For Full PFI Investigations that are a SIM, see DIOG Section 9.6.1.2 above.

9.6.4 *(U) DURATION*

(U//~~FOUO~~) A Full PFI Investigation may continue for as long as necessary until the requirement is met, or the investigation concludes they cannot satisfy the requirement.

9.6.5 *(U) FILE REVIEW*

9.6.5.1 (U) FULL INVESTIGATIONS

(U//~~FOUO~~) Supervisory file reviews of a Full PFI Investigation must be conducted at least every 90 days in accordance with DIOG Section 3.5.4. File reviews for probationary agents must be conducted at least every 60-days.

9.6.6 *(U) ANNUAL LETTERHEAD MEMORANDUM*

9.6.6.1 (U) FIELD OFFICE RESPONSIBILITY

(U//~~FOUO~~) All FO IPs must submit an annual report on each Full PFI Investigation that was open for any period of time during the previous calendar year. This report is due to FBIHQ HPMU no later than January 30th of the calendar year following each year during which a Full Investigation is open and must include the following:

A) (U//~~FOUO~~) The PFI requirement to which the investigation was responding;

B) (U//~~FOUO~~) All methods of collection used;

C) (U//~~FOUO~~) All Sensitive Investigative Matters encountered;

D) (U//~~FOUO~~) A list of all IIRs by number issued based on information collected during the investigation;

E) (U//~~FOUO~~) A summary of the PFI collected; and

F) (U//~~FOUO~~) The date the Full Investigation was opened and, if applicable, the date it was closed.

(U//~~FOUO~~) These reports should be submitted by EC. The EC must be serialized into Sentinel, as designated in the *Intelligence Program Policy Guide* (1170PG).

9.6.6.2 (U) FBIHQ RESPONSIBILITY

(U//~~FOUO~~) HPMU must compile data from each field office regarding the scope and nature of the prior year's PFI collection program. No later than April 1st of each year, the HOS/HPMU must submit a comprehensive report of all activity described above to DOJ NSD. The report must include the following information:

A) (U//~~FOUO~~) The PFI requirement to which the investigations were responding;

B) (U//~~FOUO~~) All Sensitive Investigative Matters encountered; and

C) (U//~~FOUO~~) The date all Full Investigation were opened and closed (if applicable).

9.7 (U) STANDARDS FOR OPENING OR APPROVING THE USE OF AN AUTHORIZED INVESTIGATIVE METHOD IN A FULL POSITIVE FOREIGN INTELLIGENCE INVESTIGATION

(U//~~FOUO~~) Prior to opening or approving the use of an investigative method in a Full Investigation for the purpose of collecting positive foreign intelligence pursuant to a PFI Collection Requirement, an FBI employee or approving official must determine whether:

A) (U//~~FOUO~~) The use of the particular investigative method is likely to further the authorized purpose of the Full Investigation;

B) (U//~~FOUO~~) The investigative method selected is the least intrusive method, if reasonable based upon the circumstances of the investigation and, if taken relative to an US person (USPER), the method involves open and consensual activities, to the extent practicable;

C) (U//~~FOUO~~) Open and consensual activity would likely be successful (if it would, covert non-consensual contact with an USPER may not be approved); and

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

9.8 (U) AUTHORIZED INVESTIGATIVE METHODS IN A FULL POSITIVE FOREIGN INTELLIGENCE INVESTIGATION

(U//~~FOUO~~) Prior to opening or approving the use of an investigative method, an FBI employee and approving official must apply the standards as provided in DIOG Section 9.7. With the exceptions noted below, all lawful methods may be used during a Full Investigation to collect positive foreign intelligence pursuant to PFI Collection Requirements. If actions are to be taken with respect to an USPER, the method used must be open and consensual, to the extent practicable.

(U) See DIOG Section 18 for a complete description of the following methods that may be used in Full PFI Investigations. The methods are:

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

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

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

D) (U) Online services and resources. (See Section 18.5.4)

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

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

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

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

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

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

(U//~~FOUO~~) See the classified provisions in Appendix G for additional information.

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

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

M) (U) Polygraph examinations. (Section 18.6.11)

N) (U) Undercover Operations (Section 18.6.13)

O) (U//~~FOUO~~) Pen registers and trap/trace devices for non-USPERs using FISA. (See Section 18.6.9)

P) (U) Electronic surveillance using FISA or E.O. 12333. (See Section 18.7.3)

Q) (U//~~FOUO~~) Searches – with a warrant or court order using FISA or E.O. 12333 § 2.5. The DIOG classified Appendix G provides additional information regarding certain searches. (AGG-Dom, Part V.A.12) (See Section 18.7.1)

R) (U) FISA Title VII - Acquisition of positive foreign intelligence information. (See Section 18.7.3)

S) (U//~~FOUO~~) FISA Order for business records (for records relating to a non-USPER only). (See Section 18.6.7)

9.9 (U) INVESTIGATIVE METHODS NOT AUTHORIZED DURING A FULL POSITIVE FOREIGN INTELLIGENCE INVESTIGATION

(U//~~FOUO~~) The following investigative methods are not permitted to be used for the purpose of collecting positive foreign intelligence pursuant to PFI Collection Requirements:

A) (U//~~FOUO~~) National Security Letters (15 U.S.C. §§ 1681u, 1681v; 18 U.S.C. § 2709; 12 U.S.C. § 341[a][5][A]; 50 U.S.C. § 3162). (Section 18.6.6)

B) (U//~~FOUO~~) FISA Order for business records (for records relating to an USPER). (Section 18.6.7)

C) (U//~~FOUO~~) Pen registers and trap/trace devices in conformity with FISA (on an USPER). (Section 18.6.9)

D) (U//~~FOUO~~) Pen registers and trap/trace devices in conformity with chapter 206 of 18 U.S.C. §§ 3121-3127. (Section 18.6.9)

E) (U//~~FOUO~~) Mail covers. (Section 18.6.10)

F) (U//~~FOUO~~) Grand jury subpoenas. (Section 18.6.5)

G) (U//~~FOUO~~) Administrative subpoenas. (Section 18.6.4)

H) (U//~~FOUO~~) Stored wire and electronic communications and transactional records. (Section 18.6.8)

9.10 (U) SENSITIVE INVESTIGATIVE MATTERS (SIM) IN A FULL POSITIVE FOREIGN INTELLIGENCE INVESTIGATION

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

[redacted]

9.10.1 *(U) SENSITIVE INVESTIGATIVE MATTERS (SIM)*

(U//~~FOUO~~) A SIM is an investigative matter involving the activities of a domestic public official or domestic political candidate (involving corruption or a threat to the national security), religious or domestic political organization or individual prominent in such an organization, or news media, an academic nexus, or any other matter which, in the judgment of the official authorizing an investigation, should be brought to the attention of FBIHQ and other DOJ officials. (AGG-Dom, Part VII.N.) As a matter of FBI policy, "judgment" means that the decision of the authorizing official is discretionary. DIOG Section 10 and/or the classified provisions in DIOG Appendix G [redacted] b7E

[redacted]

(U//~~FOUO~~) All Full PFI Investigations involving a SIM must be reviewed by the CDC/OGC, approved by the SAC and the HOS SC. If the Full PFI Investigation involves presidential or congressional candidates or campaigns, refer to DIOG subsection 9.6.1.2.4 for additional requirements.

9.10.2 *(U) ACADEMIC NEXUS*

(U//~~FOUO~~)

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

b7E

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

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

(U//~~FOUO~~)

b7E

9.11 (U) RETENTION OF INFORMATION

(U//~~FOUO~~) HOS must maintain a database or records systems that permits the prompt retrieval of the status of each positive foreign intelligence collection Full Investigation (open or closed), the dates of opening and closing, and the basis for the Full Investigation.

9.12 (U//~~FOUO~~) STANDARDS FOR APPROVING THE CLOSING OF A FULL POSITIVE FOREIGN INTELLIGENCE INVESTIGATION

9.12.1 *(U) STANDARDS*

(U//~~FOUO~~) At the conclusion of a Full positive foreign intelligence Investigation, each of the following items must be documented in the closing communication (EC and/or LHM):

A) (U//~~FOUO~~) A summary of the results of the investigation;

B) (U//~~FOUO~~) Whether logical and reasonable investigation was completed (i.e. the matter acquired the positive foreign intelligence information sought);

C) (U//~~FOUO~~) Whether all investigative methods initiated have been completed and/or discontinued;

D) (U//~~FOUO~~) Whether all leads set have been completed and/or discontinued;

E) (U//~~FOUO~~) Whether all evidence has been returned, destroyed or retained in accordance with evidence policy; and

F) (U//~~FOUO~~) A summary statement of the basis on which the foreign intelligence investigation will be closed, and the selection of C-4 for Administrative Closing, which includes:

1) (U//~~FOUO~~) No further investigation is warranted and/or leads have been exhausted;

2) (U//~~FOUO~~) Investigation assigned a new file number; or

3) (U//~~FOUO~~) Investigation consolidated into a new file number or an existing file number.

9.12.2 *(U) APPROVAL REQUIREMENTS*

(U//F~~OUO~~) The appropriate closing supervisor described below must review and approve the closing communication (as described in Section 9.12.1) to ensure it contains the above-required information and sufficient details of the investigation on which to base a decision to close the foreign intelligence investigation. The appropriate closing supervisors are:

9.12.2.1 (U) OPENED BY A FIELD OFFICE WITH FBIHQ APPROVAL

(U//F~~OUO~~) Closing a Full PFI Investigation opened by a field office requires a written request from the FO IP SSA and the approval of the HPMU UC.

9.12.2.2 (U) OPENED BY FBIHQ

(U//F~~OUO~~) Closing a Full PFI Investigation opened by FBIHQ requires approval from the HPMU UC and notification to the appropriate field office.

9.12.2.3 (U) SIM OPENED BY A FIELD OFFICE WITH FBIHQ APPROVAL

(U//F~~OUO~~) Closing a PFI Full Investigation opened by a field office involving a SIM requires approval from the SAC and the HOS SC. If the Full PFI Investigation involves presidential or congressional candidates or campaigns (see DIOG subsection 9.6.1.2.4), the same level of approval required to open the investigation is also required to close the investigation, (e.g. if DD approval is required to open the investigation, then the DD must also approve the closure).

9.12.2.4 (U) SIM OPENED BY FBIHQ

(U//F~~OUO~~) Closing a PFI Full Investigation opened by FBIHQ involving a SIM requires approval from the HOS SC, and written notification to the appropriate field office. If the Full PFI Investigation involves presidential or congressional candidates or campaigns (see DIOG subsection 9.6.1.2.4), the same level of approval required to open the investigation is also required to close the investigation, (e.g. if DD approval is required to open the investigation, then the DD must also approve the closure).

9.13 (U) OTHER PROGRAM SPECIFIC INVESTIGATION REQUIREMENTS

(U//F~~OUO~~) To facilitate compliance with investigative program-specific requirements, the FBI employee should consult the relevant division's PG to ascertain any program-specific requirements.

10 (U//~~FOUO~~) SENSITIVE INVESTIGATIVE MATTER (SIM) AND SENSITIVE OPERATIONS REVIEW COMMITTEE (SORC)

10.1 (U) SENSITIVE INVESTIGATIVE MATTERS (SIM)

10.1.1 *(U) OVERVIEW*

(U) Certain investigative matters should be brought to the attention of FBI management and Department of Justice (DOJ) officials because of the possibility of public notoriety and sensitivity. Accordingly, Assessments and predicated investigations involving "sensitive investigative matters" have special approval and reporting requirements. In particular, if the Type 1 & 2 Assessment or predicated investigation involves presidential or congressional candidates or campaigns there are additional requirements for notification and approval, refer to DIOG subsection 10.1.4.9 for additional requirements.

10.1.2 *(U) PURPOSE, SCOPE, AND DEFINITIONS*

10.1.2.1 (U) DEFINITION OF SENSITIVE INVESTIGATIVE MATTERS (SIM)

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

(U//~~FOUO~~) The phrase ***"investigative matter involving the activities of"*** is intended to focus on the behaviors and/or activities of the subject, target, or subject matter of the Assessment or predicated investigation. The phrase is generally not intended to include a witness or victim in the Assessment or predicated investigation. This definition does not, however, prohibit a determination that the status, involvement, or impact on a particular witness or victim would make the Assessment or predicated investigation a SIM under subsection 10.1.2.2.7 below.

10.1.2.2 (U) DEFINITIONS/DESCRIPTIONS OF SIM OFFICIALS AND ENTITIES

(U) Descriptions for each of the officials and entities contained in the SIM definition are as follows:

10.1.2.2.1 *(U) DOMESTIC PUBLIC OFFICIAL*

(U//~~FOUO~~) A domestic public official is an elected official or an appointed official serving in a judicial, legislative, management, or executive-level position in a federal, state, local, or tribal government entity or political subdivision thereof. A matter involving a domestic public official is a SIM if the Assessment or predicated investigation involves corruption or a threat to the national security.

(U//~~FOUO~~) This definition is intended to exclude lower level positions and most line positions, such as a patrol officer or office secretary from the SIM category, but it does include supervisory personnel (e.g., police sergeant or lieutenant). The SIM definition also eliminates the "position of trust" language.

10.1.2.2.2 *(U) Domestic Political Candidate*

(U//~~FOUO~~) A domestic political candidate is an individual who is seeking election to, or nomination for election to, or who has authorized others to explore on his or her behalf the possibility of election to an office in a federal, state, local or tribal governmental entity or political subdivision thereof. As with domestic public officials, a matter involving a political candidate is a SIM if the Assessment or predicated investigation involves corruption or a threat to the national security.

10.1.2.2.3 *(U) Domestic Political Organization or Individual Prominent in Such an Organization*

(U//~~FOUO~~)

b7E

(U//~~FOUO~~)

(U//~~FOUO~~)

10.1.2.2.4 *(U) Religious Organization or Individual Prominent in Such an Organization*

(U//~~FOUO~~)

b7E

10.1.2.2.5 *(U) Member of the News Media or a News Organization*

(U//~~FOUO~~)

b7E

(U//F~~OUO~~)

b7E

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

(U//F~~OUO~~) If there is doubt about whether a particular person or entity should be considered part of the "news media," the doubt should be resolved in favor of considering the person or entity to be the "news media."

(U//F~~OUO~~) See *DIOG Appendix G - Classified Provisions* [links to ~~SECRET//NOFORN~~ document] for additional guidance on SIMs.

10.1.2.2.6 *(U) ACADEMIC NEXUS*

(U//F~~OUO~~)

b7E

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

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

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

(U//~~FOUO~~) b7E

10.1.2.2.7 *(U) OTHER MATTERS*

(U//~~FOUO~~) Any matter that in the judgment of the official authorizing an investigation should be brought to the attention of FBIHQ and other DOJ officials is also a SIM. As a matter of FBI policy, "judgment" means that the decision of the authorizing official is discretionary.

10.1.3 *(U) FACTORS TO CONSIDER WHEN OPENING OR APPROVING AN INVESTIGATIVE ACTIVITY INVOLVING A SIM*

(U//~~FOUO~~) In addition to the standards for approving investigative activity in Sections 5, 6, 7, 8 and 9, the following factors should be considered by (i) the FBI employee who seeks to open an Assessment or predicated investigation involving a SIM, as well as by the (ii) Chief Division Counsel (CDC) or Office of the General Counsel (OGC) when reviewing such matters, and (iii) the approving official when determining whether the Assessment or predicated investigation involving a SIM should be authorized:

A) (U//~~FOUO~~) Seriousness/severity of the violation/threat;

B) (U//~~FOUO~~) Significance of the information sought to the violation/threat;

C) (U//~~FOUO~~) Probability that the proposed course of action will be successful;

D) (U//~~FOUO~~) Risk of public exposure, and if there is such a risk, the adverse impact or the perception of the adverse impact on civil liberties and public confidence; and

E) (U//~~FOUO~~) Risk to the national security or the public welfare if the proposed course of action is not approved (i.e., risk of doing nothing).

(U//~~FOUO~~) In the context of a SIM, particular care should be taken when considering whether the planned course of action is the least intrusive method if reasonable based upon the circumstances of the investigation.

10.1.4 *(U) OPENING DOCUMENTATION, APPROVAL, NOTICE, CHANGE IN SIM STATUS, AND SENSITIVE POTENTIAL CHS OR SENSITIVE CHARACTERISTIC DESIGNATIONS IN TYPE 5 ASSESSMENTS*

(U//~~FOUO~~) b7E

(U//~~FOUO~~) In a Type 5 Assessment, if a sensitive characteristic is an aspect being used to identify individuals during the Identification Phase. See DIOG Sections 5.6.3.4.4.1 and 5.7 for guidance on "Sensitive PCHS" and "Sensitive Characteristic" designations.

(U//F~~OUO~~) The following are required approval and notification levels for investigative activities involving SIMs:

10.1.4.1 (U) Review and Approval of SIM Assessments By A Field Office

10.1.4.1.1 *(U) Type 1 & 2 Assessments*

(U//F~~OUO~~) An agent or TFO may open a Type 1 & 2 Assessment, as described in DIOG subsection 5.6.3.1, without prior supervisory approval. A Type 1 & 2 Assessment involving a SIM must be reviewed by the CDC and approved by the special agent in charge (SAC) as soon as practicable, but no later than five business days after the opening to authorize the Assessment to continue. If the Type 1 & 2 Assessment involves presidential or congressional candidates or campaigns, refer to DIOG subsection 10.1.4.9 for additional requirements.

10.1.4.1.2 *(U) Type 3 and 4 Assessments*

(U//F~~OUO~~) An FBI employee must obtain the following review and approval to open a Type 3 and 4 Assessment as a SIM: CDC review and SAC approval. If a SIM arises after the opening of a Type 3 or 4 Assessment, the Assessment may continue, but the matter must be reviewed by the CDC and approved by the SAC as soon as practicable, but no later than five (5) business days after the SIM arises to authorize the Assessment to continue. (See DIOG Sections 5.6.3.2.4 and 5.6.3.3.4.)

10.1.4.1.3 *(U) Type 5 Assessments*

(U//F~~OUO~~) An FBI employee must obtain CDC review and the SAC's prior approval to open a Type 5 Assessment on a sensitive potential confidential human source (CHS) in the evaluation/recruitment phase, or if a sensitive characteristic is being used as an aspect to identify individuals in the identification phase. If it is determined after the opening of a Type 5 Assessment that the individual is a sensitive PCHS, the Assessment may continue, but the matter must be approved by the SAC as soon as practicable, but no later than five (5) business days after this determination is made to authorize the Assessment to continue.

(U//F~~OUO~~) See DIOG Sections 5.6.3.4.4.1 and 5.7 for guidance on captioning Type 5 Assessments involving a "Sensitive PCHS" or Sensitive Characteristic."

10.1.4.1.4 *(U) Type 6 Assessments*

(U//F~~OUO~~) An FBI employee must obtain the following review and approval to open a Type 6 Assessment as a SIM: CDC review, SAC approval, and HUMINT Operations Section (HOS) Section Chief (SC) approval. If the SIM arises after the opening of a Type 6 Assessment, the Assessment may continue, but the matter must be reviewed by the CDC and approved by the SAC and HOS SC as soon as practicable, but no later than five (5) business days after the SIM arises to authorize the Assessment to continue. (See DIOG Section 5.6.3.5.4)

(U//F~~OUO~~) FBIHQ must receive notice and approve all Type 6 Assessments whether or not they involve a SIM.

10.1.4.2 (U) Notice for SIM Assessments by a Field Office

(U//F~~OUO~~) Notice for SIM Assessments—There is no requirement to notify FBIHQ, DOJ, or the US attorney of the opening of an Assessment involving a SIM. (AGG-Dom, Part II.B.5.a).

However, if the Assessment has additional approval requirements because it involves a presidential or congressional candidate or campaign (see DIOG subsection 10.1.4.9), the case manager, in coordination with the FBIHQ operational unit, must provide written notification to the AAG(s) and the US attorney(s) with jurisdiction over the matter. The written notification may be in the form of an LHM or similar documentation.

10.1.4.3 (U) Review and Approval of SIM Predicated Investigations by a Field Office

10.1.4.3.1 *(U) Preliminary and Full Investigations Involving a SIM*

(U//F~~OUO~~) An agent or TFO must obtain CDC review and SAC approval of a preliminary or full investigation involving a SIM. (See DIOG subsections 6.7 and 7.7.) If the investigation involves presidential or congressional candidates or campaigns, refer to DIOG subsection 10.1.4.9 for additional requirements.

10.1.4.3.2 *(U) Enterprise Investigations Involving a SIM*

(U//F~~OUO~~) An agent or TFO must obtain CDC review, SAC approval, and SC approval of an enterprise investigation involving a SIM. (See DIOG subsection 8.6.) If the investigation involves presidential or congressional candidates or campaigns, refer to DIOG subsection 10.1.4.9 for additional requirements.

10.1.4.3.3 *(U) Positive Foreign Intelligence Full Investigations Involving a SIM*

(U//F~~OUO~~) An agent or TFO must obtain CDC review, SAC approval, and HOS SC approval of a full PFI investigation involving a SIM. (See DIOG subsection 9.6.) If the full PFI investigation involves presidential or congressional candidates or campaigns, refer to DIOG subsection 10.1.4.9 for additional requirements.

10.1.4.4 (U) Notice for SIM Predicated Investigations Opened by a Field Office

10.1.4.4.1 *(U) Notice for SIM Preliminary Investigations*

(U//F~~OUO~~) See DIOG subsection 6.7.1.1 for notice requirements.

10.1.4.4.2 *(U) Notice for SIM Full Investigations*

(U//F~~OUO~~) See DIOG subsection 7.7.1.1 for notice requirements.

10.1.4.4.3 *(U) Notice for SIM Enterprise Investigations*

(U//F~~OUO~~) See DIOG Section 8.6 for notice requirements.

10.1.4.4.4 *(U) Notice for SIM Positive Foreign Intelligence Full Investigations*

(U//F~~OUO~~) See DIOG Section 9.6 for notice requirements.

10.1.4.5 (U) REVIEW AND APPROVAL OF SIM ASSESSMENTS OPENED BY FBIHQ

10.1.4.5.1 *(U) TYPE 1 & 2 ASSESSMENTS*

(U//~~FOUO~~) An agent or TFO may open a Type 1 & 2 Assessment, as described in DIOG subsection 5.6.3.1, once the following criteria are met: prior consultation with the ADIC(s) or SAC(s) of all affected FOs, OGC review, and DD (nondelegable) approval. If the Type 1 & 2 Assessment involves presidential or congressional candidates or campaigns, refer to DIOG subsection 10.1.4.9 for additional requirements. b7E

10.1.4.5.2 *(U) TYPE 3 AND 4 ASSESSMENTS*

(U//~~FOUO~~) An FBI employee must obtain the following reviews and prior approvals to open a Type 3 or 4 SIM Assessment: OGC review and SC approval. If a SIM arises after the opening of a Type 3 or 4 Assessment, the Assessment may continue, but the matter must be reviewed by the OGC and approved by the SC as soon as practicable, but no later than five (5) business days thereafter to continue the Assessment.

10.1.4.5.3 *(U) TYPE 5 ASSESSMENTS*

(U//~~FOUO~~) An FBI employee must obtain OGC review and his/her SC's approval to open a Type 5 Assessment on a sensitive PCHS. If it is determined after the opening of a Type 5 Assessment that the individual is a sensitive PCHS, the Assessment may continue, but the matter must be approved by the employee's SC as soon as practicable, but no later than five (5) business days after this determination. (See Section 5.6.3.4.4.1)

10.1.4.5.4 *(U) TYPE 6 ASSESSMENTS*

(U//~~FOUO~~) An FBI employee must obtain the following reviews and approvals to open a Type 6 Assessment as a SIM: OGC review and SC approval. If a SIM arises after the opening of a Type 6 Assessment, the Assessment may continue, but the matter must be reviewed by OGC and approved by the SC as soon as practicable, but no later than five (5) business days thereafter to continue the Assessment. (See Section 5.6.3.5.4)

10.1.4.6 (U) NOTICE REQUIREMENTS FOR SIM ASSESSMENTS BY FBIHQ

(U//~~FOUO~~) There is no requirement to notify DOJ or the United States Attorney of the opening of an Assessment involving a SIM (including opening a sensitive PCHS.) (AGG-Dom, Part II.B.5.a.) However, if the Assessment has additional approval requirements because it involves a presidential or congressional candidate or campaign (see DIOG subsection 10.1.4.9), the case manager, in coordination with the FBIHQ operational unit, must provide written notification to the AAG(s) and the US attorney(s) with jurisdiction over the matter.

10.1.4.7 (U) REVIEW AND APPROVAL OF SIM PREDICATED INVESTIGATIONS BY FBIHQ

10.1.4.7.1 *(U) PRELIMINARY AND FULL INVESTIGATIONS INVOLVING A SIM*

(U//~~FOUO~~) b7E

[redacted] See DIOG subsections 6.7, 6.10, 7.7, and 7.10.) If the investigation involves presidential or congressional candidates or campaigns, refer to DIOG subsection 10.1.4.9 for additional requirements. b7E

10.1.4.7.2 *(U) ENTERPRISE INVESTIGATIONS INVOLVING A SIM*

(U//F~~OUO~~) An agent or TFO must first consult with the ADIC(s) or SAC(s) of all affected FOs, and must obtain OGC review, and DD (nondelegable) approval of an enterprise investigation involving a SIM. (See DIOG subsections 8.6.) If the investigation involves presidential or congressional candidates or campaigns, refer to DIOG subsection 10.1.4.9 for additional requirements.

10.1.4.7.3 *(U) POSITIVE FOREIGN INTELLIGENCE FULL INVESTIGATIONS INVOLVING A SIM*

(U//F~~OUO~~) An agent or TFO must obtain OGC review and HOS SC approval of a full PFI investigation involving a SIM. (See DIOG subsection 9.6.) If the investigation involves presidential or congressional candidates or campaigns, refer to DIOG subsection 10.1.4.9 for additional requirements.

10.1.4.8 (U) NOTICE FOR SIM PREDICATED INVESTIGATIONS OPENED BY FBIHQ

10.1.4.8.1 *(U) NOTICE FOR SIM PRELIMINARY INVESTIGATIONS*

(U//F~~OUO~~) See DIOG subsection 6.7.1.1 for notice requirements.

10.1.4.8.2 *(U) NOTICE FOR SIM FULL INVESTIGATIONS*

(U//F~~OUO~~) See DIOG subsection 7.7.1.1 for notice requirements.

10.1.4.8.3 *(U) NOTICE FOR SIM ENTERPRISE INVESTIGATIONS*

(U//~~FOUO~~) See DIOG Section 8.6 for notice requirements.

10.1.4.8.4 *(U) NOTICE FOR SIM FULL POSITIVE FOREIGN INTELLIGENCE INVESTIGATIONS*

(U//F~~OUO~~) See DIOG Section 9.6 for notice requirements.

10.1.4.9 (U) ADDITIONAL REQUIREMENTS FOR PRESIDENTIAL AND CONGRESSIONAL CANDIDATES AND CAMPAIGNS

10.1.4.9.1 *(U) ASSESSMENTS*

(U) In addition to the above SIM notification and approval requirements, the following additional requirements apply to certain Type 1 & 2 Assessments.

- (U//~~FOUO~~) Regarding a declared candidate for president or vice president of the United States, a presidential campaign, or a senior presidential campaign staff member or

advisor[38]; the DD must approve the opening of the Assessment. Under no circumstances are FBI personnel permitted to open a Type 1 & 2 Assessment prior to obtaining DD approval. The DD approval must be documented in writing to the Assessment file (e.g. [redacted] b7E

- (U//~~FOUO~~) Regarding a declared candidate for the US Senate or the US House of Representatives or his or her campaign; the [redacted] b7E the opening of an FBIHQ Assessment. Under no circumstances are FBI personnel permitted to open a Type 1 & 2 Assessment [redacted]

- (U//~~FOUO~~) Regarding any investigation into activities related to illegal contributions, donations, or expenditures by foreign nationals to a presidential or congressional campaign; the [redacted] the opening of a field office Assessment, or [redacted] the opening of an FBIHQ Assessment. The [redacted] b7E

(U//~~FOUO~~) If any of the above matters arise after the opening of a Type 1 & 2 Assessment, FBI personnel may continue investigative activity but must initiate required notifications and consultations, and begin seeking required approvals within five business days of the determination that the additional requirements apply.

10.1.4.9.2 *(U) PREDICATED INVESTIGATIONS*

(U) In addition to the above SIM notification and approval requirements, the following additional requirements apply to certain predicated investigations.

(U) Notifications:

(U) All investigations regarding a declared candidate for president or vice president of the United States; a presidential campaign; a senior presidential campaign staff member or advisor; a declared candidate for the US Senate or the US House of Representatives or his or her campaign; or illegal contributions, donations, or expenditures by foreign nationals to a presidential or congressional campaign require written notification to and consultation with the AAG(s) and US attorney(s) with jurisdiction over the matter. The written notification may be [redacted] b7E

(U) Approvals:

- (U//~~FOUO~~) Regarding a declared candidate for president or vice president of the United States, a presidential campaign, or a senior presidential campaign staff member or advisor; the FBI Director and the AG must approve the opening of the investigation. Under no circumstances are FBI personnel permitted to open an investigation prior to

[38] (U) This includes any person who has been publicly announced by a campaign as a staffer or a member of an official campaign advisory committee or group.

obtaining approval from the Director and AG. The Director's and AG's approval must be documented in writing to the investigative file (e.g.

- (U//~~FOUO~~) Regarding a declared candidate for the US Senate or the US House of Representatives or his or her campaign; the the opening of an FBIHQ investigation. Under no circumstances are FBI personnel permitted to open an investigation b7E
- (U//~~FOUO~~) Regarding any investigation into activities related to illegal contributions, donations, or expenditures by foreign nationals to a presidential or congressional campaign; the the opening of a field office investigation, or the opening of an FBIHQ investigation b7E

(U//~~FOUO~~) If any of the above matters arise after the opening of an investigation, FBI personnel may continue investigative activity but must initiate required notifications and consultations, and begin seeking required approvals within five business days of the determination that the additional requirements apply.

10.1.4.10 (U) CHANGE IN SIM STATUS

(U//~~FOUO~~) b7E

10.1.4.10.1 *(U) DOCUMENTATION*

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

A) (U//~~FOUO~~) ***In Type 1 & 2 Assessments:*** Update the Guardian FD-71a b7E The update must be approved by the supervisor responsible for the Assessment, reviewed by the CDC, and approved by the SAC. No notice to FBIHQ is required. If the Type 1 & 2 Assessment involves a presidential or congressional candidate or campaign (see DIOG subsection 10.1.4.9), the same level of approval required to open the Assessment is also required to change the status, (e.g. if DD approval is required to open the Assessment, then the DD must also approve removing the SIM label).

B) (U//~~FOUO~~) ***In Type 3 through 6 Assessments:***

1) (U//~~FOUO~~) Opened by a Field Office - Submit an EC that must be approved by the supervisor responsible for the Assessment, reviewed by the CDC, and approved by the SAC. No notice to FBIHQ is required.

2) (U//~~FOUO~~) Opened by FBIHQ - Submit an EC that must be approved by the appropriate UC responsible for the investigation, reviewed by OGC, and approved by the SC.

C) (U//F~~OUO~~) ***Predicated Investigations:***

1) (U//~~FOUO~~) Opened by a Field Office - Submit an EC and a letterhead memorandum (LHM) or similar documentation that must be approved by the supervisor responsible for

the investigation, reviewed by the CDC, and approved by the SAC. For predicated investigations, notification must be provided to the same FBIHQ entities (appropriate unit and section) that received notice of the SIM. If the Predicated Investigation involves presidential or congressional candidates or campaigns (see DIOG subsection 10.1.4.9), the same level of approval required to open the investigation is also required to change the status, (e.g. if DD approval is required to open the Assessment, then the DD must also approve removing the SIM label).

2) (U//F~~OUO~~) Opened by FBIHQ - Submit an EC and an LHM or similar documentation that must be approved by the appropriate UC responsible for the investigation, reviewed by OGC, and approved by the SC. If the Predicated Investigation involves presidential or congressional candidates or campaigns (see DIOG subsection 10.1.4.9), the same level of approval required to open the investigation is also required to change the status, (e.g. if DD approval is required to open the Assessment, then the DD must also approve removing the SIM label).

D) (U//F~~OUO~~) ***Enterprise Investigations:***

1) (U//F~~OUO~~) Opened by a Field Office - Submit an EC and an LHM or similar documentation that must be approved by the supervisor responsible for the investigation, reviewed by the CDC, and approved by the SAC and the appropriate SC. If the Enterprise Investigation involves presidential or congressional candidates or campaigns (see DIOG subsection 10.1.4.9), the same level of approval required to open the investigation is also required to change the status, (e.g. if DD approval is required to open the Assessment, then the DD must also approve removing the SIM label).

2) (U//F~~OUO~~) Opened by FBIHQ - Submit an EC and an LHM or similar documentation that must be approved by the appropriate UC responsible for the investigation, reviewed by OGC, and approved by the SC. If the Enterprise Investigation involves presidential or congressional candidates or campaigns (see DIOG subsection 10.1.4.9), the same level of approval required to open the investigation is also required to change the status, (e.g. if DD approval is required to open the Assessment, then the DD must also approve removing the SIM label).

E) (U//F~~OUO~~) ***Positive Foreign Intelligence Full Investigations:***

1) (U//F~~OUO~~) Opened by a Field Office - Submit an EC that must be approved by the appropriate supervisor, reviewed by the CDC, approved by the SAC and the HOS SC. If the Full PFI Investigation involves presidential or congressional candidates or campaigns (see DIOG subsection 10.1.4.9), the same level of approval required to open the investigation is also required to change the status, (e.g. if DD approval is required to open the Assessment, then the DD must also approve removing the SIM label).

2) (U//F~~OUO~~) Opened by FBIHQ - Submit an EC that must be approved by the appropriate UC responsible for the investigation, reviewed by OGC, and approved by the HOS SC. If the Full PFI Investigation involves presidential or congressional candidates or campaigns (see DIOG subsection 10.1.4.9), the same level of approval required to open the investigation is also required to change the status, (e.g. if DD approval is required to open the Assessment, then the DD must also approve removing the SIM label).

10.1.4.11 (U) CLOSING SIM INVESTIGATIONS

10.1.4.11.1 *(U) SIM ASSESSMENTS CLOSED BY A FIELD OFFICE*

A) (U//~~FOUO~~) ***Type 1 & 2 Assessments*** - These SIM Assessments must be closed on the Guardian FD-71a with approval of the supervisor responsible for the investigation and the SAC. (See DIOG subsection 5.6.3.1.) If the Type 1 & 2 Assessment involves presidential or congressional candidates or campaigns (see DIOG subsection 10.1.4.9), the same level of approval required to open the Assessment is also required to close the investigation, (e.g. if DD approval is required to open the Assessment, then the DD must also approve the closure).

B) (U//~~FOUO~~) ***Type 3, 4, and 5 Assessments*** - The closing EC must be approved by the supervisor responsible for the investigation and the SAC. (See DIOG Section 5.6.3.2, 3, and 4)

C) (U//~~FOUO~~) ***Type 6 Assessments*** - The closing EC must be approved by the supervisor responsible for the investigation, SAC and the DI SC. (See DIOG Section 5.6.3.5)

10.1.4.11.2 *(U) SIM PREDICATED INVESTIGATIONS CLOSED BY A FIELD OFFICE*

(U//~~FOUO~~) The closing standards, approvals and notice requirements for SIM predicated investigations, including Enterprise Investigations and positive foreign intelligence Full Investigations, are specified in DIOG Sections 6.12; 7.12; 8.10; and 9.12 above.

10.1.4.11.3 *(U) SIM ASSESSMENTS CLOSED BY FBIHQ*

A) (U//~~FOUO~~) ***Type 1 & 2 Assessments*** - These SIM Assessments must be closed on the Guardian FD-71a with approval of the UC responsible for the investigation and the DD (nondelegable). If the Type 1 & 2 Assessment involves presidential or congressional candidates or campaigns (see DIOG subsection 10.1.4.9), the same level of approval required to open the Assessment is also required to close the investigation, (e.g. if DD approval is required to open the Assessment, then the DD must also approve the closure).

B) (U//~~FOUO~~) ***Type 3, 4, and 5 Assessments*** - The closing EC must be approved by the UC responsible for the investigation and his/her SC.

C) (U//~~FOUO~~) ***Type 6 Assessments*** - The closing EC must be approved by the DI UC responsible for the investigation and his/her DI SC.

10.1.4.11.4 *(U) SIM PREDICATED INVESTIGATIONS CLOSED BY FBIHQ*

(U//~~FOUO~~) The closing standards, approvals and notice requirements for SIM predicated investigations, including Enterprise Investigations and positive foreign intelligence Full Investigations, are specified in DIOG Sections 6.12; 7.12; 8.10; and 9.12 above.

10.1.5 *(U) DISTINCTION BETWEEN SIM AND SENSITIVE CIRCUMSTANCE IN UNDERCOVER OPERATIONS*

(U//~~FOUO~~) The term "sensitive investigative matter," as used in the DIOG, should not be confused with the term "sensitive circumstance," as that term is used in undercover operations. "Sensitive circumstance" relates to an undercover operation requiring FBIHQ approval. A comprehensive list of sensitive circumstances for criminal activities is contained in the Attorney General's Guidelines on FBI Undercover Operations and in Section 18 of the DIOG. The Criminal Undercover Operations Review Committee (CUORC) and the [redacted] must review and approve undercover operations that involve sensitive circumstances. The policy for undercover operations is described in DIOG

b7E

Section 18.6.13, the [redacted] b7E
[redacted] and any applicable FBIHQ operational division policy guides.

10.1.6 *(U) DISTINCTION BETWEEN SIM AND SENSITIVE UNDISCLOSED PARTICIPATION*

(U//~~FOUO~~) The term "sensitive investigative matter," as used in the DIOG, should not be confused with "sensitive UDP (undisclosed participation)." The rules regarding "sensitive investigative matter" and "sensitive UDP" (see DIOG Section 16.2.3.5), while similar, must be applied independently. The SIM designation applies to the overall investigation of which FBI and DOJ officials should be aware due to potential public notoriety and sensitivity. Sensitive UDP, on the other hand, applies to participation by employees or CHSs in lawful organizations that are designated as sensitive. Sensitive UDP can occur in either SIM or non-SIM designated investigations because sensitive UDP focuses on the activity (UDP) - not on the type of investigation in which it is taking place. Certain investigative or intelligence activity, particularly in situations involving academic institutions or student groups, may be covered by one of both these rules. The following scenarios demonstrate how these policies are to be applied:

10.1.6.1 **(U) SCENARIOS**

(U//F~~OUO~~) *Scenario 1*: [redacted]

(U//F~~OUO~~) *Response 1*: [redacted]

(U//F~~OUO~~) *Scenario 2*: [redacted] b7E

(U//F~~OUO~~) *Response 2*: [redacted]

(U//F~~OUO~~) *Scenario 3*: [redacted]

(U//~~FOUO~~) *Response 3*: [redacted]

[redacted] b7E

10.2 (U//~~FOUO~~) SENSITIVE OPERATIONS REVIEW COMMITTEE

(U//~~FOUO~~) At the request of the Director, a joint DOJ/ FBI oversight committee, the Sensitive Operations Review Committee (SORC), was established to review and monitor certain aspects of FBI investigative activities that are not within the purview of other oversight committees, particularly with regard to Assessments. The SORC is described as follows:

10.2.1 *(U) MEMBERSHIP AND STAFFING*

A) (U//~~FOUO~~) **Chair:** [redacted]

B) (U) **Members:** b7E

1) (U//~~FOUO~~) **FBI:** Assistant Directors or designated Deputy Assistant Directors for the [redacted]

2) (U//~~FOUO~~) **DOJ:** Assistant Attorneys General of the [redacted] and any other appropriate representative, given the issue being considered by the SORC.

C) (U//~~FOUO~~) **Advisors:** The Unit Chief or a designee of the FBI's Internal Policy Office (IPO) will serve as a policy advisor to the SORC. In addition, both the FBI and DOJ Chief Privacy and Civil Liberties Officer or a designee will also serve as advisors to the SORC.

D) (U//~~FOUO~~) **Staff:** The staff of the SORC shall be from the executive staffs of the Executive Assistant Directors of the NSB and the CCSB. Proposals from the NSB shall be handled by its executive staff; proposals from CCSB shall be handled by its executive staff. The staffs will be collectively referred to here as "SORC Staff." The SORC Staff is responsible for ensuring that FBI and DOJ members of the SORC have the information required to perform their SORC duties and are kept fully informed of process developments in matters reviewed by the SORC.

10.2.2 *(U) FUNCTION*

(U//~~FOUO~~) The SORC will review and provide recommendations to the Director on matters submitted, as described below.

10.2.3 *(U) REVIEW AND RECOMMENDATION*

(U//~~FOUO~~) The SORC shall review sensitive activities in the categories described below and [redacted] b7E

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

(U//~~FOUO~~)

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

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

b7E

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

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

10.2.3.1 (U) FACTORS TO CONSIDER FOR REVIEW AND RECOMMENDATION

(U//~~FOUO~~) In addition to factors unique to the proposal being considered, the SORC will consider the following in determining whether to recommend that a proposed activity be approved:

b7E

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

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

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

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

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

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

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

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

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

b7E

10.2.3.2 **(U) PROCESS FOR REVIEW AND RECOMMENDATION**

(U//~~FOUO~~)

(U//F~~OUO~~)

b7E

A) (U//F~~OUO~~) The applicable FBIHQ operational

b7E

B) (U//F~~OUO~~) Upon receipt of the EC and the proposal, the

C) (U//F~~OUO~~) prior to a scheduled SORC meeting, the SORC Staff must

D) (U//~~FOUO~~) SORC meetings are to be conducted with the expectation that

b7E

E) (U//~~FOUO~~) If there is no consensus among the SORC members

b7E

F) (U//F~~OUO~~) Once the SORC has made its recommendation, the SORC Staff

b7E

G) (U//~~FOUO~~) For each proposal, at the next SORC meeting the SORC Staff

10.2.4 *(U) EMERGENCY AUTHORIZATION*

(U//~~FOUO~~) When necessary to b7E

10.2.4.1 (U) NOTICE/OVERSIGHT FUNCTION OF SORC

(U//~~FOUO~~) To facilitate its ability to

A) (U//~~FOUO~~) In a any approval to task a

B) (U//~~FOUO~~) In a any approval to task

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

D) (U//~~FOUO~~) In an

E) (U//~~FOUO~~) In an to obtain

(U//~~FOUO~~) *Note*: falling into any of the above-listed categories must be

F) (U//~~FOUO~~) The SORC may [redacted] to provide it: b7E

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

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

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

G) (U//~~FOUO~~) The SORC must [redacted] b7E

H) (U//~~FOUO~~) [redacted] to the SORC as b7E

10.2.5 *(U) LOGISTICS*

(U//~~FOUO~~) The Executive Assistant Director for the NSB is responsible for all logistical support required for the proper functioning of the SORC (i.e., schedule meetings, provide place for meetings, draft agendas, record keeping and retention functions, all necessary communications, etc.). The IPO and the OGC will assist in establishing the logistical support required for the SORC.

11 (U) LIAISON ACTIVITIES AND TRIPWIRES

11.1 (U) OVERVIEW

(U//~~FOUO~~) FBI employees are encouraged to engage in liaison with the general public, private entities, and with local, state, federal, tribal, and foreign government agencies for the purpose of building partnerships. As part of our liaison, community outreach, or investigative/intelligence mission, FBI employees may also establish tripwires with public entities, private entities, and other governmental agencies. Liaison and tripwire activities or initiatives are mutually beneficial for the FBI and the public not only because they help build cooperative relationships and educate about suspicious activities or potential threats, but also because they encourage the public to contact the FBI should they become aware of such suspicious activities or threats.

11.2 (U) PURPOSE AND SCOPE

(U//~~FOUO~~) The FBI is authorized to engage in liaison and tripwire activities. The procedures for liaison and setting tripwires, together with documentation and requirements for an Assessment or predicated investigation, are set forth below.

11.3 (U) APPROVAL REQUIREMENTS FOR LIAISON AND TRIPWIRES

(U//~~FOUO~~) Conducting liaison and tripwire activities or initiatives do not require approval or the opening of an Assessment or predicated investigation unless they use an investigative method set forth in DIOG Sections 18.5 – 18.7. Liaison and tripwire activities or initiatives may be conducted as part of an already-opened Assessment or predicated investigation.

11.3.1 *(U) SCENARIO 1*

(U//~~FOUO~~) An FBI employee makes contact with a chemical supply company to introduce himself/herself and educate the owner about the Bureau's investigative focus on the illegal use of precursor chemicals to make improvised explosive devices. The employee advises the owner to contact the FBI if he/she observes any unusual or suspicious purchases of certain precursor chemicals.

(U//~~FOUO~~) *Response:* Such a contact would not require approval or the opening of an Assessment or predicated investigation because no investigative methods are used to conduct this activity.

11.3.2 *(U) SCENARIO 2*

(U//~~FOUO~~)

b7E

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

11.4 (U) DOCUMENTATION & RECORDS RETENTION REQUIREMENTS

(U//~~FOUO~~) The terms "liaison" and "tripwire" have been defined in various ways and may differ by FBIHQ division, program, or field office. Not every contact with a member of the public will be considered liaison or tripwire activity that needs to be documented. As stated above, employees are encouraged to engage and converse with the public as part of their routine FBI investigative and intelligence mission.

(U//~~FOUO~~) Often, however, these terms are used and/or defined in a formal policy or EC to accomplish a particular investigative or intelligence objective. When an employee is directed by a supervisor, FBI policy, or a FBIHQ division to establish a liaison relationship or through an overarching tripwire initiative, acquire information or intelligence from a tripwire, that directive, as well as the actions taken by the employee, must be documented. If an employee on his or her own initiative contacts a member of the public and subsequently determines the contact was a liaison or tripwire activity, the contact must be documented using the FD-999. Any questions regarding whether the employee's contact with the public should be documented as liaison or tripwire activities should be directed to the employee's supervisor. The intent of this section is to ensure that contacts with the public which are considered to be liaison or tripwire activities be documented with the FD-999 into a single database system for tracking and reporting purposes.

(U//~~FOUO~~) When the FD-999 is used to document liaison or tripwire activities, the FD-999 must be filed pursuant to either A or B below and must be serialized [redacted] b7E

A) (U//~~FOUO~~) **No Investigative Methods Used:** If no investigative methods (DIOG Sections 18.5 - 18.7) are used in the liaison activity or tripwire, the FD-999 may be serialized into an investigative file, intelligence file, control file, or into case number 319X-HQ-A1487718-[Division sub-file name].

B) (U//~~FOUO~~) **Investigative Methods Used:** If investigative methods (DIOG Sections 18.5-18.7) are used in the liaison activity or tripwire, the FD-999 must be serialized into 319X-HQ-A1487718-[Division sub-file name] and also be serialized in one of the following:

1) (U//~~FOUO~~) an Assessment file;
2) (U//~~FOUO~~) a predicated investigation file;
3) (U//~~FOUO~~) a domestic police cooperation file (343 classification);
4) (U//~~FOUO~~) a foreign police cooperation file (163 classification); or
5) (U//~~FOUO~~) a technical assistance control file (if only technical assistance is provided).

12 (U) ASSISTANCE TO OTHER AGENCIES

12.1 (U) OVERVIEW

(U//~~FOUO~~) Part III of the *AGG-Dom* authorizes the FBI to conduct investigations in order to detect or obtain information about, and prevent and protect against, federal crimes and threats to the national security and to collect foreign intelligence. (See DIOG Section 2.) Section 12 does not apply to assistance the FBI may provide to other agencies while conducting joint investigations. In such instances, other sections of the DIOG dealing with Assessments and predicated investigations would apply. (See DIOG Section 2.12)

(U//~~FOUO~~) Section 12 specifically addresses those situations in which the FBI has been requested or is seeking to provide assistance to other agencies and does not have an open substantive Assessment or predicated investigation (*Note:* file classifications related to providing assistance using the 343 or 163 file classification series fall within the scope of this Section). Part III of the AGG-Dom, Assistance to Other Agencies, authorizes the FBI to provide investigative assistance to other federal, state, local or tribal, or foreign agencies when the investigation has the same objectives as Part II of the AGG-Dom or when the investigative assistance is otherwise legally authorized. Accordingly, FBI employees may provide assistance even if it is not for one of the purposes identified as grounds for an FBI investigation or Assessment if providing the assistance is otherwise authorized by law. For example, investigative assistance is legally authorized in certain contexts to state or local agencies in the investigation of crimes under state or local law, as provided in 28 U.S.C. § 530C(b)(1)(M)(i)—violent acts and shootings occurring in a "place of public use;" 28 U.S.C. § 540—felonious killing of state and local law enforcement officer; 28 U.S.C. § 540A—violent crime against travelers; 28 U.S.C. § 540B—serial killings, and to foreign agencies in the investigation of foreign law violations pursuant to international agreements. The FBI may use appropriate lawful methods in any authorized investigative assistance activity.

12.2 (U) PURPOSE AND SCOPE

(U) The FBI may provide investigative and technical assistance to other agencies as set forth below.

12.2.1 *(U) INVESTIGATIVE ASSISTANCE*

(U) The AGG-Dom permits FBI personnel to provide investigative assistance to:

A) (U) Authorized intelligence activities of other United States Intelligence Community (USIC) agencies;

B) (U) Any federal agency in the investigation of federal crimes, threats to the national security, foreign intelligence collection, or any other purpose that may be lawfully authorized;

C) (U) Assist the President in determining whether to use the armed forces pursuant to 10 U.S.C. §§ 251-53, when authorized by Department of Justice (DOJ), as described in Section 12.3.2.2.1.1, below;

D) (U) Collect information necessary to facilitate public demonstrations and to protect the exercise of First Amendment rights and ensure public health and safety, when authorized by DOJ and done in accordance with the restrictions described in Section 12.3.2.2.1.2, below;

E) (U) State or local agencies in the investigation of crimes under state or local law when authorized by federal law (e.g., 28 U.S.C. §§ 540—felonious killing of state and local law enforcement officer; 540A—violent crime against travelers; 540B—serial killings);

F) (U) State, local, or tribal agencies in the investigation of matters that may involve federal crimes or threats to national security, or for such other purposes as may be legally authorized;

G) (U) Foreign agencies in the investigations of foreign law violations pursuant to international agreements, and as otherwise set forth below, consistent with the interests of the United States (including national security interests) and with due consideration of the effect on any US Person (USPER); and

H) (U) The Attorney General has also authorized the FBI to provide law enforcement assistance to state or local law enforcement agencies when such assistance is requested by the governor of the state pursuant to 42 U.S.C. § 10501 (for example, federal law enforcement assistance following Hurricane Katrina). The Attorney General must approve any request for assistance under 42 U.S.C. § 10501.

(U) The procedures for providing investigative assistance, together with the standards, approval, notification, documentation, and dissemination requirements are set forth in Sections 12.3, 12.5, and 12.6 below.

12.2.2 *(U) TECHNICAL ASSISTANCE*

(U) The FBI is authorized to provide technical assistance to all duly constituted law enforcement agencies, other organizational units of the DOJ, and other federal agencies and to foreign governments (to the extent not prohibited by law or regulation). The procedures for providing technical assistance, together with the approval, notification, documentation, and dissemination requirements are set forth in Sections 12.4, 12.5 and 12.6 below.

12.3 (U) INVESTIGATIVE ASSISTANCE TO OTHER AGENCIES - STANDARDS, APPROVALS AND NOTICE REQUIREMENTS

(U) The FBI may provide investigative assistance to other agencies by participating in joint operations and investigative activities with such agencies. (AGG-Dom, Part III.E.1)

(U//~~FOUO~~) Dissemination of information to other agencies must be consistent with Director of National Intelligence (DNI) directives, the AGG-Dom, DIOG Section 14, *Foreign Dissemination of Information Policy Guide* (1015PG), the Privacy Act of 1974, and any applicable memoranda of understanding/agreement (MOU/MOA), laws, treaties or other policies. (See Sections 12.5 and 12.6 below for documentation and dissemination of information requirements.)

12.3.1 *(U) STANDARDS FOR PROVIDING INVESTIGATIVE ASSISTANCE TO OTHER AGENCIES*

(U//~~FOUO~~) The determination whether to provide FBI assistance to other agencies is discretionary but may only occur if:

A) (U//~~FOUO~~) The assistance is within the scope authorized by the AGG-Dom, federal laws, regulations, or other legal authorities;

B) (U//~~FOUO~~) The investigation being assisted is not based solely on the exercise of First Amendment rights or on the race, ethnicity, gender, national origin, religion, disability, sexual orientation, or gender identity of the subject or a combination of only these factors; and

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

12.3.2 *(U) AUTHORITY, APPROVAL AND NOTICE REQUIREMENTS FOR PROVIDING INVESTIGATIVE ASSISTANCE TO OTHER AGENCIES*

(U//~~FOUO~~) Investigative assistance that may be furnished to other agencies is described below by agency type.

12.3.2.1 (U) INVESTIGATIVE ASSISTANCE TO UNITED STATES INTELLIGENCE COMMUNITY (USIC) AGENCIES

12.3.2.1.1 *(U) AUTHORITY*

A) (U//~~FOUO~~) The FBI may provide investigative assistance (including operational support) for authorized intelligence activities of other USIC agencies. (AGG-Dom, Part III.A)

B) (U//~~FOUO~~) Investigative assistance must be in compliance with interagency MOU/MOA, if applicable. For example, specific approval and notification requirements exist for assisting the Central Intelligence Agency (CIA) and the Department of Defense (DOD) with domestic activities.

12.3.2.1.2 *(U) APPROVAL REQUIREMENTS*

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

B) (U//~~FOUO~~) ***Sensitive Investigative Matters (SIM):*** Any investigative assistance to other USIC agencies involving a SIM requires chief division counsel (CDC)/Office of the General Counsel (OGC) review, SAC/section chief (SC) approval, and notification, as specified in DIOG subsection 12.3.2.1.3.B. If the investigative assistance involves presidential or congressional candidates or campaigns, refer to DIOG subsections 6.7.1.2 and 7.7.1.2 for additional approval requirements.

12.3.2.1.3 *(U) NOTICE REQUIREMENTS*

A) (U//~~FOUO~~) ***General:*** Notice must be provided for the investigative activity or investigative method as specified in the DIOG or applicable MOU/MOAs.

B) (U//~~FOUO~~) ***Sensitive Investigative Matters (SIM):*** In addition to the above required approvals, any investigative assistance to USIC agencies involving a SIM requires notification to the appropriate FBI Headquarters (FBIHQ) operational unit chief (UC) and SC by electronic communication (EC) as soon as practicable, but no later than 15 calendar days after the initiation of the investigative assistance. The appropriate FBIHQ operational unit must provide notice to the DOJ Criminal Division or National Security Division (NSD) as soon as practicable, but not later than 30 calendar days after the initiation of any investigative assistance involving a SIM. If the investigative assistance involves presidential or congressional candidates or campaigns, refer to DIOG subsections 6.7.1.2 and 7.7.1.2 for additional approval requirements.

C) (U//~~FOUO~~) ***Classified Appendix:*** See *DIOG Appendix G Classified Provisions* [redacted] for additional notice requirements. b7E

12.3.2.1.4 *(U) DOCUMENTATION REQUIREMENTS*

(U//~~FOUO~~) Investigative assistance (including expert) to USIC agencies using an investigative method, other than those authorized in Assessments, must be documented with the FD-999, filed and serialized to an appropriate file as specified in Sections 12.5 and 12.6 below. Division PGs may require specific additional reporting requirements for their programs.

12.3.2.2 (U) INVESTIGATIVE ASSISTANCE TO OTHER UNITED STATES FEDERAL AGENCIES

12.3.2.2.1 *(U) AUTHORITY*

A) (U//~~FOUO~~) The FBI may provide investigative assistance to any other federal agency in the investigation of federal crimes or threats to the national security or in the collection of positive foreign intelligence. (Pursuant to DIOG Section 9, collection of positive foreign intelligence requires prior approval from the Collection Management Section (CMS), FBIHQ.) The FBI may provide investigative assistance to any federal agency for any other purpose that may be legally authorized, including investigative assistance to the United States Secret Service (USSS) in support of its protective responsibilities. (AGG-Dom, Part III.B.1) See DIOG Section 12.4 below for guidance in providing technical assistance to federal agencies.

B) (U//~~FOUO~~) Investigative assistance must be in compliance with interagency MOU/MOA, if applicable.

12.3.2.2.1.1 (U) ACTUAL OR THREATENED DOMESTIC CIVIL DISORDERS

A) (U) At the direction of the Attorney General, the Deputy Attorney General, or the Assistant Attorney General for the Criminal Division, the FBI shall collect information relating to actual or threatened civil disorders to assist the President in determining (pursuant to the authority of the President under 10 U.S.C. §§ 251-53) whether use of the armed forces or militia is required and how a decision to commit troops should be implemented. The information sought shall concern such matters as (AGG-Dom, Part III.B.2):

1) (U) The size of the actual or threatened disorder, both in number of people involved or affected and in geographic area;
2) (U) The potential for violence;
3) (U) The potential for expansion of the disorder in light of community conditions and underlying causes of the disorder;

4) (U) The relationship of the actual or threatened disorder to the enforcement of federal law or court orders and the likelihood that state or local authorities will assist in enforcing those laws or orders; and

5) (U) The extent of state or local resources available to handle the disorder.

B) (U) Civil disorder investigations will be authorized only for a period of 30 days, but the authorization may be renewed for subsequent 30 day periods.

C) (U) The only investigative methods that may be used during a civil disorder investigation are:

1) (U) Public information (See DIOG subsection 18.5.1);

2) (U) Records or information - FBI or DOJ (See DIOG subsection 18.5.2);

3) (U) Records or information - Other Federal, state, local, or tribal, or foreign governmental agency (See DIOG subsection 18.5.3);

4) (U) Online services and resources (See DIOG subsection 18.5.4);

5) (U) Interview or request information from the public or private entities (See DIOG subsection 18.5.6);

(U//F~~OUO~~) *Note:* Such interviews may only be conducted if the FBI employee identifies himself or herself as an FBI employee and accurately discloses the purpose of the interview.

6) (U) Information voluntarily provided by governmental or private entities (See DIOG subsection 18.5.7); and

7) (U) Any other methods may be used only if authorized by the Attorney General, the Deputy Attorney General, or the Assistant Attorney General for the Criminal Division.

12.3.2.2.1.2 (U) PUBLIC HEALTH AND SAFETY AUTHORITIES IN RELATION TO DEMONSTRATIONS

A) (U) At the direction of the Attorney General, the Deputy Attorney General, or the Assistant Attorney General for the Criminal Division, the FBI shall collect information relating to demonstration activities that are likely to require the federal government to take action to facilitate the activities and provide public health and safety measures with respect to those activities. The information sought in such an investigation shall be that needed to facilitate an adequate federal response to ensure public health and safety and to protect the exercise of First Amendment rights, such as:

1) (U) The time, place, and type of activities planned;

2) (U) The number of persons expected to participate;

3) (U) The expected means and routes of travel for participants and expected time of arrival; and

4) (U) Any plans for lodging or housing of participants in connection with the demonstration.

B) (U) The only investigative methods that may be used in an investigation under this paragraph are:

1) (U) Public Information (See DIOG subsection 18.5.1);

2) (U) Records or information – FBI and DOJ (See DIOG subsection 18.5.2);

3) (U) Records or information – other Federal, state, local, tribal, or foreign government agencies (See DIOG subsection 18.5.3);

4) (U) Use online services and resources (See DIOG subsection 18.5.4);

5) (U) Interview or request information from the public or private entities (See DIOG subsection 18.5.6);

(U//~~FOUO~~) *Note:* Such interviews may only be conducted if the FBI employee identifies himself or herself as an FBI employee and accurately discloses the purpose of the interview;

6) (U) Accept information voluntarily provided by governmental or private entities (See DIOG subsection 18.5.7); and

7) (U) Any other methods may be used only if authorized by the Attorney General, the Deputy Attorney General, or the Assistant Attorney General for the Criminal Division.

12.3.2.2.2 ***(U) APPROVAL REQUIREMENTS***

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

B) (U//~~FOUO~~) ***Sensitive Investigative Matters (SIM):*** Any investigative assistance to other federal agencies involving a SIM requires prior CDC/OGC review and SAC/SC approval, and notification, as specified in DIOG subsection 12.3.2.2.3.B. If the investigative assistance involves presidential or congressional candidates or campaigns, refer to DIOG subsections 6.7.1.2 and 7.7.1.2 for additional approval requirements.

12.3.2.2.3 ***(U) NOTICE REQUIREMENTS***

A) (U//~~FOUO~~) ***General:*** Notice must be provided for the investigative activity or investigative method as specified in the DIOG and applicable MOU/MOAs.

B) (U//~~FOUO~~) ***Sensitive Investigative Matters (SIM):*** In addition to the above required approvals, any investigative assistance to another federal agency involving a SIM requires notification to the appropriate FBIHQ operational UC and SC by EC as soon as practicable, but no later than 15 calendar days after the initiation of the assistance. The appropriate FBIHQ operational unit must provide notice to the DOJ Criminal Division or NSD as soon as practicable, but not later than 30 calendar days after the initiation of any assistance involving a SIM. If the investigative assistance involves presidential or congressional candidates or campaigns, refer to DIOG subsections 6.7.1.2 and 7.7.1.2 for additional approval requirements.

C) (U//~~FOUO~~) ***Classified Appendix:*** See the *DIOG Appendix G - Classified Provisions* [redacted] for additional notice requirements. b7E

12.3.2.2.4 ***(U)DOCUMENTATION REQUIREMENTS***

(U//~~FOUO~~) Investigative assistance (including expert) to other Federal agencies using an investigative method, other than those authorized in Assessments, must be documented with the FD-999, filed and serialized to an appropriate file as specified in Sections 12.5 and 12.6

below. Division PGs may require specific additional reporting requirements for their programs.

12.3.2.3 (U) INVESTIGATIVE ASSISTANCE TO STATE, LOCAL, AND TRIBAL AGENCIES

(U) The FBI's authority to provide investigative assistance to state, local, and tribal law enforcement agencies has been addressed in several legal opinions by DOJ's Office of Legal Counsel (OLC). OLC's formal legal opinions are binding on the FBI and the policies herein thus conform to their written opinions.

(U) The FBI has substantial authority to assist our domestic law enforcement partners in their investigations given the broad range of federal offenses that may be investigated by the FBI.

[redacted] This authority was greatly augmented by enactment of the Investigative Assistance for Violent Crimes Act of 2012 (discussed in paragraph B below), [redacted] b7E

(U) [redacted] b7E

(U) The FBI may provide investigative assistance to state, local, and tribal agencies only in the circumstances described below.[39]

A) (U) ***Investigations Involving Possible Violations of Federal Law:*** The FBI is authorized to assist state, local and tribal agencies in the investigation of any matter that may involve federal crimes or threats to the national security, except where federal law exclusively assigns investigative responsibility to another federal agency. See DIOG Section 2.2.1 above. The authority to provide such assistance flows from the statutes and regulations that establish the FBI's jurisdiction.

(U) Thus, so long as the FBI's federal jurisdictional requirement is fulfilled, the fact that violations of state law are also present, or that local authorities are also involved in the investigation, is irrelevant. When the FBI assists state, local, or tribal authorities in the course of a federal investigation, the FBI's investigative efforts (*e.g.*, witness interviews, or execution of search or arrest warrants) [redacted] b7E

[redacted] Of course, there will often be substantial or even complete overlap between the two investigations.

(U) Investigations involving possible violations of state or local law will often involve possible violations of federal law as well, permitting the FBI to open an Assessment or predicated investigation, as appropriate, and provide investigative assistance to state

[39] (U) This section addresses the FBI's authority to provide investigative assistance. For discussion of FBI agents' authority to make warrantless arrests for non-federal felonies and violent misdemeanors committed in their presence, see Section 19.3.3 below.

and local authorities. Narcotics, carjacking, terrorism, and WMD offenses generally provide a basis for FBI assistance, as such violations almost invariably violate federal law. Other frequently encountered examples include the following:

1) (U) Shootings and other crimes committed with firearms may involve violations of the federal gun laws, e.g., 18 U.S.C. §§ 922(a)(3)-(4) (transportation across state lines), 922(g) (possession by felons, fugitives, illegal aliens, and others); and 922(q) (possession in, on the grounds of, or within 1,000 feet of a school).

2) (U) Assaults and other acts of violence resulting in death or bodily injury may constitute hate crimes under 18 U.S.C. § 249, or otherwise violate the federal civil rights laws, e.g., 18 U.S.C. § 245(b) (interference with federally protected activities).

3) (U) Armed robberies and threats of physical violence that affect commerce or the movement of articles in commerce may involve violations of the Hobbs Act, 18 U.S.C. § 1951.

4) (U) Murder and certain other state law crimes, when committed in aid of a racketeering enterprise or as part of a pattern of racketeering activity, may implicate 18 U.S.C. § 1959 (violent crimes in aid of racketeering activity) or 18 U.S.C. § 1961-1963 (RICO).

5) (U) Sex crimes against children that affect commerce or involve cross-border transportation or travel may violate the federal sex trafficking statute, 18 U.S.C. § 1591, or other federal laws protecting children against sexual exploitation and abuse, e.g., 18 U.S.C. §§ 2241(c), 2251-2252A, 2423, and 2425.

6) (U) Kidnappings violate 18 U.S.C. § 1201(a)(1) if they involve cross-border transportation or travel, and federal jurisdiction is presumed to exist 24 hours after the abduction (although the FBI may initiate an investigation sooner where there is some reasonable indication that a violation of 18 U.S.C. § 1201(a)(1) has been, or is being, committed). See 18 U.S.C. § 1201(b).

7) (U) Hostage taking may violate 18 U.S.C. § 1203(a) where there is reason to believe that one of the offenders or victims is a foreign national, or demands are made upon the U.S. Government. See 18 U.S.C. § 1203(b)(2).

8) (U) Transporting stolen vehicles and other stolen goods across state lines may violate 18 U.S.C. §§ 2311-2323.

9) (U) FBI agents are authorized to investigate state law fugitives when there is a reasonable basis to believe that doing so will detect or prevent the commission of any federal crime, including violations of the Fugitive Felons Act (FFA), 18 U.S.C. § 1073. The FFA makes it a federal crime to move in interstate or foreign commerce with intent to avoid prosecution or confinement after conviction in connection with a state felony. FBI agents have authority to pursue and arrest fugitives who, in evading arrest, manifest an intent to cross state lines (as for example, by traveling on an interstate highway or purchasing a bus or airplane ticket to another state), even if they have not yet been detected crossing state lines.

10) (U) Conspiracies to commit these and other federal offenses may violate 18 U.S.C. § 371.

(U) The FBI may continue to assist state, local and tribal authorities as long as there remains a reasonable expectation that the investigation could lead to evidence of violations of federal law [redacted] b7E

B) (U) ***Investigations of Certain Non-Federal Violations:*** At the request of an appropriate state or local law enforcement official,[40] the FBI is authorized by federal statute to assist in the investigation of the following crimes:

1) (U) Violent acts and shootings occurring in a place of public use. "Place of public use" is defined broadly as "those parts of any building, land, street, waterway, or other location that are accessible or open to members of the public, whether continuously, periodically, or occasionally," and expressly encompasses "any commercial, business, cultural, historical, educational, religious, governmental, entertainment, recreational, or similar place that is so accessible or open to the public." See Investigative Assistance for Violent Crimes Act of 2012, Pub. Law 112-265 (to be codified at 28 U.S.C. 530C(b)(1)(M)(i)) and A.G. Order 3365-2013. Investigative Assistance provided under this authority must utilize file classification 356E.

2) (U) Mass killings: defined as three or more killings in a single incident and attempted mass killings. See Investigative Assistance for Violent Crimes Act of 2012, Pub. Law 112-265 (to be codified at 28 U.S.C. 530C(b)(1)(M)(i)) and A.G. Order 3365-2013 [redacted]

3) (U) Serial killings: defined as a series of three or more killings having common characteristics. See 28 U.S.C. § 540B [redacted] b7E

4) (U) Felony killings of state and local law enforcement officers. See 28 U.S.C. § 540 [redacted]

5) (U) Felony crimes of violence against travelers: "travelers" is defined as victims who do not reside in the State where the crime occurred. See 28 U.S.C. § 540A.

[40] (U) The authorities described in paragraph B of Section 12.3.2.3 address requests for assistance by state and local officials only. Other federal law permits the FBI to conduct or assist in investigations in Indian Country. See 18 U.S.C. § 1152 (Assimilative Crimes Act) and § 1153 (Major Crimes Act); *Indian Country Policy Guide* (0321PG).

(U) Prior to conducting any investigative activity under the authority of one of the above listed federal statutes, a predicated investigation must be opened. An applicable PG can provide additional guidance on procedures to follow.

(U) FBI personnel providing assistance under the authority of one of these federal statutes may participate in the execution of state-issued process (following whatever FBI approval process is required for such participation),

b7E

See Section 19.3.3 below.

C) (U) ***Crime Emergencies and Major Disasters:*** The FBI may provide certain law enforcement assistance to states when acting pursuant to the following limited emergency authorities.

1) (U) ***Crime Emergencies:*** Under the Emergency Federal Law Enforcement Assistance provisions of the Justice Assistance Act of 1984, 42 U.S.C. § 10501 et seq. ("EFLEA"), the Attorney General may provide federal law enforcement assistance at the request of a Governor of a state during a law enforcement emergency, when state and local resources are insufficient to maintain public safety and security. Such assistance may include funds, equipment, training, intelligence information, and personnel. 42 U.S.C. § 10502(1).

2) (U) ***Major Disasters:*** Under the Robert T. Stafford Disaster Relief and Emergency Assistance Act, 42 U.S.C. §§ 5121-5208 ("Stafford Act"), the President may direct federal personnel, including federal law enforcement officers, to undertake various activities in support of state and local authorities in the event of any "major disaster."

(U) Where the Attorney General directs federal officers to assist in the enforcement of state criminal law pursuant to the EFLEA, or federal officers are properly carrying out disaster relief in a local community pursuant to a Stafford Act deployment, they should, if possible, be deputized under state law to act as state peace officers.

b7E

D) (U) ***Laboratory and Other Expert Assistance:*** The FBI is authorized to provide laboratory and certain other expert assistance to state, local, and tribal law enforcement agencies upon request, even when no federal crimes are possibly involved.

1) (U) The FBI laboratories are authorized to provide scientific assistance to all duly constituted law enforcement agencies. This authority extends to FBI field office personnel on

b7E

b7E

The FBI's authority and procedures for providing laboratory assistance are set forth in more detail in relevant policy guides and policy directives.

2) (U) In addition, for the use of Investigative Genealogy (formerly, Forensic Genetic Genealogy) when no underlying federal violation exists, the FBI may provide certain limited assistance. In this regard, field office agents or TFOs are permitted to conduct reference testing[41] (voluntary request for DNA from an innocent 3rd party), but solely to the extent the voluntary request for DNA is to assist with the genealogical buildout.

3) (U) In addition, the FBI is authorized to provide the assistance of expert personnel to support state, local, and tribal law enforcement agencies "when lives are endangered," Exec. Order 12333 § 2.6(c), provided that such assistance is either approved by the FBI GC or in accordance with written guidelines approved by the FBI GC. See *id*; A.G. Order No. 2954-2008. Thus, even when the FBI lacks any other basis of authority, FBI expert personnel may respond to requests for expert assistance by local authorities in situations involving the safety of human life

b7E

4) (U) Finally, the FBI may provide certain limited non-laboratory expert assistance pursuant to its authority to "assist in conducting, at the request of a State [or] unit of local government… local and regional training programs for the training of State and local criminal justice personnel engaged in the investigation of crime and the apprehension of criminals." 42 U.S.C. § 3771(a)(3). While such training typically takes place at

b7E

[41] (U) Reference testing is defined as overtly approaching a member of the public and soliciting their voluntary cooperation to provide a DNA samples. Investigators must seek informed consent from third parties, including a truthful disclosure of the nature of the investigation, before providing testing kits and/or instructions.

[redacted]

(U) The authority to assist in a non-federal investigation through on-the-job training is narrow. [redacted] b7E [redacted] To come within this authority, the state or local agency requesting assistance must be brought into the planning and execution of the FBI's investigative efforts, and FBI personnel must provide their state or local counterparts with a thorough briefing and/or debriefing regarding procedures and techniques being used. Moreover, where local officials are sufficiently qualified to act, the authority to provide training cannot justify FBI involvement in a violation of local law.

(U) [redacted]

12.3.2.3.1 ***(U) APPROVAL REQUIREMENTS***

A) (U) ***General:*** Requests for assistance based on Section 12.3.2.3.B.1 and 12.3.2.3.B.2 above must be approved pursuant to the FBI Director's Delegation of Authority Memorandum, dated March 14, 2013, which delegates the approval authority. This delegated authority may not be redelegated.

(U) ***Requests made to Field Offices:*** Any ADIC or SAC (non-delegable).

(U) ***Requests made to FBIHQ:*** The Deputy Director, the Associate Deputy Director, the Executive Assistant Director for the Criminal, Cyber, Response and Services Branch, the Assistant Director for the Criminal Investigations Division, the Assistant Director for the Critical Incident Response Group, the Executive Assistant Director for the National Security Branch, the Assistant Director of the Counterterrorism Division, and the Assistant Director for the Weapons of Mass Destruction Division.

(U) Requests for investigative assistance based on Section 12.3.2.3.A, or 12.3.2.3.B.3 through B.5 above, must be approved pursuant to the requirements specified in DIOG Sections 6.7 or 7.7.

(U) Request for investigative assistance based on Section 12.3.2.3.C above, must be approved by the Attorney General.

B) (U) ***Non-Laboratory Expert Assistance:*** Investigative assistance based on Section 12.3.2.3.D.3 above must be approved in accordance with approval guidelines contained in an applicable PG or Policy Directive or, if no such guidelines exist, in advance by the FBI GC, except that if the FBI GC cannot be contacted through reasonable means, emergency approval may be granted by the ADIC/SAC in the field office (or the FBIHQ SC if the request is received at FBIHQ) in accordance with this policy, with notification to the GC as soon as practicable but no later than 5 business days. If the request for investigative assistance is based on Section 12.3.2.3.D.4 above and it is not covered by an existing PG or Policy Directive, the ADIC/SAC in the field office or the FBIHQ SC, as appropriate, may approve the request in accordance with this policy, with notification to the GC as soon as practicable but no later than 5 business days.

(U) Assistance based on Section 12.3.2.3.D.1 or 12.3.2.3.D.2 must be approved pursuant to procedures and guidelines set forth in relevant Lab Division policies.

(U) Assistance based on Section 12.3.2.3.D.3 or 12.3.2.3.D.4 may be approved solely if the following conditions are met:

1) (U) The head (or designee) of the state, local or tribal law enforcement agency has submitted a written request (including by email) to the FBI that identifies the need for specific expertise from the FBI and either:

   a) (U) articulates how lives are endangered (assistance based on Section 12.3.2.3.D.3); or

   b) (U) represents that the agency does not have available employees with the needed expertise or that the employees who do have the needed expertise are not sufficiently well trained to handle the immediate situation (assistance based on Section 12.3.2.3.D.4).

   (U) *Note:* If due to the exigency of the situation there is not time for the request to be submitted in writing, the request may be made orally. Any such oral request must be followed by a written request as soon as practicable, but no later than five (5) business days.

2) (U) The CDC, who is encouraged to consult with OGC, has reviewed the request and determined in writing that 1) the requested assistance may be provided under this policy and 2) doing so will not create an unwarranted risk of civil liability to the FBI or the individual employee(s).

3) (U) The requesting agency is acting in the lawful execution of an authorized function of that organization.

4) (U) The loan of FBI personnel is an appropriate use of personnel and financial resources and does not jeopardize any ongoing FBI investigation.

12.3.2.3.2 *(U) NOTICE REQUIREMENTS*

A) (U//~~FOUO~~) General: Notice must be provided for the investigative activity or investigative method as specified in the DIOG, and applicable MOU/MOAs and/or treaties.

B) (U//~~FOUO~~) Sensitive Investigative Matters: In addition to the above required approvals, any investigative assistance provided to a state, local, or tribal law enforcement agency involving a SIM requires notification to the appropriate FBIHQ operational unit and section by EC as soon as practicable, but no later than 15 calendar days after the initiation of the assistance. The appropriate FBIHQ operational unit must provide notice to the DOJ Criminal Division or NSD as soon as practicable, but not later than 30 calendar days after the initiation of any assistance involving a sensitive investigative matter. If the investigative assistance involves presidential or congressional candidates or campaigns, refer to DIOG subsections 6.7.1.2 and 7.7.1.2 for additional requirements.

(U//~~FOUO~~) ***Classified Appendix:*** See *DIOG Appendix G - Classified Provisions* [redacted] for additional notice requirements. b7E

12.3.2.3.3 *(U) DOCUMENTATION REQUIREMENTS*

(U//~~FOUO~~) Investigative assistance (including expert) using an investigative method, other than those authorized in Assessments, must be documented with the FD-999, filed and serialized to an appropriate file as specified in Sections 12.5 and 12.6 below. Division PGs may require specific additional reporting requirements for their programs.

12.3.2.3.4 ***(U) EXAMPLES OF EXPERT ASSISTANCE IN INVESTIGATIONS OF NON-FEDERAL CRIMES***

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

(U//~~FOUO~~) **Response 1:** b7E

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

(U//~~FOUO~~) **Response 2:** b7E

(U//~~FOUO~~) b7E

b7E

(U//~~FOUO~~) **Example 3:**

(U//~~FOUO~~) **Response 3**

b7E

(U//~~FOUO~~)

12.3.2.4 **(U) INVESTIGATIVE ASSISTANCE TO FOREIGN AGENCIES**

(U//~~FOUO~~) The foundation of the FBI's international program is the Legal Attaché (LEGAT). Each LEGAT is the Director's personal representative in the foreign countries in which he/she resides or has regional responsibilities. The LEGAT's job is to respond to the FBI's domestic and foreign investigative needs. The LEGAT can accomplish this because he/she develops partnerships and fosters cooperation with his or her foreign counterparts on every level and is familiar with investigative rules, protocols, and practices that differ from country to country. This is the LEGAT's primary responsibility. As such, foreign agency requests for assistance will likely come to the FBI through the LEGAT or International Operations Division (IOD).

b7E

12.3.2.4.1 ***(U) AUTHORITIES***

A) (U//~~FOUO~~) At the request of foreign law enforcement, intelligence, or security agencies, the FBI may conduct investigations or provide assistance to investigations by such agencies, consistent with the interests of the United States (including national security interests) and with due consideration of the effect on any US person (USPER). (AGG-Dom, Part III.D.1) The FBI must follow applicable MOUs and MOAs (to include those with other US Government (USG) agencies), Mutual Legal Assistance Treaties (MLAT), Letters Rogatory, and other treaties when it provides assistance to foreign governments.

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

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

b7E

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

C) (U//~~FOUO~~) The FBI may not provide assistance to a foreign law enforcement, intelligence, or security officer conducting an investigation within the United States unless such officer has provided prior written notification to the Attorney General of his/her status as an agent of a foreign government, as required by 18 U.S.C. § 951. (AGG-Dom, Part III.D.2) The notification required by 18 U.S.C. § 951 is not applicable to diplomats, consular officers or attachés.

D) (U//~~FOUO~~) Upon the request of a foreign government agency, the FBI may conduct background inquiries concerning individuals whose consent is documented. (AGG-Dom, Part III.D.3)

12.3.2.4.2 ***(U) APPROVAL REQUIREMENTS***

A) (U//~~FOUO~~) When a request to assist a foreign agency is received from a LEGAT or IOD, and such assistance will require the use of investigative methods other than those that are authorized in Assessments, prior SSA approval must be obtained and documented as specified in 12.3.2.4.4 below.

B) (U//~~FOUO~~) If a request for assistance is received directly from a foreign law enforcement or intelligence service and is not processed through a LEGAT or IOD, written notification documenting the foreign assistance request must be provided to the appropriate LEGAT and IOD by the FD-999, an EC or Sentinel Lead Request form, and IOD must grant approval prior to providing assistance, regardless of what investigative methods are used. (See also *DIOG Appendix G - Classified Provisions* [links to SECRET//NOFORN document].)

C) (U//~~FOUO~~) The Office of International Affairs (OIA) in the DOJ's Criminal Division, has the responsibility and authority for the execution of all foreign assistance requests requiring judicial action or compulsory process. FBI IOD must coordinate all such requests with the DOJ OIA. (See DAG Memorandum, dated 5/16/2011, titled "Execution of Foreign Requests for Assistance in Criminal Cases.")

D) (U//~~FOUO)~~ Higher supervisory approvals and specific notifications may be required for assistance to foreign agencies involving joint operations, SIMs, and using particular investigative methods, as noted below and in DIOG Sections 10 and 18, and in division PGs. If the investigative assistance involves presidential or congressional candidates or campaigns, refer to DIOG subsections 6.7.1.2 and 7.7.1.2 for additional requirements.

E) (U//~~FOUO~~) Investigations and assistance conducted overseas, as well as related or official foreign travel of FBI personnel, require country clearances and notification to the Chief of Mission (COM) or designee. Such overseas investigations and assistance must adhere to the supplemental guidance in the IOD PG.

12.3.2.4.3 *(U) NOTICE REQUIREMENTS*

A) (U//~~FOUO~~) When a foreign assistance request is submitted directly to a LEGAT or IOD by a foreign agency or through an FBIHQ-authorized joint task force operation involving foreign agencies that has previously been briefed to the LEGAT, IOD has notice of the request and the FBI employee does not need IOD approval prior to providing the assistance. The FBI employee must provide IOD and the LEGAT the results of the assistance.

B) (U) The FBI must notify the DOJ NSD concerning investigation or assistance when: (i) FBIHQ's approval for the activity is required (e.g., FBIHQ approval is required to use a particular investigative method); and (ii) the activity relates to a threat to the United States national security. The FBIHQ division approving the use of the investigative method must notify DOJ NSD as soon as practicable, but no later than 30 calendar days after FBIHQ approval (see classified appendix for additional notice requirements). (AGG-Dom, Part III.D.1)

C) (U//~~FOUO~~) ***Classified Appendix:*** See the classified provisions in DIOG Appendix G for additional notice requirements.

D) (U//~~FOUO~~) ***Sensitive Investigative Matters (SIM):*** Any request for investigative assistance to a foreign agency involving a SIM requires OGC review and IOD SC approval, and notification as specified below. In addition to these approvals, any investigative assistance to a foreign agency involving a SIM requires notification to the appropriate FBIHQ operational UC and SC by EC with an LHM suitable for dissemination to DOJ as soon as practicable, but no later than 15 calendar days after the initiation of the assistance. Additionally, the appropriate IOD unit must provide notice to the DOJ Criminal Division or NSD as soon as practicable, but not later than 30 calendar days after the initiation of any assistance involving a SIM. If the investigative assistance involves presidential or congressional candidates or campaigns, refer to DIOG subsections 6.7.1.2 and 7.7.1.2 for additional requirements.

12.3.2.4.4 *(U) DOCUMENTATION REQUIREMENTS*

(U//~~FOUO~~) Investigative assistance to foreign agencies must be documented with an FD-999 and serialized to an appropriate file as specified in Sections 12.5 and 12.6 below.

12.3.2.4.5 *(U) EXAMPLES*

(U//~~FOUO~~) **Example 1:** [redacted] b7E

[redacted]

[redacted]

(U//~~FOUO~~) **Example 2:** [redacted] b7E

[redacted]

12.4 (U) TECHNICAL ASSISTANCE TO OTHER AGENCIES – STANDARDS, AUTHORITY AND APPROVAL REQUIREMENTS

(U//~~FOUO~~) Certain FBI technical assistance may be provided to certain other agencies when:

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

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

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

12.4.1 *(U) AUTHORITY*

(U//~~FOUO~~) Pursuant to 28 CFR § 0.85(g), FBI laboratories, including but not limited to, the Laboratory Division, Operational Technology Division's Digital Evidence Laboratory, and Regional Computer Forensic Laboratories, are authorized to provide technical and scientific assistance, including expert testimony in federal or local courts, to all duly constituted law enforcement agencies, other organizational units of the Department of Justice, and other federal agencies (and to certain foreign agencies, see Section 12.4.2.4 below).

(U//~~FOUO~~) Additionally, pursuant to AG Order 2954-2008, the FBI is authorized to provide reasonable technical assistance to federal, state, and local law enforcement agencies (and to certain foreign agencies, see Section 12.4.2.4 below) to assist such agencies in the lawful execution of their authorized functions.[42] Under the Order, such technical assistance includes:

A) (U) Lending or sharing equipment or property;

B) (U) Sharing facilities or services;

[42] (U) AG Order 2954-2008 addresses the FBI's authority to assist federal, state, local and foreign law enforcement agencies only. Other federal law permits the FBI to conduct or assist in investigations in Indian Country. See 18 U.S.C. § 1152 (Assimilative Crimes Act) and § 1153 (Major Crimes Act); *Indian Country Policy Guide* (0321PG).

C) (U) Collaborating in the development, manufacture, production, maintenance, improvement, distribution, or protection of technical investigative capabilities;

D) (U) Sharing or providing transmission, switching, processing, storage or other services;

E) (U) Disclosing technical designs, knowledge, information or expertise, or providing training in the same;

F) (U) Providing the assistance of expert personnel in accordance with written guidelines issued by the FBI GC or approved by the GC (See Section 12.3.2.3.D.3 above); and

G) (U) Rendering other assistance and cooperation to such agencies that is not expressly precluded by applicable law.

12.4.2 *(U) APPROVAL REQUIREMENTS*

12.4.2.1 (U) TECHNICAL ASSISTANCE TO USIC AGENCIES

(U//~~FOUO~~)

b7E

12.4.2.2 (U) TECHNICAL ASSISTANCE TO FEDERAL, STATE, LOCAL AND TRIBAL (DOMESTIC) AGENCIES REGARDING ELECTRONIC SURVEILLANCE, EQUIPMENT, AND FACILITIES

(U) Field-based technical assistance requests under this section must be approved by the field office Assistant Director in Charge (ADIC) or SAC in compliance with the *Domestic Technical Assistance Policy Directive and Policy Guide* (0554DPG) (DTA DPG). If the request for technical assistance involves equipment, facilities or property from more than one field office, each field office must approve the use of its resources.

(U) As specified below, FBIHQ senior executive officials and/or officials of the DOJ must approve a request for FBI technical assistance that involves:

A) (U)

B) (U

b7E

C) (U

D) (U) Assistance to foreign law enforcement agencies (See Section 12.4.2.4 below).

(U) The *Foreign Technical Assistance Policy Directive and Policy Guide* (0641DPG) (FTA DPG) provides additional details specifying the procedures and approval process that must be followed when the

[redacted] b7E

(U) For technical assistance to foreign law enforcement agencies see Section 12.4.2.4 and the *FTA DPG*[redacted]

12.4.2.3 (U) TECHNICAL ASSISTANCE TO FEDERAL, STATE, LOCAL AND TRIBAL (DOMESTIC) AGENCIES INVOLVING EQUIPMENT OR TECHNOLOGIES OTHER THAN ELECTRONIC SURVEILLANCE EQUIPMENT

(U) There are limited other situations in which, in the absence of a federal nexus, a domestic law enforcement agency may seek technical assistance through the short term loan of equipment from the FBI. If there is an applicable PG or policy directive, the policy and procedures contained within the PG or policy directive must be followed (for example, the *National Tactical Program Policy Guide* [1235PG]). If no PG or policy directive governs the particular equipment sought to be borrowed *and* if the loan of the equipment does not necessarily also entail the loan of personnel to use or operate the equipment, then the ADIC/SAC of the field office must approve the loan of the equipment in accordance with the following policy and procedures. If the loan of the equipment necessarily entails the loan of FBI employees, the policies governing expert assistance set forth above must also be followed.

(U) Any loan of equipment must be documented through a written agreement between the ADIC/SAC and the head of the borrowing law enforcement agency or his/her designee. At a minimum, the agreement must provide that the borrowing law enforcement agency will reimburse the FBI should the equipment be lost or damaged and that the borrowing law enforcement agency will promptly return the equipment when asked to do so by the FBI. If due to the exigency of the situation there is not time for the request to be submitted in writing, the request may be made orally but must be followed by a written agreement as soon as practicable, but not more than five (5) business days following the loan.

(U) In considering whether to lend the equipment to the federal, state, local and tribal law enforcement agency, the ADIC/SAC must take into account the following:

A) (U) The purpose for which the equipment is being requested and how the equipment will be used to advance that objective;

B) (U) The likelihood that the equipment will be damaged by the requested use;

C) (U) The likelihood that the field office will need the equipment during the proposed loan period; and

D) (U) Whether the borrowing law enforcement agency has previously violated the terms of any loan of equipment or damaged any equipment previously lent by the FBI.

(U) For technical assistance to foreign law enforcement agencies see Section 12.4.2.4 below and the *FTA DPG*.

12.4.2.4 (U) TECHNICAL ASSISTANCE TO FOREIGN AGENCIES

12.4.2.4.1 *(U) AUTHORITIES*

A) (U//~~FOUO~~) The AGG-Dom, Part III.D.4 authorizes the FBI to provide other technical assistance to foreign governments to the extent not otherwise prohibited by law.

B) (U//~~FOUO~~) AG Order 2954-2008 authorizes the FBI to provide technical assistance to foreign national security and law enforcement agencies cooperating with the FBI in the execution of the FBI's counterterrorism and counterintelligence duties and to foreign law enforcement agencies to assist such agencies in the lawful execution of their authorized functions. Requests under this section for technical assistance with respect to electronic surveillance and other OTD technologies are to be handled pursuant to the *FTA DPG* [links to SECRET//NOFORN document].

12.4.2.4.2 *(U) APPROVAL REQUIREMENTS*

(U//~~FOUO~~) Approvals of requests for technical assistance to foreign agencies are to be handled pursuant to the *FTA DPG*.

12.4.2.4.3 *(U) NOTICE REQUIREMENTS*

A) (U//~~FOUO~~) ***General:*** Notice must be provided for the investigative activity or investigative method as specified in the DIOG, and applicable MOU/MOAs and/or treaties.

B) (U//~~FOUO~~) ***Sensitive Investigative Matters (SIM):*** In addition to the above required approvals, any investigative technical assistance to the agencies listed in this section involving a SIM requires approval by the SAC (HQ assistance requires SC approval) with notification to the appropriate FBIHQ operational unit and section and appropriate OTD section by EC as soon as practicable, but no later than 15 calendar days after the initiation of the assistance. The appropriate FBIHQ operational unit must provide notice to the DOJ Criminal Division or NSD as soon as practicable, but not later than 30 calendar days after the initiation of any assistance involving a SIM. If the investigative assistance involves presidential or congressional candidates or campaigns, refer to DIOG subsections 6.7.1.2 and 7.7.1.2 for additional requirements.

C) (U//~~FOUO~~) ***Classified Appendix:*** See *DIOG Appendix G - Classified Provisions* [links to SECRET//NOFORN document] for additional notice requirements.

12.4.2.4.4 *(U) DOCUMENTATION REQUIREMENTS*

(U//~~FOUO~~) All technical assistance rendered must be documented in the appropriate Foreign Police Cooperation – Technical Assistance (163V) case classification file, and completed in accordance with standards and requirements set out in the *FTA DPG*.

12.5 (U) DOCUMENTATION REQUIREMENTS FOR INVESTIGATIVE ASSISTANCE TO OTHER AGENCIES

12.5.1 *(U) DOCUMENTATION REQUIREMENTS IN GENERAL*

(U//~~FOUO~~ b7E

(U//~~FOUO~~) When an FD-999 is used to document the "dissemination" of information to another agency, it is understood that "assistance" was provided to said agency and a separate FD-999 does not have to be completed to document the assistance to that agency (domestic or foreign).

12.5.2 *(U) Documentation Requirements for Investigative Assistance (Including Expert Assistance) to Other Agencies (Domestic or Foreign)*

(U//~~FOUO~~) ***Mandatory use of the FD-999:*** The FD-999 must be used when providing

b7E

A) (U)
B) (U)
C) (U)
D) (U)

(U//~~FOUO~~) ***Exception***

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

b7E

12.5.3 *(U) Documentation Requirements for Technical Assistance to Other Agencies (Domestic or Foreign)*

(U//~~FOUO~~) The FBI Domestic Technical Assistance PG and the FBI Foreign Technical Assistance PG provide guidance and standardized sample templates and certification documents to assist employees on the procedures for providing assistance to domestic and foreign agencies. The Domestic Police Cooperation – Technical Assistance (343V) case classification and the Foreign Police Cooperation – Technical Assistance (163V) case classification were created to maintain technical assistance documentation. Additionally, technical assistance program management related control files may be used in certain circumstances.

12.6 (U) Dissemination of Information to Other Agencies – Documentation Requirements

(U//~~FOUO~~) Dissemination of investigative or intelligence information to other agencies must be consistent with Director of National Intelligence directives, the AGG-Dom, DIOG Section 14,

b7E

the Privacy Act of 1974, and any applicable MOU/MOA, law, treaty or other policy.

(U//~~FOUO~~) Classified information may only be disseminated pursuant to applicable federal law, Presidential directive, Attorney General policy and FBI policy.

(U) The Privacy Act mandates specific documentation of any dissemination of information to an agency outside the DOJ involving a U.S. Citizen or alien lawfully admitted for permanent residence, i.e., a U.S. person (USPER).

(U//~~FOUO~~) Dissemination of information to foreign agencies must be in accordance with the [redacted] b7E

(U//~~FOUO~~) ***Mandatory use of the FD-999:*** The FD-999 must be used to document the dissemination of all unclassified or classified (up to Secret level) information to:

A) (U) USIC Agencies;

B) (U) United States Federal Agencies - when the disseminated information is related to their respective responsibilities;

C) (U) State, Local, or Tribal Agencies - when the disseminated information is related to their respective responsibilities; or

D) (U) Foreign Agencies.

(U//~~FOUO~~) *Note:* Dissemination of Top Secret or higher classified information must be documented in the appropriate classified file or the Sensitive Compartmented Information Operational Network (SCION).

(U//~~FOUO~~) ***Optional use of the FD-999:*** The FD-999 is permitted, but is not required to be used, for the dissemination of information if:

A) (U//~~FOUO~~) the information disseminated is being furnished to an agency within the DOJ with which the FBI is working a joint investigation; or

B) (U//~~FOUO~~) the information is disseminated with a document intended for dissemination such as an IIR, or through another FBI document, such as an official letter, that is maintained in an approved database that permits the prompt retrieval information in accordance with DIOG Section 12.7.1 below. For example [redacted] b7E

12.7 (U) RECORDS RETENTION REQUIREMENTS

12.7.1 *(U) SERIALIZING THE FD-999 FOR DISSEMINATION OF INFORMATION*

(U//~~FOUO~~) When using the FD-999 to document the dissemination of information pursuant to section 12.6, the FD-999 must be serialized in the file from which the information was disseminated, which may be:

A) (U) an Assessment file;

B) (U) a predicated investigation file;

C) (U) a domestic police cooperation file – 343 Classification (the new 343 file classification system replaces the former 62 classification) as described below;

D) (U) a foreign police cooperation file – 163 Classification (the revised 163 file classification system) as described below;

E) (U) a zero classification file;

F) (U) an unaddressed work file; or

G) (U) a control file using a unique file number created by the field office, LEGAT, or FBIHQ division to document the dissemination of information.

(U//~~FOUO~~) These records will assume the NARA approved retention periods approved for the file classification in which they are maintained.

12.7.2 *(U) SERIALIZING THE FD-999 FOR INVESTIGATIVE ASSISTANCE*

(U//~~FOUO~~) The AGG-DOM, Part III.E.3c mandates the FBI to maintain a database or records system to document assistance it provides to other agencies for the prompt retrieval of:

A) (U) the status of the assistance activity (opened or closed);

B) (U) the dates of opening and closing; and

C) (U) the basis for the activity.

(U//~~FOUO~~) When using the FD-999 to document investigative assistance to other agencies pursuant to section 12.5, the FD-999 must be serialized to the appropriate file, which may be:

A) (U) an Assessment file;

B) (U) a predicated investigation file;

C) (U) a domestic police cooperation file – 343 Classification (the new 343 file classification system replaces the former 62 classification) as described below;

D) (U) a foreign police cooperation file – 163 Classification (the revised 163 file classification system) as described below;

E) (U) a control file using a unique file number created by the field office, LEGAT, or FBIHQ division to document investigative assistance to another agency.

(U//~~FOUO~~) These records will assume the NARA approved retention periods approved for the file classification in which they are maintained.

12.7.3 *(U) REQUEST FOR FD-999 EXEMPTION*

(U//~~FOUO~~) An FBI component may submit to the Internal Policy Office (IPO) a written request for an exemption to any mandatory use of the FD-999, provided that the component maintains a similar database to permit the prompt retrieval of the required information. IPO, in conjunction with personnel from the Office of Integrity and Compliance (OIC) and OGC, will evaluate the exemption request to determine database compliance with the AGG-Dom and other relevant requirements. IPO will approve or deny the exemption request and will maintain a list of all approved exemptions.

12.7.4 *(U//~~FOUO~~) 343 FILE CLASSIFICATION - DOMESTIC POLICE COOPERATION FILES*

(U//F~~OUO~~) The former 62 file classification may no longer be utilized to document domestic police cooperation. The new **343** file classification system with alpha-designators must be utilized to document domestic police cooperation matters.

12.7.5 *(U//~~FOUO~~) 163 FILE CLASSIFICATION – FOREIGN POLICE COOPERATION FILES*

(U//~~FOUO~~) The 163 file classification was revised with "new" alpha-designators. The 163 file classification system must be utilized to document foreign police cooperation matters.

This Page is Intentionally Blank.

13 (U) EXTRATERRITORIAL PROVISIONS

(U) This section has been replaced by *DIOG Appendix T* [redacted] b7E

[redacted]

This Page is Intentionally Blank.

14 (U) RETENTION AND SHARING OF INFORMATION

14.1 (U) PURPOSE AND SCOPE

(U//~~FOUO~~) Every FBI component is responsible for the creation and maintenance of authentic, reliable, and trustworthy records. Without complete and accessible records, the FBI cannot conduct investigations, gather and analyze intelligence, assist with the prosecution of criminals, or perform any of its critical missions effectively.

(U//~~FOUO~~) The FBI is committed to ensuring that its records management program accomplishes the following goals:

A) (U//~~FOUO~~) Facilitates the documentation of official decisions, policies, activities, and transactions;

B) (U//~~FOUO~~) Facilitates the timely retrieval of needed information;

C) (U//~~FOUO~~) Ensures continuity of FBI business;

D) (U//~~FOUO~~) Controls the creation and growth of FBI records;

E) (U//~~FOUO~~) Reduces operating costs by managing records according to FBI business needs and by disposing of unneeded records in a timely manner;

F) (U//~~FOUO~~) Improves efficiency and productivity through effective records storage and retrieval methods;

G) (U//~~FOUO~~) Ensures compliance with applicable laws and regulations;

H) (U//~~FOUO~~) Safeguards the FBI's mission-critical information;

I) (U//~~FOUO~~) Preserves the FBI's corporate memory and history; and

J) (U//~~FOUO~~) Implements records management technologies to support all of the goals listed above.

14.2 (U) THE FBI'S RECORDS RETENTION PLAN

(U//~~FOUO~~) The FBI must retain records relating to investigative activities according to the FBI's records retention plan which, has been approved by the National Archives and Records Administration (NARA). (*AGG-Dom*, Part VI.A.1)

(U//~~FOUO~~) The FBI's records retention plan provides specific instructions about the length of time that records must be maintained. In some instances, records may be destroyed after a prescribed period of time has elapsed. Other records are never destroyed and are transferred to NARA a certain number of years after an investigation is closed. The Information Management Division has the responsibility for the disposition of the FBI's investigative records. All disposition related questions should be directed to IMD via email at [redacted] b7E

14.2.1 *(U) DATABASE OR RECORDS SYSTEM*

(U//~~FOUO~~) The FBI must maintain a database or records system that permits, with respect to each predicated investigation, the prompt retrieval of the status of the investigation (open or closed), the dates of opening and closing, and the basis for the investigation. (AGG-Dom, Part VI.A.2)

(U//~~FOUO~~) The FBI's official File Classification System covers records related to all investigative and intelligence collection activities, including Assessments. Records must be maintained in Sentinel, or other designated systems of records, which provides the required maintenance and retrieval functionality.

14.2.2 *(U) Information Management Division Disposition Plan and Retention Schedules*

(U//~~FOUO~~) All investigative records, whether from Assessments or predicated investigations, must be retained in accordance with the Information Management Division Disposition Plan and Retention Schedules (see the *Records and Information Management Policy Guide* [1223PG]). No records, including those generated during Assessments, may be destroyed or expunged earlier than the destruction schedule without written approval from NARA, except in "expungement" circumstances as further described in IMD policy. Records, including those generated during Assessments, may not be retained longer than the destruction schedule unless otherwise directed by IMD to include, "legal hold" circumstances as described in the *Legal Hold Policy* (0619D). In the event an office believes they need to retain records beyond their destruction schedule, they should contact IMD for further guidance.

14.3 (U) Information Sharing

(U//~~FOUO~~) The *National Strategy for Information Sharing and Safeguarding* provides the common vision, goals, and framework needed to guide information-sharing initiatives with our federal, state, local, and tribal agency partners; foreign government counterparts; and private sector stake holders. The FBI National Information Sharing Strategy (NISS) addresses the cultural and technological changes required to move the FBI to "a responsibility to provide" culture.

14.3.1 *(U) Permissive Sharing*

(U//~~FOUO~~) Consistent with the Privacy Act, FBI policy, and any other applicable laws and memoranda of understanding (MOU) or agreement with other agencies concerning the dissemination of information, the FBI may disseminate information obtained or produced through activities under the AGG-Dom:

A) (U//~~FOUO~~) Within the FBI and to all other components of the DOJ if the recipients need the information in the performance of their official duties.

B) (U//~~FOUO~~) To other federal agencies if disclosure is compatible with the purpose for which the information was collected and it is related to their responsibilities. In relation to other USIC agencies, the determination whether the information is related to the recipient responsibilities may be left to the recipient.

C) (U//~~FOUO~~) To state, local, or Indian tribal agencies directly engaged in the criminal justice process when access is directly related to a law enforcement (LE) function of the recipient agency.

D) (U//~~FOUO~~) To Congress or to congressional committees in coordination with the FBI Office of Congressional Affairs (OCA) and the DOJ Office of Legislative Affairs. See DIOG subsections 14.4.5 and 14.5.3.

E) (U//~~FOUO~~) To foreign agencies if the FBI determines that the information is related to their responsibilities, the dissemination is consistent with the interests of the United States (including national security interests), consideration has been given to the effect on any identifiable USPER, and disclosure is compatible with the purpose for which the information was collected. See Foreign Dissemination of FBI Information Policy Guide, 1015PG.

F) (U//~~FOUO~~) If the information is publicly available, does not identify USPERs, or is disseminated with the consent of the person whom it concerns.

G) (U//~~FOUO~~) If the dissemination is necessary to protect the safety or security of persons or property, to protect against or prevent a crime or threat to the national security, or to obtain information for the conduct of an authorized FBI investigation.

H) (U//~~FOUO~~) If dissemination of the information is otherwise permitted by the Privacy Act (5 U.S.C. § 552a) (AGG-Dom, Part VI.B.1).

(U//~~FOUO~~) All FBI-information sharing activities under this section must be done in accordance with the *FBI Information Sharing Activities with Other Government Agencies* (0012D) policy directive, the *Privacy Policy Guide* (1113PG), and any amendments thereto and applicable superseding policies. See DIOG subsections 12.6 and 12.7 for detailed documentation and records retention requirements, including the appropriate use of the FD-999.

14.3.2 *(U) REQUIRED SHARING*

(U//~~FOUO~~) The FBI must share and disseminate information as required by law and applicable policy. Working through the supervisory chain and other appropriate entities, FBI employees must ensure compliance with statutes, including the Privacy Act, treaties, executive orders (EO), Presidential directives, National Security Council (NSC) directives, Homeland Security Council (HSC) directives, Director of National Intelligence directives, Attorney General (AG)-approved policies, and MOUs or MOAs. See DIOG subsections 12.6 and 12.7 for detailed documentation and records retention requirements, including the appropriate use of the FD-999.

(U) See the following subsections for specific procedures pertaining to the required dissemination of certain urgent information:

- (U) Threat to Life (subsection 14.7)
- (U) Suspected child abuse (subsection 14.8)
- (U) Suspected abuse of the elderly or otherwise vulnerable individuals (see subsection 14.9)

(U//~~FOUO~~) For policy on required sharing of information with the White House Situation Room (WHSR) regarding critical incidents (Presidential critical information requirements), see DIOG subsection 14.10

14.3.3 *(U) INFORMATION SHARING PURSUANT TO EXECUTIVE ORDER (EO) 12333*

(U) In accordance with EO 12333, Section 2.3 and procedures approved by the Attorney General pursuant to the AGG-Dom and AGG-ET, specific types of information concerning U.S. Persons may be collected, retained and disseminated by the FBI:

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

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

(C) Information obtained in the course of a lawful foreign intelligence, counterintelligence, international drug or international terrorism investigation;

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

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

(F) Information concerning persons who are reasonably believed to be potential sources or contacts for the purpose of determining their suitability or credibility;

(G) Information arising out of a lawful personnel, physical, or communications security investigation; 3.3

(H) Information acquired by overhead reconnaissance not directed at specific United States persons;

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

(J) Information necessary for administrative purposes.

14.4 (U) INFORMATION RELATED TO CRIMINAL MATTERS

14.4.1 *(U) COORDINATING WITH PROSECUTORS*

(U//~~FOUO~~) In an investigation relating to possible criminal activity in violation of federal law, the FBI employee conducting the investigation must maintain periodic written or oral contact with the appropriate federal prosecutor, as circumstances warrant and as requested by the prosecutor. When, during such an investigation, a matter appears arguably to warrant prosecution, the FBI employee must present the relevant facts to the appropriate federal prosecutor. Information on investigations that have been closed must be available on request to a

United States Attorney (USA) or his or her designee or an appropriate DOJ official. (See AGG-Dom, Part VI.C.)

14.4.2 *(U) CRIMINAL MATTERS OUTSIDE FBI JURISDICTION*

(U//~~FOUO~~) When credible information is received by an FBI employee concerning serious criminal activity not within the FBI's investigative jurisdiction, the FBI employee must promptly transmit the information or refer the complainant to a LE agency having jurisdiction, except when disclosure would jeopardize an ongoing investigation, endanger the safety of an individual, disclose the identity of a CHS, interfere with the cooperation of a CHS, or reveal legally privileged information. If full disclosure is not made for any of the reasons indicated, then, whenever feasible, the FBI employee must make at least limited disclosure to a LE agency or agencies having jurisdiction, and full disclosure must be made as soon as the need for restricting disclosure is no longer present. Where full disclosure is not made to the appropriate LE agencies within 180 calendar days of receiving the information, the FBI employee or field office (FO) must promptly notify FBIHQ in writing of the facts and circumstances concerning the criminal activity. The FBI must make periodic reports to the deputy Attorney General (DAG) of such nondisclosures and incomplete disclosures, in a form suitable to protect the identity of a CHS. (See AGG-Dom, Part VI.C.2.)

(U//FOUO) For specific policy on the requirement to report suspected child abuse, see subsection 14.8. Special procedures for seeking authorization to temporarily delay child abuse reports are located in subsection 14.8.7.

14.4.3 *(U) REPORTING CRIMINAL ACTIVITY OF AN FBI EMPLOYEE OR CHS*

(U//~~FOUO~~) When it appears that an FBI employee has engaged in criminal activity in the course of an investigation, the FBI must notify the USAO or an appropriate DOJ division. Additionally, the activity must be reported as potential misconduct pursuant to the *Office of Professional Responsibility Policy Guide* (1168PG) and the *Self-Reporting Requirements Policy Guide* (1037PG), as applicable.

(U//~~FOUO~~) When it appears that a CHS has engaged in criminal activity in the course of an investigation, the FBI must proceed as provided in the *AGG-CHS* and the *Confidential Human Source Policy Guide* (1212PG) [links to SECRET//NOFORN document].

(U//~~FOUO~~) The reporting requirements under this subsection relating to criminal activity by an FBI employee or a CHS do not apply to otherwise illegal activity that is authorized in conformity with the AGG-Dom or other AG guidelines or to minor traffic offenses. (See AGG-Dom, Part VI.C.3.b.)

14.4.4 *(U) THE WHITE HOUSE*

(U//~~FOUO~~) Consistent with the Attorney General Memorandum "Department of Justice Communications with the White House," July 21, 2021 (DIOG Appendix D.1), the FBI does not notify the White House about pending or contemplated federal criminal or civil investigations or cases, unless doing so is important for the performance of the President's duties and appropriate from a law enforcement perspective. Only the Attorney General or Deputy Attorney General may initiate may initiate contact with the White House regarding a criminal or civil investigation. See DIOG Appendix D.

(U//~~FOUO~~) For policy on required sharing of information with the White House Situation Room (WHSR) regarding critical incidents (Presidential Critical Information Requirements), see DIOG subsection 14.10.

14.4.5 *(U) CONGRESS*

(U) DOJ policy on communications with Congress is located in DIOG Appendix D.2.

(U//~~FOUO~~) Pursuant to DIOG subsection 14.3.1.D, FBI employees permissively (i.e., without a legal or regulatory requirement to do so) sharing information with Congress or Congressional committees must first coordinate with the FBI Office of Congressional Affairs (OCA), which is responsible for coordinating with the DOJ Office of Legislative Affairs, except as explicitly authorized in policy.

(U) Policy pertaining to reporting pattern-based data mining (PBDM) to Congress is located in DIOG subsection 18.5.2.4 and the *Privacy Policy Guide* (1113PG).

(U) Policy pertaining to Congressional notice and reporting requirements for criminal pen register/trap and trace orders is located in DIOG subsection 18.6.9.9.

(U//~~FOUO~~) Policy pertaining to Title III wiretap reports (WTR) for Congress is located in DIOG subsection 18.7.2.12.8.

(U) Policy pertaining to reporting whistleblower complaints to Congress is located in the *Whistleblower Policy Directive* (0971D), or its successor.

14.5 (U) INFORMATION RELATED TO NATIONAL SECURITY AND FOREIGN INTELLIGENCE MATTERS

(U//~~FOUO~~) All information sharing with a foreign government related to classified national security and foreign intelligence must be done in accordance with the law enforcement sensitive and foreign dissemination policies [redacted] b7E

[redacted] and effective policies governing MOUs.

(U//~~FOUO~~) The general principle reflected in current law and policy is that there is a responsibility to provide information as consistently and fully as possible to agencies with relevant responsibilities to protect the United States and its people from terrorism and other threats to the national security, except as limited by specific constraints on such sharing.

(U//~~FOUO~~) The FBI's responsibility in this area includes carrying out the requirements of the MOU Between the Intelligence Community, Federal Law Enforcement Agencies, and the Department of Homeland Security Concerning Information Sharing (March 4, 2003), or any successor memorandum of understanding or agreement. Specific requirements also exist for internal coordination and consultation with other DOJ components, and for sharing national security and foreign intelligence information with White House agencies, as provided below. (AGG-Dom, Part VI.D)

14.5.1 *(U) DEPARTMENT OF JUSTICE*

(U//~~FOUO~~) The DOJ National Security Division (NSD) must have access to all information obtained by the FBI through activities relating to threats to the national security or foreign intelligence. The Director of the FBI and the Assistant Attorney General for NSD must consult concerning these activities whenever requested by either of them, and the FBI must provide such reports and information concerning these activities as the Assistant Attorney General for NSD may request. In addition to any reports or information the Assistant Attorney General for NSD may specially request under this subparagraph, the FBI must provide annual reports to the NSD concerning its foreign intelligence collection program, including information concerning the scope and nature of foreign intelligence collection activities in each FBI field office. (AGG-Dom, Part VI.D.1)

(U//~~FOUO~~) The FBI must keep the NSD apprised of all information obtained through activities under the AGG-Dom that is necessary to the ability of the United States to investigate or protect against threats to the national security; this should be accomplished with regular consultations between the FBI and the NSD to exchange advice and information relevant to addressing such threats through criminal prosecution or other means. (AGG-Dom, Part VI.D.1)

(U//~~FOUO~~) Except for counterintelligence investigations, a relevant USAO must have access to and must receive information from the FBI relating to threats to the national security, and may engage in consultations with the FBI relating to such threats, to the same extent as the NSD. The relevant USAO must receive such access and information from the FBI field offices. (AGG-Dom, Part VI.D.1)

(U//~~FOUO~~) In a counterintelligence investigation (i.e., an investigation of espionage or other intelligence activities, sabotage, or assassination, conducted by, for, or on behalf of foreign powers, organizations, or persons), the employee must follow guidance set out in the [redacted] b7E

(U//~~FOUO~~) Information shared with a USAO pursuant to DIOG Section 14.5 (National Security) must be disclosed only to the USA or any AUSA designated by the USA as points of contact to receive such information. The USA and designated AUSA must have an appropriate security clearance and must receive training in the handling of classified information and information derived from FISA, including training concerning the secure handling and storage of such information and training concerning requirements and limitations relating to the use, retention, and dissemination of such information. (AGG-Dom, Part VI.D.1)

(U//~~FOUO~~) The disclosure and sharing of information by the FBI under this paragraph is subject to any limitations required in orders issued by the FISC, controls imposed by the originators of sensitive material, and restrictions established by the Attorney General or the Deputy Attorney General in particular investigations. The disclosure and sharing of information by the FBI under this paragraph that may disclose the identity of a CHS is governed by the relevant provisions of the *AGG-CHS*. (AGG-Dom, Part VI.D.1)

14.5.2 *(U) THE WHITE HOUSE*

(U//~~FOUO~~) In order to carry out their responsibilities, the President, the Vice President, the Assistant to the President for National Security Affairs, the Assistant to the President for

Homeland Security Affairs, the NSC and its staff, the HSC and its staff, and other White House officials and offices require information from all federal agencies, including foreign intelligence, and information relating to international terrorism and other threats to the national security. Accordingly, the FBI may disseminate to the White House information regarding foreign intelligence and threats to national security information obtained through activities under the AGG-Dom, subject to the following standards and procedures.

14.5.2.1 (U) REQUESTS SENT THROUGH NSC OR HSC

(U//~~FOUO~~) The White House must request such information through the NSC staff or HSC staff including, but not limited to, the NSC Legal and Intelligence Directorates and Office of Combating Terrorism, or through the President's Intelligence Advisory Board or the Counsel to the President. (AGG-Dom, Part VI.D.2.a)

(U//~~FOUO~~) If the White House sends a request for such information to the FBI without first sending the request through the entities described above, the request must be returned to the White House for resubmission.

(U//~~FOUO~~) As described in DIOG subsection 14.10.3, SIOC employees may respond to follow-up inquiries received directly from the White House Situation Room (WHSR) pertaining to national security or foreign intelligence matters when doing so is necessary to facilitate WHSR and FBI decision-making processes during the FBI's response to a critical incident. See subsection 14.10 for requirements on critical incident information sharing with the WHSR.

14.5.2.2 (U) APPROVAL BY THE ATTORNEY GENERAL

(U//~~FOUO~~) Compromising information concerning domestic officials or domestic political organizations, or information concerning activities of USPERs intended to affect the political process in the United States, may be disseminated to the White House only with the approval of the Attorney General, based on a determination that such dissemination is needed for foreign intelligence purposes, for the purpose of protecting against international terrorism or other threats to the national security, or for the conduct of foreign affairs. Such approval is not required, however, for dissemination to the White House of information concerning efforts of foreign intelligence services to penetrate the White House or concerning contacts by White House personnel with foreign intelligence service personnel. (AGG-Dom, Part VI.D.2.b)

14.5.2.3 (U) INFORMATION SUITABLE FOR DISSEMINATION

(U//~~FOUO~~) Examples of the type of information that is suitable for dissemination to the White House on a routine basis includes, but is not limited to (AGG-Dom, Part VI.D.2.c):

A) (U//~~FOUO~~) Information concerning international terrorism;

B) (U//~~FOUO~~) Information concerning activities of foreign intelligence services in the United States;

C) (U//~~FOUO~~) Information indicative of imminent hostilities involving any foreign power;

D) (U//~~FOUO~~) Information concerning potential cyber threats to the United States or its allies;

E) (U//~~FOUO~~) Information indicative of policy positions adopted by foreign officials, governments, or powers, or their reactions to United States foreign policy initiatives;

F) (U//~~FOUO~~) Information relating to possible changes in leadership positions of foreign governments, parties, factions, or powers;

G) (U//~~FOUO~~) Information concerning foreign economic or foreign political matters that might have national security ramifications; and

H) (U//~~FOUO~~) Information set forth in regularly published national intelligence requirements.

(U//~~FOUO~~) Additionally, information related to certain critical incidents is suitable for dissemination to the White House and must be reported to the WHSR pursuant to DIOG subsection 14.10.

14.5.2.4 (U) NOTIFICATION OF COMMUNICATIONS

(U//~~FOUO~~) Communications by the FBI to the White House that relate to a national security matter and concern a litigation issue for a specific pending investigation must be made known to the Office of the Attorney General, the Office of the Deputy Attorney General, or the Office of the Associate Attorney General. White House policy may limit or prescribe the White House personnel who may request information concerning such issues from the FBI. (AGG-Dom Part VI.D.2.d)

14.5.2.5 (U) DISSEMINATION OF INFORMATION RELATING TO BACKGROUND INVESTIGATIONS

(U//~~FOUO~~) The limitations on dissemination of information by the FBI to the White House under the AGG-Dom do not apply to dissemination to the White House of information acquired in the course of an FBI investigation requested by the White House into the background of a potential employee or appointee, or responses to requests from the White House under E.O. 10450 relating to security requirements for government employment. (AGG-Dom, Part VI.D.2.e)

14.5.3 *(U) CONGRESS*

(U//~~FOUO~~) FBI employees must work through supervisors and the FBI OCA to keep the Congressional intelligence committees fully and currently informed of the FBI's intelligence activities as required by the National Security Act of 1947, as amended. Advice on what activities fall within the scope of required congressional notification can be obtained from OCA. See th[redacted]

14.6 (U) SPECIAL STATUTORY REQUIREMENTS

(U) Information acquired under the FISA may be subject to the *Foreign Intelligence Surveillance Act and Standard Minimization Procedures Policy Guide* (1303PG)[redacted] b7E
[redacted] and other requirements specified in that Act. (AGG-Dom, Part VI.D.3.a)

(U) Information obtained through the use of National Security Letters (NSLs) under 15 U.S.C. § 1681v (full credit reports) may be disseminated in conformity with the general standards of AGG-Dom, Part VI, and DIOG Section 18.6.6.3.13. Information obtained through the use of NSLs under other statutes may be disseminated in conformity with the general standards of the AGG-Dom, Part VI, subject to any specific limitations in the governing statutory provisions (see DIOG Section 18): 12 U.S.C. § 3414(a)(5)(B); 15 U.S.C. § 1681u(f); 18 U.S.C. § 2709(d); 50 U.S.C. § 3162(e). (AGG-Dom, Part VI.D.3.b)

(U) Federal Rules of Criminal Procedure (FRCP) 6(e) generally prohibits disclosing "matters occurring before the grand jury" (sometimes referred to as "core grand jury material"). Unfortunately, there is no uniform definition of matters occurring before the grand jury applicable to all FBI employees, in all field offices. Generally, information developed or requested during a federal grand jury investigation does not automatically become a matter occurring before the grand jury requiring adherence to FRCP 6(e) secrecy requirements. If an employee is unsure whether the information constitutes a matter occurring before the federal grand jury, he or she must consult with the AUSA or the DOJ attorney assigned to the investigation to determine what constitutes such material in the applicable jurisdiction. Until any question is resolved, FBI employees must treat all information obtained from a federal grand jury (FGJ) subpoena as a matter occurring before the federal grand jury, and therefore protected by the special handling, nondisclosure, and secrecy rules of the FRCP 6(e).

(U) b7E

(U)

(U) See also DIOG subsections 18.6.5.11 and 12.

14.7 (U) THREAT TO LIFE – DISSEMINATION OF INFORMATION

14.7.1 *(U) OVERVIEW*

(U//~~FOUO~~) The FBI has a responsibility to notify persons of threats to their life or threats that may result in serious bodily injury and to notify other law enforcement agencies of such threats (extracted from *DOJ Office of Investigative Agnecy Policies, Resolution 20* [December 16, 1996]). Depending on the exigency of the situation, an employee, through his or her supervisor, must notify the appropriate operational division at FBIHQ of the existence of the threat and the plan for notification. That plan may be followed unless advised to the contrary by FBIHQ.

14.7.2 *(U//~~FOUO~~) INFORMATION RECEIVED THROUGH FISA SURVEILLANCE*

(U//~~FOUO~~) If information is received through a FISA-authorized investigative technique indicating a threat to life or serious bodily harm within the scope of Section 14.7, the field office case agent responsible for that FISA must immediately coordinate the matter with the FBIHQ SSA responsible for that investigation and an NSCLB attorney from the applicable counterintelligence or counterterrorism law unit. These individuals must consult the applicable FISA minimization procedures, consider the operational posture of the investigation, and collectively determine the appropriate manner in which to proceed. FBI executive management may be consulted, as appropriate (e.g., if DIDO or declassification authority is needed). The field office case agent must document the dissemination. If the decision is made not to disseminate the threat information, that decision must be approved by an ASAC or higher and the reasons must be documented in the applicable investigative file.

14.7.3 *(U) DISSEMINATION OF INFORMATION CONCERNING THREATS AGAINST INTENDED VICTIMS (PERSONS)*

14.7.3.1 (U) WARNING TO THE INTENDED VICTIM (PERSON)

14.7.3.1.1 *(U) EXPEDITIOUS WARNINGS TO IDENTIFIABLE INTENDED VICTIMS*

(U//~~FOUO~~) Except as provided below in Sections 14.7.3.1.1.1 (Exceptions) and 14.7.3.1.2 (Custody or Protectee), when an employee has information that a person who is identified or can be identified through reasonable means (hereafter a "intended victim") is subject to a credible threat to his/her life or of serious bodily injury, the FBI employee must attempt expeditiously to warn the intended victim of the nature and extent of the threat.

14.7.3.1.1.1 (U) EXCEPTIONS TO WARNING

(U//~~FOUO~~) An employee is not required to warn an intended victim if :

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

B) (U//~~FOUO~~) the intended victim knows the nature and extent of the specific threat against him/her.

14.7.3.1.1.2 (U) MEANS, MANNER, AND DOCUMENTATION OF WARNING/NOTIFICATION OR DECISION NOT TO WARN

(U//~~FOUO~~) The FBI employee, in consultation with his or her supervisor, must determine the means and manner of the warning, using the method most likely to provide direct notice to the intended victim. In some cases, this may require the assistance of a third party. The employee must document on an FD-999 the content of the warning, as well as when, where and by whom it was delivered to the intended victim. The FD-999 must be placed in a zero file or if investigative methods are used, the appropriate investigative file.

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

(U//~~FOUO~~) The employee, in consultation with his or her supervisor, may seek the assistance of another law enforcement agency to provide the warning. If this is done, the employee must document on an FD-999 that notice was provided by that law enforcement agency, as well as when, where and by whom (i.e., the name of the other agency's representative) it was delivered. The employee must also document the other agency's agreement to provide a timely warning. The FD-999 must be filed as specified above.

(U//~~FOUO~~) Whenever time and circumstances permit, an employee's decision not to provide a warning in these circumstances must be approved by an ASAC or higher. In all cases, the reasons for not providing a warning must be documented by EC in a zero file or if investigative methods are used, the appropriate investigative file.

14.7.3.1.2 *(U) Warnings When Intended Victim is in Custody or is a Protectee*

(U//~~FOUO~~) When an employee has information that a person described below is an intended victim, the employee, in consultation with his or her supervisor, must expeditiously notify the law enforcement agency that has protective or custodial jurisdiction of the threatened person.

(U//~~FOUO~~) This section applies when the intended victim is:

A) (U//~~FOUO~~) a public official who, because of his/her official position, is provided a protective detail;

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

C) (U//~~FOUO~~) detained or incarcerated.

(U//~~FOUO~~) This paragraph does not apply to employees serving on the security detail of the FBI Director or any other FBI protected persons when the threat is to the individual they protect.

14.7.3.1.2.1 (U) Means, Manner, and Documentation of Warning/Notification

(U//~~FOUO~~) The employee, in consultation with his or her supervisor, may determine the means and manner of the notification. When providing notification, the employee must provide as much information as possible regarding the threat and the credibility of the threat. The employee must document on an FD-999 what he or she informed the other law enforcement agency, and when, where, how (e.g., telephone call, email) and to whom the notice was delivered. The FD-999 must be placed in a zero file or if investigative methods are used, the appropriate investigative file.

14.7.3.2 (U) Notification to Law Enforcement Agencies That Have Investigative Jurisdiction

14.7.3.2.1 *(U) Expeditious Notification*

14.7.3.2.1.1 (U) Threats to Intended Persons

(U//~~FOUO~~) Except as provided in Sections 14.7.3.2.2, when an employee has information that a person (other than a person described above in Section 14.7.3.1.2) who is identified or can be identified through reasonable means is subject to a credible threat

to his/her life or of serious bodily injury, the employee must attempt expeditiously to notify other law enforcement agencies that have investigative jurisdiction concerning the threat.

14.7.3.2.1.2 (U) THREATS TO OCCUPIED STRUCTURES OR CONVEYANCES

(U//~~FOUO~~) When an employee has information that a structure or conveyance which can be identified through reasonable means is the subject of a credible threat which could cause a loss of life or serious bodily injury to its occupants, the employee, in consultation with his or her supervisor, must provide expeditious notification to other law enforcement agencies that have jurisdiction concerning the threat.

14.7.3.2.2 *(U) EXCEPTIONS TO NOTIFICATION*

(U//~~FOUO~~) An employee need not attempt to notify another law enforcement agency that has investigative jurisdiction concerning a threat:

A) (U//~~FOUO~~) when providing the notification to the other law enforcement agency is likely to cause equal or greater physical harm to one or more persons; or

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

(U//~~FOUO~~) Whenever time and circumstances permit, an employee's decision not to provide notification to another law enforcement agency in the foregoing circumstances must be approved by an ASAC or higher. In all cases, the reasons for an employee's decision not to provide notification must be documented in writing in a zero file or if investigative methods are used, the appropriate investigative file.

14.7.3.2.3 *MEANS, MANNER, AND DOCUMENTATION OF NOTIFICATION*

(U//~~FOUO~~) The employee may determine the means and manner of the notification. The employee must document in writing in the applicable investigative file the content of the notification, and when, where, and to whom it was delivered.

14.7.4 *(U//~~FOUO~~) DISSEMINATION OF INFORMATION CONCERNING THREATS, POSSIBLE VIOLENCE OR DEMONSTRATIONS AGAINST FOREIGN ESTABLISHMENTS OR OFFICIALS IN THE UNITED STATES*

(U//~~FOUO~~) If information is received indicating a threat to life within the scope of Section 14.7, or possible violence or demonstrations against foreign establishments or officials in the United States, the field office case agent must immediately coordinate the matter with the FBIHQ SSA responsible for the case, who must notify the Department of State (DOS), United States Secret Service (USSS), and any other Government agencies that may have an interest. See the *Agreement Between the Federal Bureau of Investigation and the US Secret Service Concerning Protective Responsibilities* (July 1973) Section IV, and the *FBI/US Secret Service "Agreement of Procedures" Regarding Violations Involving US Secret Service Protectees that Fall Within FBI Jurisdiction* (December 1978) for the FBI's information sharing responsibilities with the USSS in such cases.

14.7.5 *(U) DISSEMINATION OF INFORMATION CONCERNING THREATS AGAINST THE PRESIDENT AND OTHER DESIGNATED OFFICIALS*

(U//~~FOUO~~) The USSS has statutory authority to protect or to engage in certain activities to protect the President and certain other persons as specified in 18 U.S.C. § 3056. An MOU between the FBI and USSS specifies the FBI information that the USSS wants to receive in connection with its protective responsibilities.

(U//~~FOUO~~) Detailed guidelines regarding threats against the President of the United States and other USSS protectees can be found in the *Violent Incident Crimes Policy Guide*, 1009PG, subsection 3.13.

14.8 (U) SUSPECTED CHILD ABUSE – DISSEMINATION OF INFORMATION

(U) This section is under development, please refer to DIOG Appendix K.

14.9 (U) SUSPECTED ABUSE OF THE ELDERLY OR OTHERWISE VULNERABLE INDIVIDUALS–DISSEMINATION OF INFORMATION

(U) This section is under development, please refer to DIOG Appendix K.

14.10 (U//~~FOUO~~) REQUIRED SHARING WITH THE WHITE HOUSE SITUATION ROOM REGARDING CRITICAL INCIDENT INFORMATION (PRESIDENTIAL CRITICAL INFORMATION REQUIREMENTS)

14.10.1 *(U) REPORTABLE EVENTS*

(U//~~FOUO~~) In accordance with National Security Presidential Memorandum 32 (NSPM-32), the FBI is obligated to report certain events to the White House Situation Room (WHSR) to ensure that the President and the Vice President (and their advisors) maintain awareness of and can effectively manage incidents and crises. The Strategic Information and Operations Center (SIOC) is the primary point of contact between the FBI and the WHSR during critical incidents.

(U//F~~OUO~~) However, consistent with the Attorney General Memorandum "Department of Justice Communications with the White House," July 21, 2021, the FBI is not obligated to notify the WHSR concerning pending or contemplated federal criminal or civil investigations or cases, unless doing so is important for the performance of the President's duties and appropriate from a law enforcement perspective. For policy pertaining to sharing information with the White House outside the context of critical incidents, see DIOG subsections 14.4.4 (for information related to criminal matters) and 14.5.2 (for information related to national security and foreign intelligence matters).

(U//~~FOUO~~) For policy on disseminating information concerning threats to life, see DIOG subsection 14.7.

14.10.1.1 (U//F~~OUO~~) TIER ONE EVENTS

(U//~~FOUO~~) Pursuant to NSPM-32, the following events are "tier one" events that the FBI is required to report to the WHSR within three hours of initial observation. To meet this requirement, FBI employees who observe credible indications of the following events during the

course of their official duties must internally report the events (as described in subsection 14.10.2) as soon as practicable but no later than three hours after initial observation.

(U) Table is U//~~FOUO~~ and sourced directly from NSPM-32.

Event	**Description**
Leadership Event	The death, incapacitation, kidnapping, or attempted assassination of Cabinet member or Agency head, or the kidnapping, assassination, or attempted assassination of a senior U.S. Government official, or credible indications that such an incident is imminent
Technology Outage	The loss of any technological capability of a U.S. Government entity (including space assets) that results in the inability to perform primary mission essential functions or to fulfill command, control, communications, or intelligence requirements
Cyber Incident	A Cyber incident affecting U.S. Government systems, including space assets, resulting in the significant degradation of mission capacity or the inability to perform primary mission essential functions, or credible indications that such an incident is imminent
Security Incident	A significant security incident at a U.S. Government facility or on U.S. Government property to the extent permitted by counterintelligence and information security concerns, including: • A confirmed active shooter or casualties due to nefarious activity • A terrorist attack or credible indications that such an incident is imminent • A suspicious package or a substance that is assessed to be an actual threat, is associated with threat indicators (e.g., bomb threat phone call, threat letter, intelligence), or generates significant media attention • A demonstration, protest, or civil disorder involving violence or significant media attention • Penetration or surveillance of government facilities or installations by actors with suspicious or nefarious intent • Security concerns related to a National Special Security Event (NSSE) or Special Event Assessment Rating (SEAR) 1 or 2 event • Emerging threat and/or enhanced security posture in the National Capital Region (NCR) as a result of domestic or foreign violent extremism or violent civil disturbance

Event	Description
Media Attention	An event that has received or is likely to receive significant national media attention and/or scrutiny directed at the U.S. Government
Alert Level Change	Either of the following: • Changes to alert/readiness/posture level of federal executive branch departments or agencies (e.g., force protection condition [FPCON], continuity of government condition [COGCON]) • Changes as reported through the Continuity Status Reporting process, specifically the relocation of key leadership and critical continuity personnel supporting COOP or COG
Flight Disturbance	Any flight over or into U.S. airspace diverted due to terrorism
Homeland Terrorist Attack	An attack within the United States that is dangerous to human life, is a violation of the criminal laws of the United States or of any state, and appears intended: • to intimidate or coerce a civilian population • to influence government policy, or • to affect the conduct of the government by mass destruction, assassination, or kidnapping. Credible indications that such an act is imminent
Weapon of Mass Destruction / Electromagnetic Pulse Incident	Any WMD incident (i.e., chemical, biological, radiological, nuclear, or explosive) or EMP incident in the United States, including credible or imminent threat of a WMD or EMP attack
Active Shooter	• A verified report of an ongoing active shooter in the United States from an official source with active law enforcement response • Any high visibility law enforcement incident or event that garners national attention
Significant Cyber Incident	Any significant cyber incident (or group of related cyber incidents) that are likely to result in demonstrable harm national security, foreign relations, or economy of the United States, diminished public confidence, civil liberties, or public health and safety of the American people, and/or credible indications that such an incident may be imminent

Event	Description
Death of Federal First Responder	The death of a federal first responded in the line of duty
Hostile Use of WMD	The hostile use or theft of a weapon of mass destruction (chemical, biological, radiological, or nuclear) or the discovery of an unattended weapon of mass destruction, or credible indications that such an incident may be imminent
Hostage Taking	Any hostage-taking or killing of U.S. nationals abroad

14.10.1.2 (U//~~FOUO~~) TIER TWO EVENTS

(U//~~FOUO~~) Pursuant to NSPM-32, the following events are "tier two" events that the FBI is required to report to the WHSR within 48 hours of initial observation. To meet this requirement, FBI employees who observe credible indications of the following events during the course of their official duties must internally report the events (as described in subsection 14.10.2) as soon as practicable but no later than 48 hours after initial observation.

(U) Table is U//~~FOUO~~

Event	Description
Breach of USG Information	The significant breach, unauthorized disclosure, or publication of U.S. Government-held personally identifiable information (PII), intellectual property (IP), Controlled Unclassified Information (CUI), or classified information to the extent permitted by counterintelligence and information security concerns
Loss of Public Trust	An event that has the potential to cause the loss of public trust in a U.S. Government department or agency
Contamination Incident (Biological Agent or Toxin)	Verified contamination from a biological agent or toxin, or credible indications that such a contamination is imminent

14.10.2 *(U) REPORTING PROCEDURES*

(U) These reporting procedures are in addition to, and do not substitute for, other mandatory reports that may exist as a matter of law, executive branch directive, Presidential policy, MOU, or DOJ or FBI policy. Examples of policies with additional mandatory reports include, but are not limited to, the notification and information sharing requirements for counterterrorism threats in subsections 4.2-4.3 of the *Counterterrorism Policy Guide* (1131PG), subsection 4.5.2 of the *Weapons of Mass Destruction Directorate Policy Guide* (1069PG), subsection 4.4.3 of the *Privacy Policy Guide* (1131PG), the *Security Compliance Program Policy Guide* (0934PG), various interagency MOUs, and counterterrorism Presidential Directives like NSPM-36 and NSPD-46 Annex II. As another example, DIOG Appendix K has requirements for FBI personnel to report suspected abuse of children, elderly persons, or otherwise vulnerable individuals. Uncertainties and disagreements over notification and information sharing requirements must be resolved by the appropriate FBIHQ operational division.

14.10.2.1 (U) STANDARD REPORTING PROCEDURES FOR ALL FBI EMPLOYEES

(U//~~FOUO~~) FBI employees who observe credible indications of any of the reportable events described in subsection 14.10.1 during the course of their official duties must provide the following "pertinent event information" (to the extent known) to their immediate supervisors.

(U) Pertinent Event Information

A) (U) A summary of relevant information regarding the event and the sources of the information

B) (U) A description of FBI actions being taken in response to the event (if applicable)

C) (U) Relevant information on the FBI's coordination with other federal, state, local, tribal, or territorial entities in response to the event (if applicable)

D) (U) POCs for additional information

(U//F~~OUO)~~ FBI employees are expected to report all pertinent event information (classified or unclassified) that may be helpful to the successful advancement of WHSR and FBI decision-making processes.

(U//F~~OUO)~~ When working as part of a squad, unit, or task force, multiple FBI employees may simultaneously observe credible indications of reportable events. In these circumstances, the individual with the most direct information regarding the event must notify the supervisor. Other employees should not make duplicate notifications unless they are augmenting the original report with new information.

(U//F~~OUO~~) To the extent feasible after providing initial notification, FBI employees should continue providing updates to their immediate supervisors so that relevant information can be passed along to SIOC. This includes advising when a reportable event concludes or if the FBI's response to a reportable event transitions from a critical incident response to an investigative posture.

(U//~~FOUO~~) As explained in subsections 14.10.2.2 and 14.10.2.3, below, the processes for passing information to SIOC differ between FOs and FBIHQ. Although FBI employees assigned to Legats are unlikely to observe credible indications of reportable events during the course of their official duties, they should follow the specific reporting procedures for FBIHQ divisions (subsection 14.10.2.3) when applicable.

14.10.2.2 (U) Specific Reporting Procedures for Field Offices

(U//~~FOUO~~) Upon receiving notifications of reportable events from employees (as described in subsection 14.10.2.1), FO supervisors must expeditiously determine if the information is reportable pursuant to this policy.[44] If it is reportable, they must provide the pertinent event information to FO operations centers without delay. Consistent with DIOG subsection 3.5.3.1, first-level supervisors (e.g., SSAs and SIAs) are not permitted to delegate their authorities and responsibilities. However, once a supervisor has affirmatively determined that information is reportable pursuant to this policy, he or she may assign a subordinate employee to provide the pertinent event information to the FO operations center. Second-line supervisors (and above) may delegate their authorities and responsibilities pursuant to DIOG subsection 3.5.3.1.

(U//~~FOUO~~) Upon receiving information about reportable events, FO operations center employees must immediately notify SIOC of the events by telephone.[45] After providing

[44] (U//~~FOUO~~) When supervisors are unsure whether provided information is reportable pursuant to this policy, they should err on the side of caution and pass it along to FO operations centers, as described in this subsection. All pertinent event information is vetted by SIOC watch commanders before it is disseminated to the WHSR.
[45] (U//~~FOUO~~) If the reportable information is classified, FO operations center employees must either limit the content of the initial notification to unclassified information or make initial contact with SIOC using a secure telephone line.

telephonic notifications, FO operations center employees must also, in addition to complying with reporting procedures as a matter of law, executive branch directive, Presidential policy, MOU, or DOJ or FBI policy (see subsection 14.10.2):

- (U//~~FOUO~~) Send email notifications to SIOC containing all pertinent event information (to the extent known). See subsection 14.10.2.1 for a list of pertinent event information. Email notifications should be completed as soon as practicable [redacted] b7E
- (U//~~FOUO~~) Make corresponding entries for each SIOC notification in their respective FO Situational Awareness tools (i.e., Virtual Command Center [VCC]) as soon as practicable following the notifications.
- (U//~~FOUO~~) Notify the FO head (i.e., ADIC or SAC) of the events.

(U//~~FOUO~~) FO heads are responsible for ensuring that operations center employees complete telephonic and email notifications in accordance with the processes, procedures, and timelines articulated in this subsection.

14.10.2.3 (U) SPECIFIC REPORTING PROCEDURES FOR FBI HEADQUARTERS

(U//~~FOUO~~) Upon receiving notifications of reportable events from employees (as described in subsection 14.10.2.1), FBIHQ supervisors must expeditiously determine if the information is reportable pursuant to this policy.[46] If it is reportable, they must notify SIOC by telephone without delay.[47] After providing telephonic notifications, FBIHQ supervisors must also:

- (U//~~FOUO~~) Follow up with an email to SIOC containing all pertinent event information (to the extent known). See subsection 14.10.2.1 for a list of pertinent event information. Email notifications should be completed as soon as practicable, but no later than three hours after initial observation of a tier one event (see subsection 14.10.1.1) and no later than 48 hours after initial observation of a tier two event (see subsection 14.10.1.2).
- (U//~~FOUO~~) Notify the FBIHQ division head of the events.

(U//~~FOUO~~) Consistent with DIOG subsection 3.5.3.1, first-level supervisors (e.g., SSAs and SIAs) are not permitted to delegate their authorities and responsibilities. However, once a supervisor has affirmatively determined that information is reportable pursuant to this policy, he or she may assign a subordinate employee to complete the notifications to SIOC articulated in this subsection. Second-line supervisors (and above) may delegate their authorities and responsibilities to a subordinate supervisor pursuant to DIOG subsection 3.5.3.1.

(U//~~FOUO~~) FBIHQ division heads are responsible for ensuring that FBIHQ personnel complete telephonic and email notifications in accordance with the processes, procedures, and timelines articulated in this subsection.

---

[46] (U//~~FOUO~~) When supervisors are unsure whether provided information is reportable pursuant to this policy, they should err on the side of caution and pass it along to SIOC, as described in this subsection. All pertinent event information is vetted by SIOC watch commanders before it is disseminated to the WHSR.

[47] (U//~~FOUO~~) If the reportable information is classified, supervisors must either limit the content of the initial notification to unclassified information or make initial contact with SIOC using a secure telephone line.

14.10.3 *(U//~~FOUO~~) DISSEMINATION PROCEDURES FOR THE STRATEGIC INFORMATION AND OPERATIONS CENTER*

(U//~~FOUO~~) Immediately after receiving notifications from FOs and FBIHQ divisions of reportable events (as described in subsection 14.10.2), SIOC employees must notify the on-duty watch commander (i.e., SIOC SSA), who is responsible for expeditiously reviewing the information and ensuring that it meets the reporting criteria in this policy and DIOG Appendix D.1.

(U//~~FOUO~~) If the information is reportable, the watch commander must notify the WHSR by telephone (using the unclassified or Top Secret lines, as appropriate). After providing telephonic notification, the watch commander must also send a corresponding email notification to the WHSR with all available information. Email notifications should be completed on the appropriate enclave as soon as practicable. [redacted] b7E

(U//~~FOUO~~) Consistent with DIOG subsection 3.5.3.1, SIOC watch commanders, as first-line supervisors, are not permitted to delegate their authorities and responsibilities. However, once a watch commander has affirmatively determined that information is reportable pursuant to this policy, he or she may assign a subordinate SIOC employee to facilitate the initial and follow-up dissemination of pertinent event information to the WHSR.

(U//~~FOUO~~) When providing notifications to the WHSR, watch commanders (or assigned SIOC employees) must clearly indicate whether the incident is ongoing or concluded and if they anticipate providing additional, subsequent updates. When subsequent updates are provided, watch commanders (or assigned SIOC employees) must clearly notate pertinent changes or corrections to previously reported information.

(U//~~FOUO~~) Watch commanders (or assigned SIOC employees) must abide by the requirements and restrictions in DIOG subsection 14.5.2 when sharing information related to national security and foreign intelligence matters with the WHSR. Notwithstanding the restrictions in DIOG subsection 14.5.2.1, watch commanders (or assigned SIOC employees) may respond to follow-up inquiries received directly from the WHSR that pertain to national security or foreign intelligence matters when doing so is necessary to facilitate WHSR and FBI decision-making processes during the FBI's response to a critical incident. However, watch commanders (or assigned SIOC employees) must abide by all requirements in DIOG subsections 14.5.2.2 and 14.5.2.4 if follow-up inquiries implicate the requirements and restrictions contained in those subsections. SIOC employees who have questions about the permissibility of sharing information with the WHSR must immediately contact the watch commander and/or the CIRG Legal Unit for guidance.

(U//~~FOUO~~) Once a reportable event concludes or the FBI's response to a reportable event transitions from a critical incident response to an investigative posture, SIOC must terminate ongoing notifications to the WHSR. The watch commander, in consultation with the applicable FBIHQ division/FO head(s), is responsible for determining when to discontinue notifications to the WHSR. When an event has concluded or the FBI has transitioned to an investigative response, the watch commander (or an assigned SIOC employee) must provide a final email notification to the WHSR indicating the discontinuation of notifications.

(U//~~FOUO~~) Pursuant to DIOG subsections 12.6 and 12.7.1, watch commanders (or assigned SIOC employees) who disseminate FBI information to the WHSR [redacted] as soon as practicable after events conclude. b7E

14.10.4 *(U) REQUESTS FOR MODIFICATIONS TO NOTIFICATION REQUIREMENTS*

(U//~~FOUO~~) To request a modification to these notification requirements, an FBI employee must submit an EC to the Policy and Exercise Unit (PEU), CIRG. PEU must coordinate modification requests with FBI stakeholders (including IPO) and the DOJ PCIR Working Group before submitting them for adjudication to the National Security Council (NSC) Executive Secretary. PEU must then notify IPO of any NSC-approved modifications.

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

15 (U) INTELLIGENCE ANALYSIS AND PLANNING

15.1 (U) OVERVIEW

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

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

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

15.2 (U) PURPOSE AND SCOPE

15.2.1 *(U) FUNCTIONS AUTHORIZED*

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

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

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

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

15.2.2 *(U) INTEGRATION OF INTELLIGENCE ACTIVITIES*

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

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

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

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

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

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

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

(U//~~FOUO~~) Without opening an Assessment, an FBI employee may produce written intelligence products that include, but are not limited to, an Intelligence Assessment (analytical product), Intelligence Bulletin and Geospatial Intelligence (mapping) from information already within FBI records. An FBI employee can also analyze information that is obtained pursuant to DIOG Section 5.1.1. If the employee needs information in order to conduct desired analysis and planning that requires the use of Assessment investigative methods beyond those permitted in DIOG Section 5.1.1, the employee must open a Type 3 Assessment or Type 4 Assessment in accordance with DIOG Sections 5.6.3.3. The applicable 801I-807I (Type 3 Assessments) or the applicable 818A-G (Type 4 Assessments) classification file (or other 801-series classification file as directed in the *Intelligence Program Policy Guide* (1170PG) must be used to document this analysis. See the *Intelligence Program Policy Guide* for file classification guidance.

15.3 (U) Civil Liberties and Privacy

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

15.4 (U) Legal Authority

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

(U//~~FOUO~~) The scope of authorized activities under Part II of the AGG-Dom is not limited to "investigations" in a narrow sense, such as solving particular investigations or obtaining evidence for use in particular criminal prosecutions. Rather, the investigative activities

authorized under the AGG-Dom may be properly used to provide critical information needed for broader analytic and intelligence purposes to facilitate the solution and prevention of crime, protect the national security, and further foreign intelligence objectives. These purposes include use of the information in intelligence analysis and planning under AGG-Dom, Part IV, and dissemination of the information to other law enforcement, USIC, and White House agencies under AGG-Dom, Part VI. Accordingly, information obtained at all stages of investigative activity is to be retained and disseminated for these purposes as provided in the AGG-Dom, or in FBI policy consistent with the AGG-Dom, regardless of whether it furthers investigative objectives in a narrower or more immediate sense. (AGG-Dom, Part II)

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

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

15.6 (U) AUTHORIZED ACTIVITIES IN INTELLIGENCE ANALYSIS AND PLANNING

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

15.6.1 *(U) INTELLIGENCE ANALYSIS*

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

15.6.1.1 (U) ANALYTIC INTELLIGENCE PRODUCTS

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

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

related to an investigation must be filed in the appropriate investigative file(s) and must include appropriate classification markings.

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

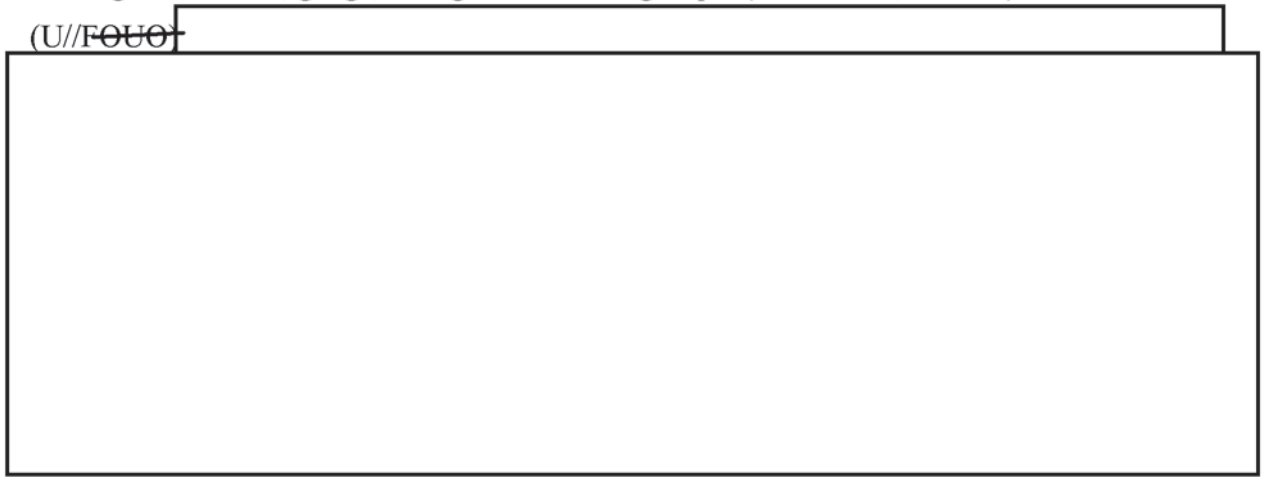
15.6.1.2 (U) UNITED STATES PERSON (USPER) INFORMATION

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

15.6.1.3 (U) INTELLIGENCE SYSTEMS

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

(U//~~FOUO~~)



b7E

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

16 (U) UNDISCLOSED PARTICIPATION (UDP)

16.1 (U) OVERVIEW

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

16.1.1 *(U) AUTHORITIES*

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

(U) First, Executive Order (E.O.) 12333 (see Appendix B) broadly establishes policy for the United States Intelligence Community (USIC). E.O. 12333 requires the adoption of procedures for undisclosed participation in organizations on behalf of elements of the USIC within the United States. Specifically, the Order provides "No one acting on behalf of elements of the Intelligence Community may join or otherwise participate in any organization in the United States on behalf of any element of the Intelligence Community without first disclosing such person's intelligence affiliation to appropriate officials of the organization, except in accordance with procedures established by the head of the Intelligence Community element concerned …. Such participation shall be authorized only if it is essential to achieving lawful purposes as determined by the Intelligence Community element head or designee." (E.O. 12333, Section 2.9, Undisclosed Participation in Organizations within the United States). The Order also provides, at Section 2.2, that "[n]othing in [E.O. 12333] shall be construed to apply to or interfere with any authorized civil or criminal law enforcement responsibility of any department or agency."

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

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

16.1.2 *(U) MITIGATION OF RISK*

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

b7E

16.1.3 *(U) SENSITIVE UDP DEFINED*

(U//~~FOUO~~)

b7E

16.1.4 *(U) NON-SENSITIVE UDP DEFINED*

(U//~~FOUO~~)

b7E

16.1.5 *(U) TYPE OF ACTIVITY*

(U//~~FOUO~~)

b7E

16.2 (U) PURPOSE, SCOPE, AND DEFINITIONS

16.2.1 *(U) ORGANIZATION*

(U//~~FOUO~~)

b7E

16.2.2 *(U) LEGITIMATE ORGANIZATION*

(U//~~FOUO~~)

b7E

b7E

16.2.3 *(U) PARTICIPATION*

(U//~~FOUO~~)

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

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

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

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

(U//~~FOUO~~)

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

(U//~~FOUO~~)

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

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

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

B) (U//~~FOUO~~) *Example 2*: b7E

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

16.2.3.1 **(U) UNDISCLOSED PARTICIPATION**

(U//~~FOUO~~) b7E

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

(U//~~FOUO~~) b7E

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

(U//~~FOUO~~) b7E

16.2.3.4 **(U) APPROPRIATE OFFICIAL**

(U//~~FOUO~~) b7E

16.2.3.5 **(U) SENSITIVE UNDISCLOSED PARTICIPATION**

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

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

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

b7E

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

(U//~~FOUO~~)

(U//~~FOUO~~)

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

(U//~~FOUO~~)

b7E

16.3 (U) REQUIREMENTS FOR APPROVAL

16.3.1 *(U) GENERAL REQUIREMENTS*

(U//~~FOUO~~)

b7E

16.3.1.1 (U) UNDERCOVER ACTIVITY

(U//~~FOUO~~)

b7E

b7E

16.3.1.2 **(U) CONCURRENT APPROVAL**

(U//~~FOUO~~)

b7E

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

(U//~~FOUO~~)

b7E

(U//~~FOUO~~)

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

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

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

b7E

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

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

(U//~~FOUO~~)

b7E

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

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

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

b7E

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

b7E

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

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

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

b7E

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

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

(U//~~FOUO~~) b7E

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

(U//~~FOUO~~)

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

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

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

16.4 (U) SUPERVISORY APPROVAL NOT REQUIRED

(U//~~FOUO~~) b7E

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

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

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

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

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

16.5 (U) STANDARDS FOR REVIEW AND APPROVAL

(U//~~FOUO~~)

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

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

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

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

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

(U//~~FOUO~~)

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

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

(U//~~FOUO~~) b7E

(U//~~FOUO~~)

b7E

16.6 (U) REQUESTS FOR APPROVAL OF UNDISCLOSED PARTICIPATION

(U//~~FOUO~~)

b7E

(U//~~FOUO~~)

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

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

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

b7E

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

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

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

(U//~~FOUO~~)

b7E

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

16.7 (U) DURATION

(U//~~FOUO~~)

b7E

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

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

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

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

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

b7E

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

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

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

b7E

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

16.9 (U) FBIHQ APPROVAL PROCESS OF UDP REQUESTS

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

(U//~~FOUO~~)

b7E

b7E

(U//~~FOUO~~)

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

(U//~~FOUO~~) b7E

b7E

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

(U//~~FOUO~~)

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

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

b7E

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

b7E

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

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

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

b7E

b7E

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

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

(U//~~FOUO~~)

b7E

(U//~~FOUO~~)

b7E

(U//~~FOUO~~)

16.10 (U) UDP EXAMPLES

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

b7E

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

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

b7E

(U//~~FOUO~~) **Analysis B**

b7E

C) (U//~~FOUO~~) **Example C**

b7E

(U//~~FOUO~~) **Analysis C**

D) (U//~~FOUO~~) **Example D**

b7E

(U//~~FOUO~~) **Analysis D:**

b7E

E) (U//~~FOUO~~) **Example E**

(U//~~FOUO~~) **Analysis E**

F) (U//~~FOUO~~) **Example F**

b7E

(U//~~FOUO~~) **Analysis F:**

G) (U//~~FOUO~~) **Example G**

b7E

(U//~~FOUO~~) **Analysis G**

b7E

(U//~~FOUO~~

(U//~~FOUO~~

b7E

H) (U//~~FOUO~~) **Example H:**

(U//~~FOUO~~) **Analysis H:** b7E

I) (U//~~FOUO~~) **Example I:**

(U//~~FOUO~~) **Analysis I:** b7E

J) (U//~~FOUO~~) **Example J:**

(U//~~FOUO~~) **Analysis J:** b7E

K) (U//~~FOUO~~) **Example K:**

(U//~~FOUO~~) **Analysis K:**

L) (U//~~FOUO~~) **Example L:**

(U//~~FOUO~~) **Analysis L:**

b7E

M) (U//~~FOUO~~) **Example M**

(U//~~FOUO~~) **Analysis M**

b7E

17 (U) OTHERWISE ILLEGAL ACTIVITY (OIA)

17.1 (U) OVERVIEW

(U//~~FOUO~~) Otherwise Illegal Activity (OIA) is conduct in the course of duties by an FBI employee (to include an undercover employee (UCE)) or a confidential human source (CHS) which constitutes a crime under local, state, or federal law if engaged in by a person acting without authorization. Certain types of OIA cannot be authorized, such as participation in conduct that would constitute an unlawful investigative technique (e.g., an illegal wiretap) or participation in an act of violence. In this context, "participation in an act of violence" does not include acts taken in self-defense and defense of others by the FBI employee or CHS because such actions would not be illegal.

17.2 (U) PURPOSE AND SCOPE

(U//~~FOUO~~) The use of OIA may be approved in the course of undercover activities or operations that involve an FBI employee or that involve use of a CHS. When approved, OIA should be limited or minimized in scope to only that which is reasonably necessary under the circumstances including the duration and geographic area to which approval applies, if appropriate.

17.3 (U//~~FOUO~~) APPLICATION

(U//~~FOUO~~) OIA can be authorized for an FBI employee or CHS to obtain information or evidence necessary for the success of an investigation under the following limited circumstances:

A) (U//~~FOUO~~) when that information or evidence is not reasonably available without participation in the OIA;

B) (U//~~FOUO~~) [redacted] b7E

C) (U//~~FOUO~~) when necessary to prevent serious bodily injury or death.

17.4 (U) LEGAL AUTHORITY

A) (U) The Attorney General's Guidelines for Domestic FBI Operations, Part V.C;

B) (U) The Attorney General's Guidelines on Federal Bureau of Investigation Undercover Operations, Part IV.H.

17.5 (U//~~FOUO~~) STANDARDS AND APPROVAL REQUIREMENTS FOR OIA

17.5.1 *(U) GENERAL APPROVAL REQUIREMENTS*

(U//~~FOUO~~) OIA that is not within the scope of [redacted] section 17.5.3, or is not part of an approved UCO, must be approved by the [redacted] (*AGG-Dom* Part V, Section C.3). For national security related investigations [redacted] is the approving component for OIA that requires approval beyond that authorized for SAC approval. However, as authorized by [redacted] may approve OIA in such investigations. For criminal b7E

investigations [redacted] is the approving component for OIA that requires approval beyond that authorized [redacted] b7E

17.5.2 *(U) OIA IN AN UNDERCOVER ACTIVITY*

(U//~~FOUO~~) General: The use of the undercover method is discussed in the DIOG Section 18.6.13. OIA is often proposed as part of an undercover scenario or in making the initial undercover contacts before the operation is approved. Specific approval for OIA must be obtained in the context of these undercover activities or operations in addition to general approval of the scenario or the operation.

(U//~~FOUO~~) OIA by an FBI employee in an undercover operation relating to activity in violation of federal criminal law that does not concern a threat to the national security or foreign intelligence must be approved in conformity with *The Attorney General's Guidelines on FBI Undercover Operations (AGG-UCO)*. Approval of OIA in conformity with the *AGG-UCO* is sufficient and satisfies any approval requirement that would otherwise apply under the *AGG-Dom*. Additional discussion is provided in the [redacted] b7E

[redacted] A Special Agent in Charge (SAC) may approve the OIA described in subsection 17.5.3.

(U//~~FOUO~~) OIA by an FBI employee in an undercover operation (UCO) relating to a threat to the national security or foreign intelligence collection must conform to the *AGG-Dom* and the [redacted] b7E

17.5.3 *(U//~~FOUO~~) FIELD OFFICE REVIEW AND APPROVAL OF OIA FOR AN FBI AGENT OR EMPLOYEE*

(U//~~FOUO~~)An SAC may authorize the following OIA for an FBI employee only when consistent with other requirements of this section, the *AGG-Dom*, the *AGG-UCO*, and other FBI policy. OIA activities described in subsections B, C, D, and F below, require CDC review prior to SAC approval:

A) (U//~~FOUO~~) Otherwise illegal activity that would not be a felony under federal, state, local, or tribal law;

B) (U//~~FOUO~~) [redacted] b7E

(U//~~FOUO~~) *Note* [redacted]

[50] (U//~~FOUO~~) In a controlled transaction, the item(s) will be monitored by the FBI and retained or seized at the conclusion of the transaction.

C) (U//~~FOUO~~) [redacted] b7E

D) (U//~~FOUO~~) [redacted]

(U//~~FOUO~~) *Note:* the payment of bribes and the amount of such bribes in a public corruption matter may be limited by other FBI policy (see the *Public Corruption Policy Directive and Policy Guide* [0702DPG] and the *Confidential Funding Policy Guide* [1284PG] [redacted] b7E

E) (U//~~FOUO~~) The making of false representations in concealment of personal identity or the true ownership of a proprietary, but not including sworn testimony; and

F) (U//~~FOUO~~) Conducting a money laundering transactions (including acting as an unlicensed money transmitter or using other methods to conduct the transactions) involving an aggregate amount not exceeding $1 million;

G) (U//~~FOUO~~) The advertising or soliciting of unlawful goods or services; and

H) (U//~~FOUO~~) Gambling activities.

(U//~~FOUO~~) SACs are not permitted to authorize violations of economic sanctions, export control laws, or laws concerning the proliferation of weapons of mass destruction (WMD). See the [redacted] b7E See the [redacted] However, SACs may authorize activities that may otherwise violate prohibitions of [redacted] but only in accordance with standards established by the FBI Director and agreed to by the Assistant Attorney General for National Security (see DIOG subsection 17.5.5 for OIA Related to [redacted]

(U//~~FOUO~~) Field offices should notify the appropriate FBIHQ operational division and OGC of any proposed OIA that in the judgment of the approving official may expose employees or others to significant personal safety risks, create a risk of civil liability, result in adverse publicity, or raise any other sensitive operational concern. As a matter of FBI policy, "judgment" means that the decision of the authorizing official is discretionary.

17.5.3.1 *(U//~~FOUO~~) WRITTEN OPERATIONS ORDERS FOR CONTROLLED FIREARMS TRANSACTIONS*

(U) The controlled purchase, receipt, delivery, or sale of firearms can quickly escalate into violent confrontations and result in the death of, or serious bodily injury to, law enforcement personnel, subjects, or the general public. In an effort to mitigate foreseeable risks and to plan for contingencies, an agent or task force officer (TFO) must prepare a written FD-888 Law Enforcement Operations order (OPORDER) for each planned firearms transaction conducted

[51] (U) Additional approval authority is necessary for the payment of bribes and kickbacks in undercover operations that are considered "sensitive circumstances. See the [redacted] b7E

pursuant to subsection 17.5.3.B. Each OPORDER must address the five "SMEAC" categories that comprise the "Five Paragraph Order:"

A) (U) Situation

B) (U) Mission

C) (U) Execution

D) (U) Administration (e.g., equipment)

E) (U) Command & Control (e.g., communication)

(U) When the OPORDER drafter has knowledge that children or disabled individuals may be encountered during a planned operation, their potential presence must be accounted for in the same way as any other operational contingency.

(U//~~FOUO~~) The safety of law enforcement personnel and sound tactical judgment should always be paramount considerations when preparing an OPORDER. When FBI employees know that a planned operation involves a higher-than-normal risk, they must consult with an FBI SWAT team or the Critical Incident Response Group's (CIRG) Tactical Section. These elements may deploy for the operation in accordance with the *National Tactical Program Policy Guide* (1235PG), which contains the criteria for high risk operations and the parameters for mandatory use of a SWAT team or CIRG's Tactical Section resources. SWAT teams and CIRG's Tactical Section are responsible for their own OPORDERs (rather than using the FD-888 template).

(U//~~FOUO~~) SACs (nondelegable) are the final approvers for OPORDERs drafted by field office employees pursuant to subsection 17.5.3.1.B. Prior to granting approval, SACs must seek CDC (or OGC) review and diligently review each OPORDER to ensure that careful and thorough planning has been conducted for each operation. They also must ensure that plans are adapted for the specific situation and include relevant details to enhance the safety and effectiveness of the employees involved in the operation. If a planned firearms transaction involves a significant amount of risk, but does not meet the risk threshold for mandatory deployment of a SWAT team or resources from CIRG's Tactical Section, the SAC is encouraged to consult with the SWAT senior team leader (STL) or a certified tactical instructor before approving the OPORDER. SACs may also ask other relevant subject matter experts (e.g., a principal firearms instructor) to review OPORDERs prior to approval.

(U//~~FOUO~~) Before executing a planned operation, the written OPORDER must be presented in an oral briefing to all employees involved. The briefer should cover all of the SMEAC categories and remind participants that the operation may become dangerous. An SAC may also require the SWAT STL, a certified tactical instructor, or the CDC to brief participating employees on tactics or the use of force policy (see Appendix F).

(U//~~FOUO~~) If appropriate under the circumstances, an SSA should notify local authorities of the planned operation in advance of its execution. Although the method, manner, and timing of this notification is left to the discretion of the SSA, he or she must consider the jurisdiction of local law enforcement, its responsibility to its community, and its need to be aware of law enforcement actions in its jurisdiction.

(U) As soon as practicable, but no later than five business days after executing a planned operation, the OPORDER must be uploaded and serialized to the associated case file.

(U) In the event of exigent circumstances (i.e., an emergent and pressing necessity that requires immediate action), an SAC (nondelegable) may permit an abbreviated written operational plan and/or an oral briefing in lieu of a formal OPORDER. However, the abbreviated written operational plan and/or oral briefing must address all of the topics outlined in the FD-888, including the SMEAC categories. As applicable, the briefer should also remind participants about the use of force policy. As soon as practicable, but no later than five business days after executing a planned firearms transaction under exigent circumstances, an agent or TFO must document the following information in the associated case file: (1) the details of the operation (e.g., subject); (2) anyone encountered on scene; (3) the participating employees; and (4) the SAC's approval.

b7E

(U//~~FOUO~~) For policy on required OPORDERs for searches and arrests, see subsections 18.7.1.6.1.6 and 19.2.3, respectively. These requirements also appear in subsection 18.6.13.5.1 in the context of OIA [redacted]

17.5.4 *(U//~~FOUO~~) OIA BY A CONFIDENTIAL HUMAN SOURCE (CHS) APPROVAL*

(U//~~FOUO~~) OIA by a CHS must be approved and documented in conformity with the *AGG-CHS* and the FBI *Confidential Human Source Policy Guide* (1212PG) [redacted]

b7E

17.5.5 *(U//~~FOUO~~) OIA RELATED TO* [redacted]

(U//~~FOUO~~) In accordance with Part V.C.3 of the AGG-Dom, the Director of the FBI and the Assistant Attorney General for the NSD of the DOJ established the following policy for FBI employees and CHS' concerning OIA as it relates to [redacted] (see as reference EC dated 01/16/2009, 319W-HQ-A1487699-OGC Serial 35).

A) (U//~~FOUO~~) [redacted]

b7E

B) (U//~~FOUO~~) NSD has represented that, except in exceptional circumstances, NSD shall act upon such an oral request within 24 hours and shall, within 72 hours, provide the FBI documentation of the authorization, including any terms and conditions.

C) (U//~~FOUO~~) [redacted]

D) (U//~~FOUO~~) Except in exceptional circumstances, any request for approval of OIA that [redacted] other than those described in paragraph A, must be made in writing to NSD.

(U//~~FOUO~~) For additional information regarding other governmental approvals that may be required for activities that are in violation of federal laws and regulations overseen by federal agencies other than the Department of Justice, see section 17.10.

17.5.5.1 (U//~~FOUO~~) PROCEDURES ON REQUESTS AND APPROVAL FOR OIA RELATED TO [redacted] b7E

(U//~~FOUO~~) For requests, standards of review, and approval procedures of OIA related to [redacted] see the [redacted]

(U//~~FOUO~~) Any questions about this policy or its implementation should be directed to OGC, National Security and Cyber Law Branch, Counterterrorism Law Units.

17.6 (U//~~FOUO~~) DOCUMENTATION OF REQUESTS TO ENGAGE IN OIA BY AN FBI AGENT OR EMPLOYEE

(U//~~FOUO~~) Requests to engage in OIA by an FBI agent or employee must be documented in an EC [redacted] and electronically placed into the appropriate investigative case file. The request must include: b7E

A) (U//~~FOUO~~) A synopsis of the investigation to date in which the OIA is being requested;

B) (U//~~FOUO~~) The name of the agent or employee who will engage in the OIA;

C) (U//~~FOUO~~)The specific proposed OIA in which the agent or employee will engage;

D) (U//~~FOUO~~) The expected duration of the OIA; and

E) (U//~~FOUO~~) Explanation of the justification for the use of OIA.

17.7 (U//~~FOUO~~) STANDARDS FOR REVIEW AND APPROVAL OF OIA

(U//~~FOUO~~) The appropriate approving official for the particular OIA must determine that the benefits to engaging in the requested OIA outweigh the risks involved and are necessary to:

A) (U//~~FOUO~~) To obtain information or evidence necessary for the success of the investigation and not reasonably available without participation in the otherwise illegal activity;

B) (U//~~FOUO~~) [redacted] b7E

C) (U//~~FOUO~~) To prevent death or serious bodily injury.

(U//~~FOUO~~) The approval of OIA must be documented in an EC [redacted] and electronically placed into the appropriate investigative case file. The approval must include:

A) (U//~~FOUO~~) the specific OIA activities approved;

B) (U//~~FOUO~~) the duration of the OIA; b7E

C) (U//~~FOUO~~) If the OIA is required to be approved by an [redacted] a copy of the [redacted] approval letter must be electronically placed into the case file.

17.8 (U) OIA NOT AUTHORIZED

(U//~~FOUO~~) The following activities may not be authorized as OIA:

A) (U//~~FOUO~~) Directing or participating in acts of violence;
(U//~~FOUO~~) Self-defense and defense of others. FBI employees are authorized to engage in any lawful use of force, including the use of force in self-defense or defense of others in the lawful discharge of their duties.

B) (U//~~FOUO~~) Activities or investigative methods that cannot be authorized because they are prohibited by law, including activities that would violate protected constitutional or federal statutory rights in the absence of a court order or warrant such as illegal wiretaps and searches. For example, approving a nonconsensual, nonemergency wiretap without a court order; approving the search of a home without a warrant or an exception to the warrant requirement, etc.

17.9 APPROVAL AND DOCUMENTATION OF EMERGENCY OIA

(U//~~FOUO~~) Without prior approval, an FBI employee may engage in OIA that could be authorized under this section only if necessary to meet an immediate threat to the safety of persons or property or to the national security, or to prevent the compromise of an investigation or the loss of a significant investigative opportunity. In such a situation, prior to engaging in the OIA, every effort should be made by the FBI employee to consult with the SAC, and by the SAC to consult with the United States Attorney's Office (USAO) or appropriate DOJ Division where the authorization of that office or division would be required unless the circumstances preclude such consultation. Circumstances in which OIA occur pursuant to this paragraph without the authorization required must be reported as soon as practicable, but not more than five (5) business days to the SAC, and by the SAC to FBIHQ and to the USAO or appropriate DOJ Division within five (5) business days of being notified. For the requirements for emergency authorization of OIA in [redacted] see the [redacted] b7E

17.10 OTHER GOVERNMENTAL APPROVALS

(U//~~FOUO~~) In addition to the approvals set forth above, additional coordination with other federal agencies may be necessary. Extraterritorial activity may involve conduct which would be in violation of laws and regulations overseen by federal agencies other than the Department of Justice. [redacted] b7E

[redacted] Upon FBI request, when necessary, each of those agencies may issue licenses to authorize activity that is otherwise prohibited.

This Page is Intentionally Blank.

18 (U) INVESTIGATIVE METHODS

18.1 (U) OVERVIEW

18.1.1 *(U) INVESTIGATIVE METHODS LISTED BY SUB-SECTION NUMBER*

(U) The following investigative methods are listed by DIOG Sub-Section number:

18.5.1 (U) Public information.

18.5.2 (U) Records or information - FBI and DOJ.

18.5.3.1 (U) Records or information - Other federal, state, local, tribal, or foreign government agency.

18.5.4 (U) Online services and resources.

18.5.5 (U) CHS use and recruitment.

18.5.6 (U) Interview or request information from the public or private entities.

18.5.7 (U) Information voluntarily provided by governmental or private entities.

18.5.8 (U) Physical Surveillance (not requiring a court order).

18.5.9 (U) Grand jury subpoenas – to providers of electronic communication services or remote computing services for subscriber or customer information only in Type 1 & 2 Assessments.

18.6.1 (U) Consensual monitoring of communications, including electronic communications.

18.6.2 (U) Intercepting the communications of a computer trespasser.

18.6.3 (U) Closed-circuit television/video surveillance, direction finders, and other monitoring devices.

18.6.4 (U) Administrative subpoenas.

18.6.5 (U) Grand jury subpoenas.

18.6.6 (U) National Security Letters.

18.6.7 (U) FISA Order for business records.

18.6.8 (U) Stored wire and electronic communications and transactional records.

18.6.9 (U) Pen registers and trap/trace devices.

18.6.10 (U) Mail covers.

18.6.11 (U) Polygraph examinations.

18.6.12 (U) Searches that Do Not Require a Warrant or Court Order (Trash Cover, Abandoned Property from a Public Receptacle, Administrative Inventory Search of a Lost/Misplaced Item) and Inventory Searches Generally

18.6.13 (U) Undercover operations.

18.7.1 (U) Searches – with a warrant or court order.

18.7.2 (U) Electronic surveillance – Title III.

18.7.3 (U) Electronic surveillance – FISA and FISA Title VII (acquisition of foreign intelligence information).

18.1.2 *(U) INVESTIGATIVE METHODS LISTED BY NAME (ALPHABETIZED)*

(U) The following investigative methods are listed alphabetized by DIOG name:

(U) Administrative subpoenas. (Section 18.6.4)

(U) CHS use and recruitment. (Section 18.5.5)

(U) Closed-circuit television/video surveillance, direction finders, and other monitoring devices. (Section 18.6.3)

(U) Consensual monitoring of communications, including electronic communications. (Section 18.6.1)

(U) Electronic surveillance – FISA and FISA Title VII (acquisition of foreign intelligence information). (Section 18.7.3)

18.7.3)

(U) Electronic surveillance – Title III. (Section 18.7.2)

(U) FISA Order for business records. (Section 18.6.7)

(U) Grand jury subpoenas. (Section 18.6.5)

(U) Grand jury subpoenas –to providers of electronic communication services or remote computing services for subscriber or customer information only in Type 1 & 2 Assessments. (Section 18.5.9)

(U) Information voluntarily provided by governmental or private entities. (Section 18.5.7)

(U) Intercepting the communications of a computer trespasser. (Section 18.6.2)

(U) Interview or request information from the public or private entities. (Section 18.5.6)

(U) Mail covers. (Section 18.6.10)

(U) National Security Letters. (Section 18.6.6)

(U) Online services and resources. (Section 18.5.4)

(U) Pen registers and trap/trace devices. (Section 18.6.9)

(U) Physical Surveillance (not requiring a court order). (Section 18.5.8)

(U) Polygraph examinations. (Section 18.6.11)

(U) Public information. (Section 18.5.1)

(U) Records or information - FBI and DOJ. (Section 18.5.2)

(U) Records or information - Other federal, state, local, tribal, or foreign government agency. (Section 18.5.3.1)

(U) Searches – with a warrant or court order. (Section 18.7.1)

(U) Searches that Do Not Require a Warrant or Court Order (Trash Cover, Abandoned Property from a Public Receptacle, Administrative Inventory Search of a Lost/Misplaced Item) and Inventory Searches Generally. (Section 18.6.12)

(U) Stored wire and electronic communications and transactional records. (Section 18.6.8)

(U) Undercover Operations. (Section 18.6.13)

18.1.3 *(U) GENERAL OVERVIEW*

(U//FOUO) The conduct of Assessments, predicated investigations (Preliminary Investigations and Full Investigations) and other activities authorized by the *AGG-Dom* may present choices between the use of different investigative methods (formerly investigative "techniques") that are each reasonable and effective based upon the circumstances of the investigation, but that are more or less intrusive, considering such factors as the effect on the privacy and civil liberties of individuals and the potential damage to reputation. The least intrusive method if reasonable based upon the circumstances of the investigation is to be used in such situations. However, the choice of methods is a matter of judgment. The FBI is authorized to use any lawful method consistent with the AGG-Dom, even if intrusive, where the degree of intrusiveness is warranted in light of the seriousness of a criminal or national security threat or the strength of the information indicating its existence, or in light of the importance of the foreign intelligence sought to the United States' interests. (AGG-Dom, Part I.C.2.)

(U) The availability of a particular investigative method in a particular investigation may depend upon the level of investigative activity (Assessment, Preliminary Investigation, Full Investigation, and Assistance to Other Agencies).

18.1.4 *(U) CONDUCTING INVESTIGATIVE ACTIVITY IN ANOTHER FIELD OFFICE'S AOR*

(U) Investigative information that may be within another field office's AOR can generally be obtained by setting an investigative lead to that field office. However, investigative circumstances may require employees to travel to another office's AOR to conduct investigative activity. In such circumstances, an employee, with the approval of [redacted] and the [redacted] in the other field office, may enter that office's AOR and conduct the necessary investigative activity (e.g. interview). However, if unplanned investigative activities or exigent circumstances prevent an employee from obtaining advance [redacted] and advance [redacted] before entering another field office's AOR, notification should be made as soon as practicable to the [redacted] and [redacted] in the other office's AOR, including the type of investigative activity(s) that occurred and the circumstances that made obtaining prior approval and concurrence unfeasible. b7E

18.2 (U) LEAST INTRUSIVE METHOD

(U) The AGG-Dom requires that the "least intrusive" means or method be considered and—if reasonable based upon the circumstances of the investigation—used to obtain intelligence or evidence in lieu of more intrusive methods. This principle is also reflected in Executive Order 12333 (Appendix B), which governs the activities of the United States intelligence community (USIC). The concept of least intrusive method applies to the collection of intelligence and evidence.

(U) Selection of the least intrusive means is a balancing test as to which FBI employees must use common sense and sound judgment to effectively execute their duties while mitigating the potential negative impact on the privacy and civil liberties of all people encompassed within the Assessment or predicated investigation, including targets, witnesses, and victims. This principle is not intended to discourage investigators from seeking relevant and necessary intelligence, information, or evidence, but rather is intended to encourage investigators to choose the least intrusive—yet still reasonable —means from the available options to obtain the material. Additionally, FBI employees should operate openly and consensually with United States persons (USPERs) to the extent practicable when collecting foreign intelligence that does not concern criminal activities or threats to the national security.

(U) DIOG Section 4.4 describes the least intrusive methods concept and the standards to be applied by FBI employees.

18.3 (U) PARTICULAR INVESTIGATIVE METHODS

(U//~~FOUO~~) All lawful investigative methods may be used in activities under the AGG-Dom as authorized by the AGG-Dom. Lawful investigative methods include those investigative methods contained in this DIOG as well as additional investigative methods and resources authorized in other FBI policy and guidance (for example, future additions to DIOG Sections 18, as well as PGs). In some instances the authorized investigative methods are subject to special restrictions or review or approval requirements. (AGG-Dom, Part V.A.)

18.3.1 *(U) USE OF CRIMINAL INVESTIGATIVE METHODS IN NATIONAL SECURITY INVESTIGATIONS*

(U//~~FOUO~~) Because national security investigations may implicate criminal issues as well, the availability of criminal investigative methods should be considered when appropriate. However, any use of criminal investigative methods should be closely coordinated with FBIHQ, both operational units and the NSCLB, prior to any anticipated use of this criminal investigative process. The NSCLB maintains liaison with DOJ OI respecting the use of FISA authorized investigative methods in national security investigations.

18.4 (U) INFORMATION OR EVIDENCE OBTAINED IN ASSESSMENTS AND PREDICATED INVESTIGATIONS

(U) The use, retention and/or dissemination of information obtained during authorized investigations must comply with the AGG-Dom and the DIOG. If the originator of information reported to the FBI characterizes an individual, group, or activity in a certain way, and that characterization should be documented for completeness of the FBI record, the FBI record (i.e., 302, EC, LHM) should reflect that another party, and not the FBI, is the originator of the characterization.

(U) During the course of an Assessment or predicated investigation, FBI employees lawfully may collect or passively receive items of evidence or intelligence from a variety of sources. Experience has demonstrated that the relevance of every item of evidence or intelligence collected or received is not always apparent at the time it is obtained. Accordingly, FBI employees have wide latitude to establish or determine the relevance of information as the Assessment or investigation develops. Nevertheless, as a matter of administrative efficiency and

sound business practice, if an FBI employee obtains an item of evidence which clearly is not relevant to the Assessment or investigation and there is no foreseeable future evidentiary or intelligence value of the item for the FBI or the USIC, the item should be returned or destroyed as circumstances warrant, with a record of the disposition documented in the file or in the Guardian FD-71a. Items that are lawfully collected, but for which the relevance is not immediately known, may be sequestered in the investigative file. If it is later determined that the item is relevant, the item may be used in the investigation upon such determination. The determination of relevancy will be made on a case-by-case basis with supervisory direction and may include consultation with the appropriate federal prosecuting office and/or the Chief Division Counsel (CDC) or the Office of the General Counsel (OGC). This policy does not supersede Sections 18.6.4.1 (Administrative Subpoenas); 18.6.5.1 (Federal Grand Jury Subpoena); 18.6.6.1 (National Security Letters); or 18.6.7 (FISA Order for Business Records), or any requirement imposed by statute, regulation or other applicable law.

18.5 (U) AUTHORIZED INVESTIGATIVE METHODS IN ASSESSMENTS

(U) AGG-Dom, Part II.A.4.

(U//~~FOUO~~) [redacted] in the Guardian FD-71a or [redacted] b7E

[redacted]

(U) In conducting an Assessment, only the following investigative methods are authorized:

A) (U) Public information. (See Section 18.5.1)

B) (U) Records or information - FBI and DOJ. (See Section 18.5.2)

C) (U) Records or information - Other federal, state, local, tribal, or foreign government agency. (See Section 18.5.3.1)

D) (U) Online services and resources. (See Section 18.5.4)

E) (U) CHS use and recruitment. (See Section 18.5.5)

F) (U) Interview or request information from the public or private entities. (See Section 18.5.6)

G) (U) Information voluntarily provided by governmental or private entities. (See Section 18.5.7)

H) (U) Physical Surveillance (not requiring a court order). (See Section 18.5.8)

I) (U//~~FOUO~~) Grand jury subpoenas - to providers of electronic communication services or remote computing services for subscriber or customer information only during a Type 1 & 2 Assessment (See Sections 18.5.9 and 18.6.5)

(U//~~FOUO~~) In Assessments, supervisory approval is required prior to use of the following investigative methods: certain interviews, tasking of a CHS in certain circumstances [redacted] b7E

[redacted] and physical surveillance not requiring [redacted]

This Page is Intentionally Blank.

18.5.1 *(U) INVESTIGATIVE METHOD: PUBLIC INFORMATION ("PUBLICLY AVAILABLE INFORMATION")*

18.5.1.1 (U) SCOPE

(U//~~FOUO~~) An FBI employee may obtain public information. (AGG-Dom, Part II.A.4.a and Part VII.L) Public information is "Publicly Available Information" that is:

A) (U) Published or broadcast for public consumption;

B) (U) Available on request to the public;

C) (U) Accessible online or otherwise to the public;

D) (U) Available to the public by subscription or purchase;

E) (U) Made available at a meeting open to the public;

F) (U) Obtained by visiting any place or attending an event that is open to the public (e.g., public places); or

G) (U) Observed, heard, smelled, detected or obtained by any casual observer or member of the public and does not involve unconsented intrusion into private places.

(U//~~FOUO~~) The phrase "observed, heard, smelled, detected or obtained by any casual observer or member of the public" includes, for example, plain view observations; overhearing a conversation taking place at an adjacent table in a public restaurant; odor detection (by a person, drug dog, or technical device) emanating from a vehicle, in a public place, or from locations to which the employee has gained lawful access; searching property that has been intentionally abandoned, including property discarded in public trash containers or public dumpsters (but does not include a "trash cover" as set forth in DIOG Section 18.6.12).

(U//~~FOUO~~) The following are examples:

1) (U) Viewing the vehicle identification number or personal property that is exposed to public view and may be seen when looking through the window of a car that is parked in an area that is open to and accessible by members of the public;

2) (U) The examination of books and magazines in a book store or the purchase of such items. See Maryland v. Macon, 472 U.S. 463 (1985); and

3) (U) A deliberate overflight in navigable air space to photograph marijuana plants is not a search, despite the landowner's subjective expectation of privacy. See California v. Ciraolo, 476 U.S. 207 (1986).

(U//~~FOUO~~) *Note:* Consent Searches are authorized in Assessments, as well as in predicated investigations.

(U//~~FOUO~~) *Note:* If the originator of information reported to the FBI characterizes an individual, group, or activity in a certain way, and that characterization should be documented for completeness of the FBI record, the FBI record (i.e., 302, EC, LHM) should reflect that another party, and not the FBI, is the originator of the characterization.

18.5.1.2 **(U) APPLICATION**

(U//~~FOUO~~) b7E

18.5.1.3 **(U) APPROVAL**

(U//~~FOUO~~) Supervisory approval is not required for use of this method, except for the special rule for attending a religious service, even if it is open to the public. (See DIOG Section 18.5.1.3.1)

18.5.1.3.1 ***(U//~~FOUO~~) SPECIAL RULES: "SPECIAL RULE FOR RELIGIOUS SERVICES" AND "SPECIAL RULE FOR OTHER SENSITIVE ORGANIZATIONS"***

18.5.1.3.1.1 **(U//~~FOUO~~) SPECIAL RULE FOR RELIGIOUS SERVICES – REGARDLESS OF WHETHER IT IS OPEN TO THE GENERAL PUBLIC**

A) **(U//~~FOUO~~)** ***In Assessments:*** b7E
An FBI employee attending a religious service overtly must have SSA approval. Higher approvals may be required under certain circumstances, such as attendance that rises to the level of UDP (see DIOG Section 16).

B) **(U//~~FOUO~~)** ***In Predicated Investigations:***
An FBI employee attending a religious service overtly must have SSA approval. Higher approvals may be required under certain circumstances, such as attendance that rises to the level of UDP (see DIOG Section 16).
(see DIOG Section 18.6.13).

18.5.1.3.1.2 **(U//~~FOUO~~) SPECIAL RULE FOR OTHER SENSITIVE ORGANIZATIONS**

A) **(U//~~FOUO~~)** ***In Assessments:***
b7E

B) **(U//~~FOUO~~)** ***In Predicated Investigations:***

18.5.1.4 **(U) USE/DISSEMINATION**

(U//~~FOUO~~) The use or dissemination of information obtained by this method must comply with the AGG-Dom and DIOG Section 14.

18.5.2 *(U) INVESTIGATIVE METHOD: RECORDS OR INFORMATION – FBI AND DEPARTMENT OF JUSTICE (DOJ)*

18.5.2.1 (U) SCOPE

(U//~~FOUO~~) An FBI employee may access and examine FBI and other DOJ records and may obtain information from any FBI personnel or other DOJ personnel. Access to certain FBI records may be restricted to designated FBI personnel because of the sensitive nature of the information in the record, the classification of the record, or the tool(s) used to gather the information contained in the record. These include but are not limited to: FBI records concerning confidential human source (CHS) identification; espionage investigations; code word; other compartmented information; records that include raw FISA collections; and Rule 6(e) material. (AGG-Dom, Part II.A.4.b)

(U//~~FOUO~~) *Note:* If the originator of information reported to the FBI characterizes an individual, group, or activity in a certain way, and that characterization should be documented for completeness of the FBI record, the FBI record (i.e., 302, EC, LHM) should reflect that another party, and not the FBI, is the originator of the characterization.

18.5.2.1.1 *(U//~~FOUO~~) FACIAL RECOGNITION TECHNOLOGY*

(U//~~FOUO~~) Facial recognition technology (FRT) refers to any system or service that creates a mathematical template of a face depicted in an image or video (i.e., a "template") and compares that template against other facial image templates to determine the degree of similarity between those facial images. FRT that utilizes FBI and DOJ records or information are subject to the requirements and restrictions within DIOG subsection 18.5.2.

(U) For further details on the proper use of FRT systems or services, refer to the *Facial Recognition Technology Use Policy Directive* (1276D).

18.5.2.2 (U) APPLICATION

(U//~~FOUO~~) [redacted] b7E

(U//~~FOUO~~) [redacted]

18.5.2.3 (U) APPROVAL

(U//~~FOUO~~) Supervisory approval is not required to use this method, except:

A. (U//~~FOUO~~) If the use of records constitutes pattern-based data mining under the Federal Data Mining Reporting Act of 2007, which must be reviewed and approved according to subsection 18.5.2.4 below.

B. (U//~~FOUO~~) When using FRT during an Assessment or predicated investigation (see DIOG Sections 5 through 9), which requires supervisory approval.

(U//~~FOUO~~) When determining whether to approve the use of FRT, supervisors should confirm that there is a legitimate purpose for conducting the query using the requested FRT system or service. Questions about FRT may be directed to Computer Analysis Response Team (CART) supervisors, who can coordinate with the Operational Technology Division (OTD) and the Criminal Justice Information Services (CJIS) Division, as necessary.

18.5.2.4 (U) PATTERN-BASED DATA MINING (PBDM)

(U//~~FOUO~~) As used in FBI policy, PBDM means queries or other analysis of electronic databases using two or more search criteria designed to discover or locate a predictive pattern or anomaly indicative of terrorist or criminal activity on the part of any individual or individuals (as defined in the [redacted] b7E
[redacted] Any such analysis based solely on racial, ethnic, national origin or religious characteristics is strictly prohibited.

(U//~~FOUO~~) For purposes of this requirement, PBDM does not include activities using one or more personal identifiers to identify an individual or analysis designed to discover links between a specific subject and unknown individuals or entities, even if the subject's actual identity is not yet known. PBDM does not include queries or analysis designed solely to identify potential human sources of intelligence nor does it include activities designed to identify an individual or individuals associated with criminal or terrorist activity that has already occurred. Queries designed to identify individuals or entities who have had contact with a specific individual are not pattern-based data mining; rather, such queries are subject-based data mining, even if the specific individual's actual identity is presently unknown.

(U//~~FOUO~~) The majority of data analysis performed during FBI Assessments and predicated investigations is based on specific individuals or events and therefore does not constitute PBDM because it is either link analysis or is not predictive of future behavior.

(U//~~FOUO~~) A Privacy Threshold Analysis (PTA) for PBDM must be completed and forwarded to OGC's Privacy and Civil Liberties Unit. See the *Privacy Policy Guide* (1113PG) for additional details.

(U//~~FOUO~~) FBI employees must also provide notice of any proposed use of PBDM to the Sensitive Operations Review Committee (SORC). Additionally, pursuant to the *Federal Agency Data Mining Reporting Act of 2007*,[52] the FBI must advise the DOJ of all agency initiatives that involve the use of PBMD, so that those activities may be included in the Department's annual report to Congress. (See the *Pattern-Based Data Mining Reporting Requirements Policy Directive*).

18.5.2.5 (U) USE, DISSEMINATION, AND RECORDKEEPING

(U//~~FOUO~~) The use or dissemination of information obtained by this method must comply with the AGG-Dom and DIOG Section 14.

(U//~~FOUO~~) The request for the records and the records received from DOJ and used during an Assessment or predicated investigation must be maintained as part of the appropriate file (e.g., 801 classification file, or investigation file).

[52] (U) 42 U.S.C. § 2000ee-3

18.5.3 *(U) INVESTIGATIVE METHOD: RECORDS OR INFORMATION – OTHER FEDERAL, STATE, LOCAL, TRIBAL, OR FOREIGN GOVERNMENT AGENCY*

18.5.3.1 (U) SCOPE

(U//~~FOUO~~) An FBI employee may access and examine records maintained by, and request information from, other federal, state, local, or tribal, or foreign governmental entities or agencies. When requesting information using this authority, care must be taken to ensure the entity to which the request is made understands that it is not compelled to provide such information or create a new record to assist the FBI. (AGG-Dom, Part II.A.4.c)

(U//F~~OUO~~) *Note:* If the originator of information reported to the FBI characterizes an individual, group, or activity in a certain way, and that characterization should be documented for completeness of the FBI record, the FBI record (i.e., 302, EC, LHM) should reflect that another party, and not the FBI, is the originator of the characterization.

18.5.3.1.1 *(U//~~FOUO~~)*

b7E

(U//~~FOUO~~)

(U

18.5.3.2 (U) APPLICATION

b7E

(U//~~FOUO~~)

(U//F~~OUO~~)

18.5.3.3 (U) APPROVAL AND COORDINATION

b7E

(U//~~FOUO~~)

A. (U//F~~OUO~~)

B. (U//~~FOUO~~)

(U//~~FOUO~~)

b7E

(U//~~FOUO~~)

18.5.3.3.1 ***(U) REQUESTS TO OTHER FEDERAL AGENCIES***

(U//~~FOUO~~) The FBI may request, for a law enforcement purpose, that another federal agency disclose Privacy Act-protected records through a written request (5 U.S.C. 552a(b)(7)). Such written requests must be for a civil or criminal law enforcement purpose and must be made by the Director or his designee. (See 28 CFR 16.40(c); OMB Guidelines, 40 Fed. Reg. at 28 sec. 955.) Pursuant to these provisions, the Director hereby delegates his authority to request formally from federal agencies information and records otherwise protected from disclosure by the Privacy Act, at FBIHQ, to all section chiefs and above, and in the field, to all SACs and ADICs. This authority may not be redelegated to a person below the rank of SAC in the field and SC at FBIHQ.

(U) The FBI may also request another federal agency to disclose Privacy Act-protected records pursuant to that agency's published routine uses. See 5 U.S.C. sec. 552a(b)(3). These requests need not be made in writing, and there are no restrictions on which FBI personnel may request such information.

18.5.3.3.2 ***(U) REQUESTS TO FOREIGN AGENCIES***

(U//~~FOUO~~) Requests for records or information from a foreign government entity or agency must be appropriately coordinated through the applicable FBI LEGAT office, International Operations Division (IOD), INTERPOL, relevant FBIHQ operational division, and/or DOJ Office of International Affairs, as necessary. Direct contact with foreign government agencies is authorized in certain circumstances, such as an imminent threat situation.

(U//~~FOUO~~) If the analysis of records obtained in this manner constitutes Pattern-based Data Mining (PBDM) under the Federal Data Mining Reporting Act of 2007, it must be reviewed and approved according to Section 18.5.2.3, above.

18.5.3.4 **(U) USE, DISSEMINATION, AND RECORDKEEPING**

(U//~~FOUO~~) The use and/or dissemination of information obtained by this method must comply with the AGG-Dom and DIOG Section 14.

(U//~~FOUO~~) The request for the records and the records received from an outside entity and used during an Assessment or predicated investigation must be maintained as part of the appropriate file (e.g., 801 classification file or investigative file).

18.5.4 *(U) INVESTIGATIVE METHOD: ONLINE SERVICES AND RESOURCES*

18.5.4.1 (U) SCOPE

(U//~~FOUO~~) An FBI employee may use any online service or resource that is publically available or for which the FBI has obtained authorized access for official use by way of subscription or purchase (including those that are only available to law enforcement entities), and complies with the United States Constitution, applicable laws, regulations, and policies. These online services and resources include, but are not limited to [redacted] b7E
[redacted] and vehicle, casualty, [redacted] including those that are only available to law enforcement entities. (AGG-Dom, Part II.A.4.d)

(U//~~FOUO~~) *Note:* If the originator of information reported to the FBI characterizes an individual, group, or activity in a certain way, and that characterization should be documented for completeness of the FBI record, the FBI record (i.e., 302, EC, LHM) should reflect that another party, and not the FBI, is the originator of the characterization.

18.5.4.1.1 *(U//~~FOUO~~)* [redacted] b7E

(U//~~FOUO~~) [redacted]

(U) [redacted]

18.5.4.2 (U) APPLICATION

(U//~~FOUO~~) This investigative method may be used in Assessments, predicated investigations, foreign intelligence collection investigations, and for assistance to other agencies in accordance with DIOG Section 12. The method may also be used during the initial processing of complaints and tips.

(U//~~FOUO~~) [redacted] b7E

(U//~~FOUO~~) See DIOG Appendix L for additional information on the standards for online activity by FBI employees in both affiliated and nonaffiliated capacities, and in both public and private venues.

18.5.4.3 (U) APPROVAL

(U//~~FOUO~~) Supervisory approval is not required to use this method, except:

A. (U//~~FOUO~~) [redacted] b7E

(U//~~FOUO~~) [redacted]

b7E

(U//~~FOUO~~) Additionally, subscribing to or purchasing any new service or resource must be done according to FBI contracting procedures and, in many instances, employees are required to successfully complete an online training curriculum prior to accessing or using FBI-sponsored applications, tools or, systems.

18.5.4.4 **(U) USE, DISSEMINATION, AND RECORDKEEPING**

(U//~~FOUO~~) The use or dissemination of information obtained by this method must comply with the AGG-Dom and DIOG Section 14.

This Page Is Intentionally Blank.

18.5.5 *(U) INVESTIGATIVE METHOD: CHS USE AND RECRUITMENT*

18.5.5.1 (U) SCOPE

(U//~~FOUO~~) The FBI may use and recruit human sources in Assessments and predicated investigations in conformity with the *AGG-Dom* (Part II.A.4.e), *AGG-CHS*, and the *Confidential Human Source Policy Guide* (1212PG) (CHSPG) [links to SECRET//NOFORN document]. In this context, "use" means obtaining information from, tasking, or otherwise operating such sources (AGG-Dom, Part VII.V).

(U//~~FOUO~~) *Note:* If the originator of information reported to the FBI characterizes an individual, group, or activity in a certain way, and that characterization should be documented for completeness of the FBI record, the FBI record (i.e., 302, EC, LHM) should reflect that another party, and not the FBI, is the originator of the characterization.

(U [redacted] b7E

18.5.5.2 (U) APPLICATION

(U//F~~OUO~~) This investigative method may be used in Assessments, predicated investigations, foreign intelligence collection investigations, and for assistance to other agencies when it is not otherwise prohibited by AGG-Dom, Part III.B.2.

(U) When collecting positive foreign intelligence, the FBI must operate openly and consensually with an USPER, to the extent practicable.

(U//~~FOUO~~) A CHS can be "used" in support of an Assessment and a predicated investigation or for the purpose of validating, vetting or determining the suitability of another CHS as part of an Assessment.

18.5.5.3 (U) APPROVALS

(U//F~~OUO~~) All investigative methods should be evaluated to ensure compliance with the admonition that the FBI should use the least intrusive method if reasonable based upon the circumstances of the investigation. That requirement should be particularly observed during an Assessment when using a CHS because the use of a CHS during an Assessment may be more intrusive than many other investigative methods. Use of a CHS in an Assessment should take place only after considering whether there are effective, less intrusive means available to obtain the desired information. The CHS must comply with all constitutional, statutory, and regulatory restrictions and limitations. In addition:

A) (U//F~~OUO~~) CHS use and direction must be limited in focus and scope to what is necessary to accomplish the authorized purpose and objective of the Assessment or predicated investigation [redacted] b7E

B) (U//F~~OUO~~) During an Assessment, [redacted] (see the Special Rule for Religious Services and the Special Rule for Other Sensitive Organizations below) only to the extent that such information is necessary to achieve the specific objective of the Assessment. If such contact reveals information or facts about an individual, group or organization that meets the requirements to open a predicated investigation, a predicated investigation may be opened, as appropriate.

C) (U//~~FOUO~~) **Special Rule for Religious Services** – regardless of whether it is open to the general public:

1) (U//~~FOUO~~) ***In Assessments*** [redacted] b7E
[redacted] An FBI employee attending a religious service overtly must have SSA approval. Higher approvals may be required under certain circumstances, such as attendance that rises to the level of UDP (see DIOG Section 16).
[redacted]

2) (U//~~FOUO~~) ***In Predicated Investigations:*** [redacted]
[redacted] An FBI employee attending a religious service overtly must have SSA approval. Higher approvals may be required under certain circumstances, such as attendance that rises to the level of UDP (see DIOG Section 16) [redacted]
[redacted] (see DIOG Section 18.6.13).

D) (U//~~FOUO~~) **Special Rule for Other Sensitive Organizations:**

1) (U//~~FOUO~~) ***In Assessments:*** [redacted] b7E
[redacted]

2) (U//~~FOUO~~) ***In Predicated Investigations*** [redacted]
[redacted]

E) (U//~~FOUO~~) **Public Information** [redacted]
[redacted]

F) (U//~~FOUO~~) **Non-Public Information:** [redacted] b7E
[redacted]

G) (U//~~FOUO~~) [redacted]
[redacted] This principle does not, however, eliminate the legal concept of a consent search or the doctrine of misplaced confidence that may be relied on by the government to gain access to otherwise protected places or information when the CHS has been granted access by a consenting party and the CHS stays within the scope of the consent provided. The doctrine of misplaced confidence provides that a person assumes the risk when dealing with a third party that the third party might be a government agent and might breach the person's confidence [redacted]

b7E

(U) Example:

(U//~~FOUO~~) *Scenario*

(U//~~FOUO~~) *Response*

b7E

(U//~~FOUO~~)

18.5.5.4 (U//~~FOUO~~) Applicability of the Misplaced Confidence Doctrine During CHS Online Activity

(U//~~FOUO~~)

b7E

(U//~~FOUO~~)

[redacted] b7E

(U//~~FOUO~~) [redacted]

[redacted]

18.5.5.5 **(U) USE/DISSEMINATION**

(U//~~FOUO~~) The use or dissemination of information obtained by this method must comply with the AGG-Dom, DIOG Section 14, and the *CHSPG* [redacted]

[redacted]

18.5.6 *(U) INVESTIGATIVE METHOD: INTERVIEW OR REQUEST INFORMATION FROM THE PUBLIC OR PRIVATE ENTITIES*

18.5.6.1 (U) SCOPE

(U//~~FOUO)~~ An interview is the questioning of an individual (including a subject or target) in order to gather information that is pertinent to and within the scope of an authorized Assessment or predicated investigation, or otherwise within the scope of FBI authority. An "interrogation" is a type of interview. For purposes of this policy provision, the terms "interview" and "interrogation" are interchangeable. In accordance with DIOG Section 5.1.1, the initial questioning of a complainant is not an interview, nor is re-contacting a complainant to clarify information that was initially provided. Normally, an FBI employee should disclose the employee's affiliation with the FBI and true purpose of the interview at the outset. The person being interviewed is voluntarily providing information and his/her Constitutional rights must be respected. (AGG-Dom, Part II.A.4.f and AGG-Dom, Part II.B.4)

(U//~~FOUO~~) It is the policy of the FBI that an employee[53] must not use force, threats, improper promises, or physical abuse when conducting an interview, or the threat of such abuse to the person being interviewed, or to any third party. It is also the policy of the FBI that an employee must not impose severe physical conditions on the person being interviewed.

(U//F~~OUO~~) All persons, whether in custody or not, located domestically or overseas, who are interviewed by FBI employees must be treated in accordance with FBI policy at all times. In addition, FBI employees must adhere, at all times, to the Constitution and laws of the United States, including but not limited to the prohibition against torture found in chapter 113C of Title 18, United States Code, when conducting any interview or interrogation regardless of geographic location of the interview or interrogation.

(U) During custodial and noncustodial interviews, when an agent knows or reasonably should know that the person being interviewed has a disability, reasonable and necessary steps must have taken to provide physical accessibility, reasonable accommodations, and effective communication. The factual circumstances of the interview will determine what reasonable and necessary steps should be taken.

(U//~~FOUO)~~ FBI employees do not have the authority to promise leniency or immunity from prosecution. Additionally, the interviewer should make reasonable efforts to obtain information that is accurate, relevant, timely, and complete. An interview may only elicit a description of how an individual exercises a right guaranteed by the First Amendment to the Constitution if such information is pertinent to and within the scope of an authorized activity; similarly, regardless of how such information is elicited, it may not be maintained in FBI files unless it is pertinent to and within the scope of an authorized activity.

(U//~~FOUO~~) Nothing in this section prohibits asking for or accepting volunteered access to personal or real property. "Consent Searches" are authorized in Assessments, as well as in predicated investigations.

---

[53] The term "FBI employee" includes, but is not limited to, professional investigative staff, intelligence analyst, special agent, task force officer (TFO), task force member (TFM), task force participant (TFP), detailee, and FBI contractor.

(U//~~FOUO~~)

b7E

(U//~~FOUO~~) *Note:* If the originator of information reported to the FBI characterizes an individual, group, or activity in a certain way, and that characterization should be documented for completeness of the FBI record, the FBI record (i.e., 302, EC, LHM) should reflect that another party, and not the FBI, is the originator of the characterization.

18.5.6.2 (U) APPLICATION

(U//~~FOUO~~)

b7E

18.5.6.3 (U) VOLUNTARINESS

(U//F~~OUO~~) Information that is sought during an interview must be provided voluntarily. It is the policy of the FBI that an employee must not use force, threats, improper promises, or physical abuse when conducting an interview, or the threat of such abuse to the person being interviewed, or to any third party. It is also the policy of the FBI that an employee must not impose severe physical conditions on the person being interviewed.

(U//F~~OUO~~) FBI employees do not have the authority to promise leniency or immunity from prosecution. If, during a noncustodial interview, the interviewee indicates he or she wishes to consult an attorney, the interviewer should assess whether continuing the interview would negatively affect the voluntariness of any further information provided. In determining whether a statement has been given voluntarily, courts evaluate a "totality of the circumstances," which may include consideration of the following factors:

A) (U//~~FOUO~~) Whether the interviewee was notified of any charges against him/her or advised of his/her rights;

B) (U//~~FOUO~~) The interviewee's age, intelligence, experience, and physical condition;

C) (U//F~~OUO~~) Whether there was any physical abuse or threats of abuse during the interview;

b7E

D) (U//~~FOUO~~) The number of officers present and whether weapons were displayed during the interview;

E) (U//~~FOUO~~) Whether threats or psychological pressure was used during the interview;

F) (U//~~FOUO~~) Whether the interviewee was deprived of food, sleep, medication, or outside communication during the interview;

G) (U//~~FOUO~~) The duration of the interview, and whether any trickery, ruse, or deception was used; and

H) (U//~~FOUO~~) Whether there were any promises of leniency or other inducements made during the interview.

(U//~~FOUO~~) See Sections 18.5.6.3.8, 18.5.6.3.9, and 18.5.6.4.13 below for additional considerations when interviewing juveniles.

(U//~~FOUO~~) These factors are illustrative. The presence of any one or more of the factors mentioned above will not necessarily make a statement involuntary.

18.5.6.4 (U) APPROVAL/PROCEDURES

(U//~~FOUO~~) Generally, interviews do not require supervisory approval, except for:

A) (U//~~FOUO~~) Circumstances involving the Advice of Rights in Connection with Operational Terrorists inside the United States (See Section 18.5.6.4.1.4 below);

B) (U) Contact with Represented Parties (See Section 18.5.6.4.5 below);

C) (U) Member of the U.S. Congress and their Staffs (See Section 18.5.6.4.6 below);

D) (U) White House Personnel (See Section 18.5.6.4.7 below);

E) (U) Members of the News Media (See Section 18.5.6.4.8 below); and

F) (U//~~FOUO~~) [redacted] b7E

[redacted]

(U//~~FOUO~~) PGs may require prior notice to FBIHQ for other interview types.

18.5.6.4.1 *(U) DOMESTIC CUSTODIAL INTERVIEWS*[56]

(U//~~FOUO~~) An FBI employee must advise a person who is in custody of his or her *Miranda* rights, per the FD-395, "Advice of Rights" form, before beginning an interview inside the United States with the exception of questioning reasonably prompted by a concern for public safety, (See DIOG Section 18.5.6.4.1.3 below), or questioning in connection with an operational terrorist inside the United States (See DIOG Section 18.5.6.4.1.4 below). It is critical that the person understand his/her rights before questioning. By signing the FD-395, the defendant acknowledges that he/she has been advised of his/her rights and is willing to proceed without a lawyer present. Once the advice of rights is provided and the interviewee voluntarily, knowingly, and intelligently waives those rights, the interview may proceed until such time as the interviewee invokes a right to silence and/or counsel. [redacted] b7E

[redacted]

[56] (U) For policy concerning interviews outside the United States, see Section 18.5.6.6.

b7E

(U//~~FOUO~~) A person is "in custody" for purposes of *Miranda* when his/her freedom of movement is significantly restricted. Custody can arise short of formal arrest when, judging from the totality of the circumstances, a reasonable person in the position of the interviewee would believe that he/she is in custody. A brief, temporary investigative detention is not custody provided it is reasonable in scope. In assessing whether a temporary detention is reasonable in scope and thus not custody for purposes of *Miranda*, factors to consider include the degree of force used to affect the detention, use of restraining devices and whether the individual was moved from the location of the stop. Employees can clarify custodial status by telling the person that he/she is not under arrest. See DIOG subsection 18.5.6.4.17.3 below regarding requirements for recording custodial interviews. All statements made during a custodial interview of persons arrested by the FBI for federal crimes,[57] prior to initial appearance and while in a place of detention with suitable recording equipment, must be electronically recorded (with very limited exceptions as listed in DIOG subsection 18.5.6.4.17.4, below).

(U//~~FOUO~~) For specific requirements to interview a federal prisoner held in the custody of the Bureau of Prisons (BOP) or United States Marshals Service (USMS) see DIOG Appendix C.

18.5.6.4.1.1 (U) MIRANDA WARNINGS REQUIRED DOMESTICALLY

(U//~~FOUO~~) *Miranda* warnings are required when a person:

A) (U//~~FOUO~~) Has been arrested and is in federal, tribal, state, or local custody;

B) (U//~~FOUO~~) Is significantly restricted in his freedom of movement to a degree normally associated with a formal arrest; or

C) (U//~~FOUO~~) Regardless of custody, has previously been formally charged, prosecution is pending, and the subject matter of the interview concerns the pending charge.

(U//~~FOUO~~) For the purposes of *Miranda*, an interview refers to express questioning and any words or actions that are reasonably likely to elicit an incriminating response. In a custodial interview, the individual must be advised of the names and official identities of the employee(s) conducting the interview, the nature of the inquiry, and provided *Miranda* warnings, per the FD-395 form, before being interviewed. After being advised of his/her rights, if an interviewee who is in custody, invokes the right to counsel and/or the right to remain silent, this must be honored and the interview must cease. However, once the advice of rights is provided and the interviewee voluntarily, knowingly, and intelligently waives those rights, the interview may proceed until such time as the interviewee invokes a right to silence and/or counsel.

b7E

Once the interviewee invokes his or her right to remain silent and/or right to counsel, the interview must immediately be terminated. The fact that the interviewee invoked the right

[57] This policy does not apply to a person arrested for a state or local crime during a joint or Task Force investigation.

to counsel and/or the right to remain silent should be recorded on the FD-395 and the form should be executed in all other respects.

18.5.6.4.1.2 (U) MIRANDA WARNINGS NOT REQUIRED DOMESTICALLY

(U//~~FOUO~~) There are certain custodial interviews in which the protection *Miranda* provides against self-incrimination may not be served by reading the standard warnings and obtaining a waiver. In the following circumstances, *Miranda* warnings are not required for custodial interviews:

A) (U//F~~OUO~~) standard booking questions;

B) (U//~~FOUO~~) an interview of the incarcerated individual as a victim or witness in an unrelated matter that does not pertain to any pending charges against the interviewee;

C) (U//F~~OUO~~) the public safety exception (discussed in more detail below); and

D) (U//F~~OUO~~) in connection with arrests of operational terrorists inside the United States (discussed in more detail below).

18.5.6.4.1.3 (U//~~FOUO~~) PUBLIC SAFETY EXCEPTION

(U//F~~OUO~~) The warning and waiver of rights is not required when questions are asked that are reasonably prompted by a concern for public safety. [redacted] b7E

[redacted] This public safety exception could also apply to other situations where imminent threat(s) to the safety of law enforcement officers or member(s) of the public could be alleviated by questions necessary to neutralize the threat.

18.5.6.4.1.4 (U//F~~OUO~~) ADVICE OF RIGHTS IN CONNECTION WITH ARRESTS OF OPERATIONAL TERRORISTS INSIDE THE UNITED STATES[58]

(U//~~FOUO~~) Identifying and apprehending suspected terrorists, interrogating them to obtain intelligence about terrorist activities and impending terrorist attacks, and lawfully detaining them so that they do not pose a continuing threat to our communities are critical to protecting the American people. The DOJ and the FBI believe that we can maximize our ability to accomplish these objectives by continuing to adhere to FBI policy regarding the use of *Miranda* warnings for custodial interrogation of operational terrorists[59] who are arrested inside the United States:

---

[58] (U//~~FOUO~~) This guidance applies only to arrestees who have not been indicted and who are not known to be represented by an attorney. For policy concerning the interrogation of indicted defendants, see Section 18.5.6.4.1; and for policy concerning contact with represented persons, see DIOG Section 18.5.6.4.5.

[59] (U//FOUO) For these purposes, an operational terrorist is an arrestee who is reasonably believed to be either a high-level member of an international terrorist group; or an operative who has personally conducted or attempted to conduct a terrorist operation that involved risk to life; or an individual knowledgeable about operational details of a pending terrorist operation.

A) (U//F~~OUO~~) If applicable, agents should ask any and all questions that are reasonably prompted by an immediate concern for the safety of the public or the arresting agents without advising the arrestee of his *Miranda* rights.[60]

B) (U//F~~OUO~~) After all applicable public safety questions have been exhausted, agents should advise the arrestee of his/her *Miranda* rights and seek a waiver of those rights before any further interrogation occurs, absent the exceptional circumstances described below.

C) (U//F~~OUO~~) There may be exceptional cases in which, although all relevant public safety questions have been asked, agents nonetheless conclude that continued unwarned interrogation is necessary to collect valuable and timely intelligence not related to any immediate threat, and that the government's interest in obtaining this intelligence outweighs the disadvantages of proceeding with unwarned interrogation.[61]

(U//F~~OUO~~) In these exceptional cases, agents must seek SAC approval, which cannot be delegated, to proceed with an unwarned interrogation after the public safety questioning is concluded. Whenever feasible, the SAC will consult with FBIHQ (including OGC) and DOJ attorneys before granting approval. Presentment of an arrestee may not be delayed simply to continue the interrogation, unless the arrestee has timely waived prompt presentment.

(U//F~~OUO~~) The determination whether particular unwarned questions are justified on public safety grounds must always be made on a case-by-case basis based on all the facts and circumstances. In light of the magnitude and complexity of the threat often posed by terrorist organizations, particularly international terrorist organizations, and the nature of their attacks, the circumstances surrounding an arrest of an operational terrorist may warrant significantly more extensive public safety interrogation without *Miranda* warnings than would be permissible in an ordinary criminal investigation. Depending on the facts, such interrogation might include, for example, [redacted] b7E

[redacted]

(U//F~~OUO~~) As noted above, if there is time to consult with FBIHQ (including OGC) and Department of Justice attorneys regarding the interrogation strategy to be followed prior to reading the arrestee his *Miranda* rights, the field office should endeavor to do so. Nevertheless, the agents on the scene who are interacting with the arrestee are in the best

---

[60](U//F~~OUO~~) The Supreme Court held in *New York v. Quarles*, 467 U.S. 649 (1984), that if law enforcement officials engage in custodial interrogation of an individual that is "reasonably prompted by a concern for the public safety," any statements the individual provides in the course of such interrogation shall not be inadmissible in any criminal proceeding on the basis that the warnings described in *Miranda V. Arizona*, 384 U.S. 436 (1966), were not provided. The Court noted that this exception to the *Miranda* rule is a narrow one and that "in each case it will be circumscribed by the {public safety} exigency which justifies it." 467 U.S. at 657.

[61](U//F~~OUO~~) The Supreme Court has strongly suggested that an arrestee's Fifth Amendment right against self-incrimination is not violated at the time a statement is taken without *Miranda* warnings, but instead may be violated only if and when the government introduces an unwarned statement in a criminal proceeding against the defendant. *See Chavez v. Martinez*, 538 U.S. 760, 769 (2003) (plurality op.); *id.* at 789 (Kennedy, J., concurring in part and dissenting in part); *cf. also id.* at 778-79 (Souter, J., concurring in the judgment); *See also United States v. Patane,* 542 U.S. 630, 641 (2004) (plurality opinion) ("[V]iolations [of the Fifth Amendment right against self-incrimination] occur, if at all, only upon the admission of unwarned statements into evidence at trial."); *United States v. Verdugo-Urguidez,* 494 U.S. 259, 264 (1990) ("[A] violation [of the Fifth Amendment right against self-incrimination] occurs only at trial.").

position to assess what questions are necessary to secure their safety and the safety of the public, and how long the post-arrest interview can practically be delayed while interrogation strategy is being discussed.

18.5.6.4.2 *(U//~~FOUO~~) MIRANDA WARNINGS FOR SUSPECTS IN CUSTODY OVERSEAS*

(U//~~FOUO~~) Please see *DIOG Appendix T* [links to a SECRET//NOFORN document] for policy governing all extraterritorial activities.

18.5.6.4.3 *(U) CONSTITUTIONAL RIGHTS TO SILENCE AND COUNSEL UNDER MIRANDA*

A) (U//~~FOUO~~) ***Silence:*** If a custodial interviewee invokes his/her right to remain silent, FBI employees should not attempt a subsequent interview until a significant period of time has elapsed (a two-hour period has been held to be significant) or the interviewee requests to be interviewed anew. In either case, an FBI employee will ensure that the interviewee is again advised of his/her *Miranda* rights and indicates that he/she understand those rights before further questioning. If the interviewee again asserts his/her right to remain silent or the right to counsel, questioning must cease at that time. Assertion of the right to silence, like assertion of the right to counsel, must be unequivocal and unambiguous. A waiver of the right to remain silent occurs when an interviewee knowingly and voluntarily makes a statement; assertion of the right to remain silent requires more than mere silence in the face of questioning. This right, like the right to counsel, can be invoked at any time during custodial interrogation. Agents may continue questioning someone who has not clearly invoked his/her right to remain silent, but if the custodial interviewee asserts his/her right to silence, questioning must cease at that time.

B) (U//F~~OUO~~) ***Counsel:*** If a custodial interviewee invokes his/her right to counsel, questioning must cease. FBI employees may not attempt a subsequent interview unless counsel is present, the custodial interviewee initiates contact, or there has been a break in custody of at least 14 days.

1) (U//F~~OUO~~) When a custodial interviewee who has invoked his/her right to counsel initiates a subsequent interview, an FBI employee must ensure that the interviewee is advised of and understands his/her *Miranda* rights before proceeding with the interview. Not every statement by a custodial interviewee can fairly be interpreted as initiating a subsequent interview. In order to constitute the initiation of an interview, the custodial interviewee must either directly request such or use words that are reasonably interpreted as expressing a desire to be interviewed. If the words used are ambiguous, the FBI employee should clarify the custodial interviewee's intent by asking directly whether the custodial interviewee wants to be interviewed. The words and responses, if any, to such clarifying questions should be documented. General conversation by a custodial interviewee cannot be interpreted as indicating a desire to be interviewed and cannot be used standing alone to predicate a second interview after the right to counsel has been invoked. If the interviewee again asserts his/her right to counsel, or invokes his/her right to silence, questioning must cease at that time.

2) (U//F~~OUO~~) When an uncharged and/or unrepresented interviewee who has previously invoked his/her right to counsel experiences a break-in-custody of at least 14 days, he/she may be approached for a subsequent interview. FBI employees, however, must ensure that the custodial interviewee is again advised of and waives his/her *Miranda* rights before proceeding with the interview. A break-in-custody for these purposes can occur even if an

interviewee is continuously incarcerated. Questions as to what constitutes a break-in-custody should be directed to the CDC or OGC.

3) (U//F~~OUO~~) Contact with a represented person outside the presence of his/her counsel may implicate state ethics rules for attorneys (AUSAs). Before making such contact, employees are encouraged to contact the CDC, OGC, or the USAO. Once a represented person has been charged, information may only be elicited from the person: 1) regarding an unrelated or uncharged matter or 2) when counsel is present. Questions as to whether an individual is in fact represented or may be questioned as to a particular matter should be directed to the CDC or OGC.

18.5.6.4.4 *(U) SIXTH AMENDMENT RIGHT TO COUNSEL*

(U//~~FOUO~~) The Sixth Amendment Right to Counsel requires the government to advise and obtain a waiver of the Right to Counsel prior to interviewing the person to whom the right has attached. The Right to Counsel attaches upon indictment regardless of whether the indicted person realizes an indictment has been returned. The Right to Counsel also attaches upon the filing of information and at the time of an initial appearance on a Federal Complaint. The Right to Counsel is offense specific. When applicable, a warning regarding the Right to Counsel and subsequent knowing and voluntary waiver must occur prior to an interview, regardless of whether the person is in custody. Providing a person with a *Miranda* warning and obtaining a waiver per the use of Form FD-395 will permit the interview of the person after the Right to Counsel has attached. The Sixth Amendment right to counsel does not prohibit the government from re-contacting the subject if the subject refuses initially to waive this right or otherwise has requested or obtained counsel following an Initial Appearance. However, further attempts to interview the subject may be prohibited if the subject invoked his right to counsel and remained in continuous custody or there was an insufficient break in custody (consistent with *Miranda* and its progeny). In addition, b7E

18.5.6.4.5 *(U) CONTACT WITH REPRESENTED PERSONS*

(U//~~FOUO~~) CDC or OGC review is required before contact with represented persons in the absence of prior notice to counsel. Such contact may implicate legal restrictions and affect the admissibility of resulting evidence. Hence, if an individual is known to be represented by counsel in a particular matter, the CDC must follow applicable law and DOJ procedure when reviewing the request to contact the represented individual in the absence of prior notice to counsel. The SAC, CDC, or their designees, and the United States Attorney or his or her designees must consult periodically on applicable law and DOJ procedure relative to contact with represented persons. The field office may raise inconsistent application of: (i) state ethics rules; or (ii) rules for contacts with represented persons with the USAO and request that it consult with the DOJ Professional Responsibility Advisory Office. (AGG-Dom, Part V.B.1)

18.5.6.4.6 *(U) MEMBERS OF THE UNITED STATES CONGRESS AND THEIR STAFFS*

(U//~~FOUO~~) Generally, FBI employees may accept information offered from Congressional offices just as they would accept information from other sources, and they may act upon it accordingly. b7E

b7E

[redacted]

18.5.6.4.7 ***(U) WHITE HOUSE PERSONNEL***

(U//~~FOUO~~) FBI employees may accept information offered by White House personnel just as they would accept information from other sources, and they may act upon it accordingly. [redacted] b7E

[redacted] Additional guidance regarding contact with White House personnel may be found in the AG Memorandum captioned "Communications with White House and Congress" dated May 11, 2009. (See DIOG Appendix D) *Note:* [redacted]

18.5.6.4.8 ***(U) MEMBERS OF THE NEWS MEDIA***

18.5.6.4.8.1 **(U) APPROVAL REQUIREMENTS**

(U) Attorney General approval, including notice to the Director of the DOJ's Office of Public Affairs, must be obtained prior to conducting an interview of a member of the news media for any offense which the member of the news media is suspected of having committed in the course of, or arising out of, the coverage or investigation of a news story, or while engaged in the performance of his/her official duties as a member of the news media. [redacted] b7E

[redacted]

(U//~~FOUO~~) Requests for this approval must be submitted with an EC to the AD of the operational FBIHQ division that is responsible for the investigative classification and the AD of the Office of Public Affairs (OPA). The requesting EC must be reviewed by the CDC and approved by the SAC after coordinating the request with the local USAO. The EC must contain the necessary facts and investigative justification for the interview consistent with the DOJ guidelines set forth in 28 CFR § 50.10(f). See also the AG Memorandum "Updated Policy Regarding Obtaining Information From, or Records Of, Members of the News Media; and Regarding Questioning, Arresting, or Charging Member of the News Media" (February 2014), 28 CFR § 50.10, and the AG Memoranudm "Updated Policy Regarding Obtaining Information From, or Records Of, Members of the News Media; and Regarding Questioning, Arressting, Or Charging Member of the News Media" (January 2015).

(U) *Note:* 28 CFR § 50.10(b)(1)(ii) provides guidance on categories of individuals and entities not covered under the requirements set out above.

18.5.6.4.8.1.1 ***(U) EXIGENT CIRCUMSTANCES***

(U) [redacted] may authorize the questioning of a member of the news media as described in DIOG subsection *18*.5.6.4.8.1 if he/she determines that exigent use of such a technique is necessary [redacted] b7E

(U) [redacted] b7E

(U) See also the AG Memorandum "Updated Policy Regarding Obtaining Information From, or Records Of, Members of the News Media; and Regarding Questioning, Arresting, or Charging Member of the News Media" (February 2014), 28 CFR § 50.10, and the AG Memoranudm "Updated Policy Regarding Obtaining Information From, or Records Of, Members of the News Media; and Regarding Questioning, Arressting, Or Charging Member of the News Media" (January 2015).

18.5.6.4.8.2 **(U) USE OF SUBTERFUGE WITH A MEMBER OF THE NEWS MEDIA**

(U//~~FOUO~~) To the extent operational needs allow, investigators must operate openly and consensually with members of the news media. [redacted] b7E

After consultation with the OPA and OGC, the AD of the operational division must decide whether to approve the request. If the request requires approval by DOJ (because the interview is related to an offense committed by the member of the news media during the course of news gathering) the AD of the operational division is responsible for submitting all requests for approval to the DOJ per 28 CFR 50.10.

(U//~~FOUO~~) FBIHQ operational division PGs may contain additional notice requirements.

18.5.6.4.9 *(U) DURING AN ASSESSMENT - REQUESTING INFORMATION WITHOUT REVEALING FBI AFFILIATION OR THE TRUE PURPOSE OF A REQUEST*

A) (U//~~FOUO~~) In the normal course of an interview, an FBI employee should divulge the employee's affiliation with the FBI and the true purpose of the interview. b7E

B) (U//~~FOUO~~)

C) (U//~~FOUO~~)

D) (U//~~FOUO~~)

1) (U//~~FOUO~~) b7E

2) (U//~~FOUO~~)

3) (U//~~FOUO~~)

4) (U//~~FOUO~~)

5) (U//~~FOUO~~) officer;

6) (U//~~FOUO~~)

7) (U//~~FOUO~~)

(U//~~FOUO~~) b7E

(U//~~FOUO~~)

(U//~~FOUO~~)

b7E

(U//~~FOUO~~

18.5.6.4.10 ***(U) CONSULTATION AND DISCUSSION***

(U//~~FOUO~~

b7E

18.5.6.4.11 ***(U) EXAMPLES***

18.5.6.4.11.1 **(U) EXAMPLE 1**

b7E

(U//~~FOUO~~

(U//~~FOUO~~) Answer:

18.5.6.4.11.2 **(U) EXAMPLE 2**

b7E

(U//~~FOUO~~

(U//~~FOUO~~) Answer

18.5.6.4.11.3 **(U) EXAMPLE 3**

(U//~~FOUO~~)

b7E

(U//F~~OUO~~) Answer

18.5.6.4.11.4 **(U) EXAMPLE 4**

(U//~~FOUO~~

b7E

(U//~~FOUO~~) Answer:

18.5.6.4.11.5 **(U) EXAMPLE 5**

(U//F~~OUO~~)

b7E

(U//~~FOUO~~) Answer:

18.5.6.4.11.6 **(U) EXAMPLE 6**

(U//~~FOUO~~)

b7E

b7E

(U//F~~OUO~~) Answer:

18.5.6.4.11.7 **(U) EXAMPLE 7**

b7E

(U//F~~OUO~~)

(U//F~~OUO~~) Answer:

18.5.6.4.11.8 **(U) EXAMPLE 8**

b7E

(U//F~~OUO~~)

(U//F~~OUO~~) Answer:

18.5.6.4.11.9 **(U) EXAMPLE 9**

b7E

(U//F~~OUO~~)

b7E

(U//~~FOUO~~) Answer

18.5.6.4.12 ***(U//~~FOUO~~) PREDICATED INVESTIGATIONS - REQUESTING INFORMATION WITHOUT REVEALING FBI AFFILIATION OR THE TRUE PURPOSE OF A REQUEST***

(U//~~FOUO~~) In the normal course of an interview, the FBI employee should divulge the employee's affiliation with the FBI and the true purpose of the interview

b7E

(U//~~FOUO~~)

18.5.6.4.13 ***(U) INTERVIEWS OF PARTICULARLY VULNERABLE VICTIMS***

(U//~~FOUO~~) Interviews of some victims and witnesses require additional consideration so that FBI employees can elicit accurate information while minimizing potential trauma.

(U//~~FOUO~~) In accordance with the *Attorney General Guidelines for Victim and Witness Assistance (AGG-VWA)*, the FBI must utilize personnel properly trained in forensic interviewing techniques when a minor victim or witness[62] is interviewed, absent exceptional operational circumstances (as defined by the *Victim Services Policy Guide* [1010PG]). A forensic interview may also be appropriate for a victim or witness (of any age) who reports that he or she was victimized as a minor or who is cognitively impaired.

(U//~~FOUO~~) If a Child and Adolescent Forensic Interviewer (CAFI) is unavailable to conduct a forensic interview, other professional interviewers employed by child advocacy centers (CAC) may be utilized. A CAFI may refer the case agent to a CAC forensic interviewer. The complete policy and procedures for conducting forensic interviews are located in the *Victim Services Policy Guide* (1010PG), which also includes procedures for exceptional operational circumstances.

[62] (U) Defined as a victim or witness who is under the age of 18 years.

(U//~~FOUO~~) Whenever feasible and appropriate under the circumstances of an investigation, FBI personnel should obtain consent to conduct an interview from the parent/guardian of a minor victim or witness, or the guardian/caregiver of a cognitively impaired adult victim or witness.

(U//~~FOUO~~) FBI employees should consider all of the following factors when conducting forensic interviews:

A. (U//~~FOUO~~) The age, mental health, exposure to trauma, maturity, and competency of the victim or witness
B. (U//~~FOUO~~) Whether the victim or witness is an emancipated minor
C. (U//~~FOUO~~) The victim's or witness's relationship to the suspect(s)
D. (U//~~FOUO~~) Safety concerns
E. (U//~~FOUO~~) The gravity of the offense at issue
F. (U//~~FOUO~~) Any alternative sources of evidence
G. (U//~~FOUO~~) The importance of the information or potential testimony to the investigation
H. (U//~~FOUO~~) The victim's or witness's degree of involvement, if any, with the offense under investigation

(U//~~FOUO~~) An interview of a minor or vulnerable victim by a Special Agent or TFO must take place in person unless an exceptional operational circumstance exists and is properly approved in accordance with subsection 4.4.3.2 of the *Victim Services Policy Guide* (1010PG).

(U//~~FOUO~~) CAFI interviews should take place in person unless an exceptional operational circumstance exists and a remote interview (i.e. by telephone or video conference) is approved in accordance with subsection 4.4.3.2 of the *Victim Services Policy Guide* (1010PG).

18.5.6.4.14 *(U) Interviews of Juvenile Subjects*

18.5.6.4.14.1 (U) Custodial Interviews (No Arrest)

(U//~~FOUO~~) If a juvenile is not placed under arrest, but is deemed to be "in custody" based on the objective circumstances surrounding the interview, the interviewer must advise the juvenile of his or her rights as set forth on the FD-395 before beginning an interview and cease the interview if the juvenile invokes a right. See DIOG subsection 18.5.6.4.1.

(U//~~FOUO~~) In determining whether a juvenile is in custody, agents must apply an objective test: Was there a formal arrest or a deprivation of freedom of movement equivalent to an arrest? If the juvenile's age is known to the interviewer or is objectively apparent, the juvenile's age must be considered in the custody analysis. Age is not necessarily the determining or decisive factor in every case, but should be carefully considered given that a reasonable adult may view the circumstances surrounding the interview differently than a reasonable juvenile.

18.5.6.4.14.2 (U) Interviews Between Arrests for Federal Offenses and Initial Appearances Before Magistrate Judges

(U//~~FOUO~~) The requirements of the Juvenile Delinquency Act apply after a juvenile, as defined by federal law, is arrested for a federal offense. See DIOG subsection 19.12 for policy on arrests of juveniles.

(U) An act of juvenile delinquency is defined as a violation of 18 U.S.C. § 922(x)(2) or a violation of a federal law by an individual who has not attained his or her 18th birthday, which would have been a crime if committed by an adult. For the purpose of juvenile delinquency proceedings, a juvenile delinquent (i.e., a juvenile subject) is an individual who committed a crime before his or her 18th birthday who has not attained his or her 21st birthday at the time charges are commenced.

(U//~~FOUO~~) Whether a juvenile may be interviewed for a confession or admission of his or her own guilt between the time of arrest for a federal offense and the initial appearance before the magistrate depends on the law of the circuit in which the arrest occurs and requires the approval of a CDC or an AUSA.

A. (U//~~FOUO~~) If a CDC or an AUSA approves an interview of a juvenile based on the law of the circuit, the juvenile may waive his or her Fifth Amendment rights and consent to an interview. Whether a waiver is knowing and voluntary will be determined based on the totality of the circumstances surrounding the interview. Among the factors the court will likely consider are:

   i. (U//~~FOUO~~) The juvenile's age, experience, education, background, and intelligence.
   ii. (U//~~FOUO~~) Whether the juvenile has the capacity to understand the warnings given, the nature of Fifth Amendment rights, and the consequences of waiving them.

   (U//~~FOUO~~) The presence and co-signature of a parent or guardian during the waiver of rights (FD-395) may not necessarily be required for a voluntary waiver, but is always a significant factor to be considered and tends to dispel claims of coercion.

   (U//~~FOUO~~) An agent may also question a juvenile concerning the guilt of a third party if such questioning does not cause any delay in bringing the juvenile before the magistrate.

   (U//~~FOUO~~) When an agent conducts a custodial interview of an arrested juvenile prior to initial appearance and while in a place of detention with suitable recording equipment, the interview must be recorded in accordance with DIOG subsection 18.5.6.4.17.3.

B. If the interview is <u>not</u> allowed under the law of the circuit, information volunteered by the arrested juvenile concerning his or her own guilt should be recorded in the agent's notes for use in subsequent proceedings. Any questions concerning the law that applies in the particular circuit should be directed to the CDC or AUSA.

18.5.6.4.14.3 (U) INTERVIEWS OF JUVENILES UNDER ARREST BY NON-FEDERAL LAW ENFORCEMENT

(U//~~FOUO~~) The requirements of the Juvenile Delinquency Act, as described in subsections 18.5.6.4.14.2 and 19.12 only apply when a juvenile (as defined by federal law) is arrested for a federal offense. Therefore, Juvenile Delinquency Act requirements do not apply if a juvenile is suspected of having committed a federal offense but is under arrest by state or local law enforcement officers on a state or local charge. FBI employees are cautioned, however, that they may not collude or create the appearance of collusion with non-federal officers to delay an arrest on federal charges to circumvent the Juvenile Delinquency Act requirements. Agents should consult a CDC or AUSA as to the advisability of a juvenile interview under the particular circumstances.

18.5.6.4.15 *(U) DOCUMENTATION*

(U//F~~OUO~~) When it is anticipated that the results of an interview may become the subject of court testimony, the interview must be recorded on an FD-302 (or FD-1023 for debriefing of CHSs). See DIOG subsection 18.5.6.4.16 below for guidance on the use of the FD-302. The FD-302 must contain a record of statements made by the interviewee and not contain the interviewer's opinion or contextual comments. If the interviewer's opinions or contextual comments are relevant, they must be documented in an EC or other appropriate document.

(U) If the interviewee characterizes an individual, group, or activity in a certain way, FBI records (i.e., 302s, ECs, LHMs) should reflect that the interviewee, not the FBI, is the source of the characterization.

(U//F~~OUO~~) Certain types of written material developed during the course of an interview must be retained including:

A) (U//~~FOUO~~) Written statements signed by the witness. When possible, written statements should be taken in all investigations in which a confession or admission of guilt is obtained unless the confession is obtained during an electronically-recorded interview session. If a witness gives a signed statement, and then gives additional information orally, both the signed statement and the oral information should be recorded on an FD-302 or [redacted] b7E

B) (U//~~FOUO~~) Written statements, unsigned by the witness, but approved or adopted in any manner by the witness. An example of such a written statement would be a written statement that the subject orally admits is true but will not sign; and

C) (U//~~FOUO~~) Original notes of an interview when the results may become the subject of court testimony. Materials generated via email, text messages, or similar means during an online interview must be retained as original notes. Because some forms of synchronous communication tools, such as text messaging, have limited or no storage, print, or production capabilities, they should not be used for substantive communications with law enforcement colleagues or civilians who may become witnesses. **If these tools are, nonetheless, used for substantive communications as part of an interview, the communications must be memorialized verbatim in an FD-302**.

D) (U//~~FOUO~~) If an FBI employee and an AUSA conduct an interview, and the AUSA asks or tells the FBI employee to refrain from recording the substance of the interview or taking notes, the FBI employee should decline to participate in the interview and should not be present when it takes place unless the interview is part of the trial preparation of the witness (or unless another law enforcement agent present is given the responsibility for taking notes and

documenting the substance of the interview). FBI employees generally do not report the substance of trial preparation unless new material information or impeachment information is developed. FBI employees should consult with the trial AUSA to determine how to document any new information, including impeaching information, developed during the trial preparation interviews.

E) (U) [redacted] b7E

[redacted]

(U) See also DIOG subsection 3.3.1.14 (Retain Original Notes Made During An Investigation).

(U//~~FOUO~~) All original handwritten interview notes must be retained as "original note material" in the 1A section of a file. The original handwritten notes may be scanned, but the physical original handwritten notes must be retained regardless of whether or not the notes are scanned. Also see the *Importing Nontransitory Records into Sentinel and Preserving Certain Investigative Nontransitory Records in Original Formats* (1001D) policy directive.

18.5.6.4.16 *(U) USE OF THE FD-302*

(U) **Documenting Information of Record:** Any matter that may be testimonial must be documented using an FD-302 within Sentinel[63]. [redacted] b7E

[redacted]

(U) Whenever a person being interviewed could be called upon to testify at any time in a future trial, or hearing, the results of the interview must be reported in an FD-302.

(U) All FBI employees present during an interview [redacted] b7E must be identified by name on the FD-302. The employee preparing the FD-302 is listed as the author of the document and all other employees present must be listed as co-authors. The author and co-author(s) of the FD-302 must review the FD-302, and then electronically sign the final FD-302 in Sentinel to attest it is accurate and complete. If someone other than an FBI employee and co-author(s) are present during the interview, [redacted] the third party's presence during all or part of the interview must be noted in the FD-302.

(U) The FD-302 opening paragraph must state the official identity of the interviewing agent(s), the purpose of the interview, and the identity of the individual being interviewed to include relevant identifying information such as a date of birth, address, or other identifying data. It is also permissible to place more details or extensive personal, biographical, criminal

[63] (U) [redacted] b7E

[redacted]

history, business related information, other agency record information, etc. in the body or at the end of the report. When an ongoing interview is carried out over a period of days, the dates should also be set out in the details of the FD-302. In such cases, the report should clearly delineate the particular date(s) the information was obtained. A composite interview report may be utilized in certain circumstances (see "composite FD-302" below for additional guidance).

(U) If during an interview, the interviewee provides unrelated information relevant to other criminal, national security, intelligence, or public safety matters from the original purpose of the interview, the interviewer may take the information. When documenting such unrelated information, each topic must be documented in a separate FD-302, filed to the appropriate investigative classification, and disseminated as appropriate.

(U) The preparation of the FD-302 must be initiated as soon as practicable [redacted] following the conclusion of the interview or other activity that may be testimonial. b7E

(U) Interview notes must be retained in accordance with DIOG subsections 3.3.1.14 and 18.5.6.4.15 above.

(U) **Composite FD-302**: In limited situations involving an extended or a series of related interviews of a subject, witness, or victim, the preparation of a composite FD-302 may be necessary. Preparation of a composite FD-302 at the conclusion of the interview may be the most logical and orderly way in which to document the totality of the interview. In these situations, in the judgment of the interviewer, a single composite FD-302 might be appropriate when:

(U) [redacted] b7E

(U) [redacted]

(U) [redacted]

(U) [redacted]

(U) [redacted]

(U) If agents elect to prepare a composite FD-302, they must, without exception, ensure the composite FD-302 captures all material information in the extended interviews, including that which may also be considered exculpatory or impeaching. This includes, but is not limited to, any materially inconsistent statements of the witness and anything that may tend to mitigate guilt or punishment of the accused.

(U) The preparation of the composite FD-302 must be initiated as soon as practicable, [redacted] following the conclusion of the last interview. b7E

(U) Interview notes must be retained in accordance with DIOG subsections 3.3.1.14 and 18.5.6.4.15.

(U) **Adoption of an FD-302**: In consultation with the assigned AUSA or DOJ attorney, the agent may seek to have the interviewee adopt an FD-302 as the statement he/she intended to give. Adoption by the witness may be in the form of (1) a signed statement, (2) an unsigned statement adopted by oral declaration, or (3) the report of information furnished by the witness, the substance of which was reviewed fully with the witness and adopted by the interviewee as the full and correct report of the statement he/she desired to furnish. Should the witness adopt an FD-302 as their statement, the agent must have the witness declare that it represents a full and correct report of their statement and then sign and date the first page of the FD-302, including any corrections, edits or additions he/she make on that page. The witness should also initial and date each subsequent page of the report and also make any corrections, edits or additions to the FD-302. The adoption of the FD-302 by the witness can provide a defense to any allegations that the FD-302 represents information the interviewer claims the witness said, rather than what the witness actually stated. The original (i.e. physical paper version) FD-302 adopted by the witness should be retained in the 1A section of the investigative file after it has been scanned and electronically placed into the relevant investigative file(s).

18.5.6.4.17 *(U) Electronic Recording of Interviews*

18.5.6.4.17.1 (U) Overview

(U)

(U//~~FOUO~~)

b7E

(U//~~FOUO~~)

(U//~~FOUO~~)

18.5.6.4.17.2 (U) RECORDED NONCUSTODIAL INTERVIEWS

18.5.6.4.17.2.1 *(U) OVERTLY RECORDED NONCUSTODIAL INTERVIEWS*

(U//~~FOUO~~) FBI employees have the option to conduct an overtly recorded noncustodial interview. An overtly recorded interview occurs when an FBI employee, identified as such, advises the interviewee that the interview is or will be recorded, or the interviewee is otherwise clearly aware that the interview is in fact being recorded [redacted] b7E

[redacted]

(U//~~FOUO~~) The FBI employee must provide notification to [redacted] as soon as practicable, [redacted] after completion of an overtly recorded noncustodial interview(s). The notification may be in the form of the interview summary FD-302 described in DIOG subsection 18.5.6.4.17.2.2 below. b7E

(U//~~FOUO~~) Additionally, prior to conducting the interview, the interviewing employee should consider the factors listed below [redacted] b7E

[redacted]

A. (U//~~FOUO~~) Whether the purpose of the interview is to gather evidence for prosecution or intelligence for analysis or both;
B. (U//~~FOUO~~) If prosecution is anticipated, the type and seriousness of the crime, including, in particular, whether the crime requires mens rea, or a mental element, such as knowledge or intent to defraud, proof of which would be considerably aided by the interviewee's admissions in his/her own words;
C. (U//~~FOUO~~) Whether the interviewee's own words and appearance (in video recordings) would help rebut any doubt about the meaning, context or voluntariness of his/her statement or confession raised by his/her age, mental state, educational level, or understanding of the English language; or is otherwise expected to be an issue at trial, such as to rebut an insanity defense; or may be of value to behavioral analysts;
D. (U//~~FOUO~~) If interviewers anticipate that the interviewee might be untruthful during an interview, whether a recording of the false statement would enhance the likelihood of charging and convicting the person for making a false statement;
E. (U//~~FOUO~~) The insufficiency of other available evidence to prove the charge beyond a reasonable doubt;
F. (U//~~FOUO~~) The preference of the USAO and the Federal District Court regarding recorded interviews or confessions;
G. (U//~~FOUO~~) Local laws and practice—particularly in task force investigations where state prosecution is possible;
H. (U//~~FOUO~~) Whether interviews with other witnesses or subjects in the same or related investigations have been electronically recorded; and
I. (U//~~FOUO~~) The potential to enlist the witness or subject's cooperation and the value of using his/her own words to elicit his/her cooperation.

18.5.6.4.17.2.2 *(U) OVERTLY RECORDED NONCUSTODIAL INTERVIEW: DOCUMENTATION AND HANDLING*

(U//~~FOUO~~) After completing the recorded interview, the agent must document in an FD-302 the fact that the interview took place. b7E

(U)

(U//~~FOUO~~)

(U//~~FOUO~~) b7E

(U//~~FOUO~~) Any handwritten notes taken during the recorded interview must be retained as original note material. See also DIOG Section 3.3.1.14 ("Retain Original Notes during an Investigation").

18.5.6.4.17.2.3 *(U) SURREPTITIOUSLY RECORDED NONCUSTODIAL INTERVIEWS*

(U//~~FOUO~~) b7E

b7E

18.5.6.4.17.2.4 ***(U) SURREPTITIOUSLY RECORDED NONCUSTODIAL INTERVIEW: DOCUMENTATION AND HANDLING***

(U//~~FOUO~~)

b7E

(U

(U//~~FOUO~~)

(U//~~FOUO~~)

(U//~~FOUO~~)

18.5.6.4.17.3 (U) CUSTODIAL RECORDED INTERVIEWS (WARRANT/PROBABLE CAUSE)

18.5.6.4.17.3.1 *(U) OVERVIEW*

(U//~~FOUO~~) There is a presumption that statements made by persons in FBI custody must be recorded following arrest and prior to initial appearance when the arrestee is in a place of detention with suitable recording equipment. All statements made during a custodial interview of persons arrested by the FBI for federal crimes,[64] prior to initial appearance and while in a place of detention with suitable recording equipment, must be electronically recorded (with very limited exceptions as listed in DIOG subsection 18.5.6.4.17.4, below)

b7E

(U//~~FOUO~~)

For factors bearing on voluntariness, see DIOG subsection 18.5.6.3. For factors bearing on Miranda compliance, see DIOG subsection 18.5.6.4.1.1

(U//~~FOUO~~) Employees must use suitable equipment as approved by

(U//~~FOUO~~)

b7E

(U//~~FOUO~~)

[64] This policy does not apply to a person arrested for a state or local crime during a joint or Task Force investigation.

b7E

18.5.6.4.17.3.2 ***(U) OVERTLY RECORDED CUSTODIAL INTERVIEWS***

(U//~~FOUO~~) FBI employees may conduct an overtly recorded custodial interview. An overtly recorded custodial interview occurs when an FBI employee, identified as such, advises the interviewee that the interview is or will be recorded, or the interviewee is otherwise clearly aware that the interview is in fact being recorded.

b7E

18.5.6.4.17.3.3 ***(U) OVERTLY RECORDED CUSTODIAL INTERVIEW: DOCUMENTATION AND HANDLING***

(U//~~FOUO~~) After completing the recorded interview, the agent must document in an FD-302 the fact that the interview took place.

b7E

(U) Transcription of the recording is optional. The FBI will provide electronic copies for distribution pre-indictment. Post-indictment, the USAO will pay for transcripts of recordings as necessary.

(U//~~FOUO~~) Any handwritten notes taken during the recorded interview must be retained as original note material. See DIOG Section 3.3.1.14 ("Retain Original Notes during Investigation").

(U//~~FOUO~~)

b7E

18.5.6.4.17.3.4 ***(U) SURREPTITIOUSLY RECORDED CUSTODIAL INTERVIEWS***

(U//~~FOUO~~) FBI employees may conduct a surreptitiously recorded custodial interview. b7E

18.5.6.4.17.3.5 ***(U) SURREPTITIOUSLY RECORDED CUSTODIAL INTERVIEW: DOCUMENTATION AND HANDLING***

(U//~~FOUO~~) After completing the recorded interview, the agent must document in an FD-302 the fact that the interview took place. b7E

(U) Transcription of the recording is optional. The FBI will provide electronic copies for distribution pre-indictment. Post-indictment, the USAO will pay for transcripts of recordings as necessary.

(U//~~FOUO~~) Any handwritten notes taken during the recorded interview must be retained as original note material. See DIOG Section 3.3.1.14 ("Retain Original Notes during Investigation").

(U//~~FOUO~~) b7E

18.5.6.4.17.4 (U) EXCEPTIONS TO MANDATORY RECORDING OF POST-ARREST CUSTODIAL INTERVIEWS

(U//~~FOUO~~) Unless conducted pursuant to prior written approval, the interviewing employee must document in an EC, as soon as practicable, [redacted] after the completion of the interview, the exercise of an exception to the mandated requirement to record a custodial post-arrest interview. The EC must be captioned, [redacted] and must specifically address the reason(s) why the interview was not recorded [redacted] Upon [redacted] approval, the EC must be electronically placed into the substantive investigative case file, and a notification copy sent to the FBIHQ operational unit with program responsibility over the investigative classification, appropriate OGC/ILU or NLSB Unit, and to the Division's Compliance Officer. For tracking purposes and for a periodic review by DOJ, the EC must be electronically placed into file [redacted] A copy of this EC documenting the basis for utilizing an exception to the mandatory recording of post-arrest custodial recorded interview policy must be made available to the AUSA by the "office of origin" field office overseeing the investigation. b7E

A. (U//~~FOUO~~) Refusal of subject to be recorded during the interview: If the subject is advised that the interview will be recorded and they indicate that they are willing to provide a statement but wish not to be recorded, then the recording need not take place.
   a. (U//~~FOUO~~) [redacted] b7E

B. (U//~~FOUO~~) Public Safety Exception: If the questioning is reasonably prompted by an immediate concern for the safety of the public or the arresting agent under New York v. Quarles then recording is not mandatory (see, e.g. DIOG 18.5.6.4.1.3).

C. (U//~~FOUO~~) [redacted] b7E

   a. (U//~~FOUO~~) [redacted]

b. (U//F~~OUO~~

b7E

c. (U//F~~OUO~~)

d. (U//F~~OUO~~)

i. (U//F~~OUO~~)

ii. (U//F~~OUO~~)

iii. (U//F~~OUO~~)

iv. (U//F~~OUO~~)

b7E

v. (U//F~~OUO~~)

vi. (U//F~~OUO~~)

e. (U//F~~OUO~~) This is not meant to be an exhaustive list and other considerations may counsel in favor of

b7E

D. (U//~~FOUO~~) Recording is not reasonably practicable: In the event that the circumstances of the arrest does not allow for the recording of the interview such as law enforcement safety, equipment malfunction, an unexpected need to move the interview from the detention center (i.e., medical facility), or a need for large-scale take downs with multiple interviews in a limited timeframe exceeding the number of recording facilities.
E. (U//~~FOUO~~) "Residual" Exception: The ADIC/SAC and the United States Attorney, or their designees, agree that a significant and articulable law enforcement (e.g., avoiding disclosure of a sensitive law enforcement technique) purpose requires not recording the interview. Some considerations may include the potential safety and welfare of a CHS. This exception is to be used judiciously and very infrequently.

18.5.6.4.17.5 (U) ELECTRONICALLY RECORDED INTERVIEW QUICK REFERENCE GUIDE

(U//~~FOUO~~) See the Electronically Recorded Interview quick reference guide (QRG) in the IPO's QRG Library.

18.5.6.4.18 *(U) INTERVIEWS RELATING TO CLOSED FILES*

(U//~~FOUO~~) An interview initiated by an employee should only be conducted if it is within the scope of an open authorized Assessment or predicated investigation. On the other hand, there are situations in which an individual contacts the FBI to report information concerning a matter that has been closed or placed in a zero file classification, or is unrelated to any current or previous investigation. In these situations, an FBI employee may collect whatever information the person is willing to provide, except solely First Amendment information, and may document the results of the contact in a Guardian FD-71a, an EC, or an FD-302. These documents may be electronically placed in files that are relevant to an open Assessment or predicated investigation, a closed Assessment or predicated investigation, a zero classification file, or a control file (if no further investigative activity is required).

(U//~~FOUO~~) [redacted] b7E

[redacted]

18.5.6.4.19 *(U) FBIHQ OPERATIONAL DIVISION REQUIREMENTS*

A) (U//~~FOUO~~) *Counterintelligence Division* [redacted] b7E

[redacted]

B) (U//~~FOUO~~) *Other FBIHQ Divisions:* Each FBIHQ division may provide additional interview notice requirements in its PG.

18.5.6.5 (U) USE/DISSEMINATION

(U//~~FOUO~~) The use or dissemination of information obtained by this method must comply with the AGG-Dom and DIOG Section 14.

18.5.6.6 (U//FOUO) OVERSEAS INTERVIEWS

(U//~~FOUO~~) Please see *DIOG Appendix I* [redacted] for policy governing all extraterritorial activities, including interviews. b7E

18.5.7 *(U) INVESTIGATIVE METHOD: INFORMATION VOLUNTARILY PROVIDED BY GOVERNMENTAL OR PRIVATE ENTITIES*

18.5.7.1 (U) SCOPE

(U//F~~OUO~~) An FBI employee may accept information voluntarily provided by federal, state, local, tribal, or foreign governmental or private entities and individuals. (AGG-Dom, Part II.A.4.g) Voluntarily provided information includes, but is not limited to, oral as well as documentary and physical evidence such as a computer hard drive or other electronic media that contains information, paper documents containing information, or physical objects (e.g., handgun or narcotics).

(U//F~~OUO~~) Nothing in this section prohibits asking for or accepting volunteered access to personal or real property.

(U//F~~OUO~~) *Note:* Consent Searches are authorized in Assessments, as well as predicated investigations.

(U//~~FOUO~~) *Note:* If the originator of information reported to the FBI characterizes an individual, group, or activity in a certain way, and that characterization should be documented for completeness of the FBI record, the FBI record (i.e., 302, EC, LHM) should reflect that another party, and not the FBI, is the originator of the characterization.

18.5.7.2 (U) APPLICATION

(U//F~~OUO~~) [redacted] b7E

[redacted]

18.5.7.3 (U) APPROVAL

(U//~~FOUO~~) Supervisory approval is not required to accept voluntarily provided information. Personnel may not request nor knowingly accept information where disclosure would be prohibited by federal law. See, e.g., 18 U.S.C. § 2702 (prohibiting an entity providing electronic communications services from divulging certain communications and other records, except in certain circumstances).

18.5.7.4 (U) USE/DISSEMINATION

(U//F~~OUO~~) The use or dissemination of information obtained by this method must comply with the AGG-Dom and DIOG Section 14.

This Page Is Intentionally Blank.