

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



DATE: 03-21-2013
CLASSIFIED BY NSICG F85M26K45
REASON: 1.4 (C, G)
DECLASSIFY ON: 03-21-2038

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

DOMESTIC INVESTIGATIONS AND OPERATIONS GUIDE

FEDERAL BUREAU OF INVESTIGATION
RELEASED OCTOBER 15, 2011
UPDATED JUNE 15, 2012

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.

ACLU EC-105

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

~~SECRET~~

NOTICE OF SUPERSESSION AND UPDATE:

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

Updated pages are denoted with “Version Dated: June 15, 2012”

CONTACT INFORMATION:

**Questions or comments pertaining to the DIOG can be directed to:
The Resource Planning Office (RPO), Corporate Policy Office (CPO) at
HQ_DIV00_CORPORATE_POLICY_OFFICE
or the Office of the General Counsel (OGC)**

PRIVILEGED INFORMATION:

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

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

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

ACLU EC-106

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.....	2-2
2.2.1 (U) Conduct Investigations and Collect Intelligence and Evidence.....	2-2
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	2-3
2.4.1 (U) Introduction.....	2-3
2.4.2 (U) Terrorism and Counterterrorism Investigations	2-3
2.4.3 (U) Counterintelligence and Espionage Investigations	2-8
2.4.4 (U) Criminal Investigations.....	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	2-10
2.6.4 (U) Records of Departures from the AGG-Dom	2-11
2.7 (U) Departures from the DIOG	2-11
2.7.1 (U) Definition	2-11
2.7.2 (U) Departure from the DIOG.....	2-11
2.7.3 (U) Emergency Departures from the DIOG.....	2-11
2.7.4 (U) Records of Departures from the DIOG.....	2-12
2.8 (U) Discovery of Non-compliance with DIOG Requirements after-the-fact	2-12
2.8.1 (U) Substantial Non-Compliance with the DIOG	2-12
2.8.2 (U) Documentation of Substantial non-Compliance	2-13

16.6 (U) Requests for Approval of Undisclosed Participation 16-10

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 16-12

16.9 (U) FBIHQ Approval Process of UDP Requests 16-12

 16.9.1 (U) Submitting the UDP request to FBIHQ 16-12

 16.9.2 (U//FOUO) [REDACTED] 16-13

 16.9.3 (U//FOUO) [REDACTED] 16-13 b7E

 [REDACTED] 16-13

 16.9.4 (U//FOUO) Procedures for approving emergency UDP requests that otherwise require FBIHQ approval 16-14

16.10 (U) UDP Examples 16-15

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) OIA in Undercover Activity 17-1

17.4 (U//FOUO) OIA by a Confidential Human Source (CHS) 17-2

17.5 (U//FOUO) Approval of OIA by a Special Agent in Charge (SAC) – Not including material Support of Terrorism 17-2

17.6 (U//FOUO) OIA Related to [REDACTED] 17-4 b7E

 [REDACTED] 17-4

17.7 (U//FOUO) Standards for Review and Approval of OIA 17-4

17.8 (U) OIA not authorized 17-4

17.9 (U) Emergency Situations 17-5

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

18.2 (U) Least Intrusive Method 18-3

18.5.8.4	(U) Other Physical Surveillance	18-43
18.5.8.5	(U) Maintain a “Surveillance Log” during Physical Surveillance.....	18-43
18.5.8.6	(U) Use/Dissemination.....	18-43
18.5.9	(U) Investigative Method: Grand Jury Subpoenas – for telephone or electronic mail subscriber information only (in Type 1 & 2 Assessments)	18-45
18.5.9.1	(U) Scope	18-45
18.5.9.2	(U) Application.....	18-45
18.5.9.3	(U) Approval	18-45
18.5.9.4	(U) Electronic Communications Privacy Act (ECPA) (18 U.S.C. §§ 2701-2712) ..	18-45
18.5.9.5	(U) Use/Dissemination.....	18-46
18.6	(U) Authorized Investigative Methods in Preliminary Investigations.....	18-47
18.6.1	(U) Investigative Method: Consensual Monitoring of Communications, including Electronic Communications	18-49
18.6.1.1	(U) Summary.....	18-49
18.6.1.2	(U) Application.....	18-49
18.6.1.3	(U) Legal Authority.....	18-49
18.6.1.4	(U) Definition of Investigative Method	18-49
18.6.1.5	(U) Standards and Approval Requirements for Consensual Monitoring	18-51
18.6.1.5.1	(U) General Approval Requirements.....	18-51
18.6.1.6	(U) Consensual Monitoring Situations Requiring Additional Approval.....	18-53
18.6.1.6.1	(U) Party Located Outside the United States.....	18-53
18.6.1.6.2	(U) Consent of More than One Party Required for Consensual Monitoring.....	18-53
18.6.1.6.3	(U) Sensitive Monitoring Circumstance	18-54
18.6.1.7	(U) Duration of Approval.....	18-57
18.6.1.8	(U) Specific Procedures	18-57
18.6.1.8.1	(U) Documenting Consent to Monitor/Record.....	18-57
18.6.1.8.2	(U) Documenting Approval	18-58
18.6.1.8.3	(U) Retention of Consensually Monitored Communications.....	18-58
18.6.1.8.4	(U) Multiple Communications	18-58
18.6.1.8.5	(U) Investigation Specific Approval	18-58
18.6.1.9	(U) Compliance and Monitoring	18-58
18.6.2	(U) Investigative Method: Intercepting the Communications of a Computer Trespasser	18-61
18.6.2.1	(U) Summary.....	18-61
18.6.2.2	(U) Application.....	18-61
18.6.2.3	(U) Legal Authority.....	18-61
18.6.2.4	(U) Definition of the Communications of a Computer Trespasser	18-61

- 18.6.2.5 (U//FOUO) Use and Approval Requirements for Intercepting the Communications of a Computer Trespasser..... 18-63
 - 18.6.2.5.1 (U) General Approval Requirements..... 18-63
- 18.6.2.6 (U) Duration of Approval for Intercepting the Communications of a Computer Trespasser..... 18-65
- 18.6.2.7 (U) Specific Procedures for Intercepting the Communications of a Computer Trespasser..... 18-65
 - 18.6.2.7.1 (U) Documenting Authorization to Intercept 18-65
 - 18.6.2.7.2 (U) Acquiring Only the Trespasser Communications..... 18-65
 - 18.6.2.7.3 (U) Reviewing the Accuracy of the Interception 18-66
 - 18.6.2.7.4 (U) Reviewing the Relevancy of the Interception 18-67
 - 18.6.2.7.5 (U) Duration of Approval..... 18-67
 - 18.6.2.7.6 (U) ELSUR Requirements 18-67
 - 18.6.2.7.7 (U) Multiple Communications 18-67
 - 18.6.2.7.8 (U) Investigation Specific Approval 18-67
- 18.6.2.8 (U) Compliance and Monitoring 18-67
- 18.6.3 (U) Investigative Method: Closed-Circuit Television/Video Surveillance, Direction Finders, and other Monitoring Devices..... 18-69
 - 18.6.3.1 (U) Summary..... 18-69
 - 18.6.3.2 (U) Application..... 18-69
 - 18.6.3.3 (U) Legal Authority..... 18-69
 - 18.6.3.4 (U) Definition of Investigative Method 18-69
 - 18.6.3.5 (U//FOUO) *Standards for Use and Approval* Requirements for Investigative Method..... 18-69
 - 18.6.3.6 (U) Duration of Approval..... 18-70
 - 18.6.3.7 (U) Specific Procedures 18-70
 - 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..... 18-71
 - 18.6.3.8.1 (U) Warrant or Court Order 18-71
 - 18.6.3.8.2 (U//FOUO) Required Consultation with Technical Advisor (TA) or Technically Trained Agent (TTA)..... 18-71
 - 18.6.3.9 (U) Evidence Handling..... 18-72
 - 18.6.3.10 (U) CCTV/Video Surveillance Equipment – Types, Availability, Repair And Disposal..... 18-72
 - 18.6.3.10.1 (U) Equipment Types..... 18-72
 - 18.6.3.10.2 (U) Equipment Availability..... 18-72
 - (U//FOUO) If CCTV/Video Surveillance equipment is not available from the existing field office inventory, the TA/TTA must use the [redacted] [redacted] b7E to forward requests to the appropriate VSU program manager (PM)..... 18-72
 - 18.6.3.10.3 (U) Equipment Repair..... 18-73

18.6.3.10.4 (U) Equipment Disposal.....	18-73
18.6.3.11 (U) Compliance and Monitoring	18-73
18.6.4 (U) Investigative Method: Administrative Subpoenas (compulsory process).....	18-75
18.6.4.1 (U) Overview of Compulsory Process.....	18-75
18.6.4.2 (U) Application.....	18-75
18.6.4.3 (U) Administrative Subpoenas	18-75
18.6.4.3.1 (U) Summary	18-75
18.6.4.3.2 (U) Legal Authority and Delegation.....	18-76
18.6.4.3.3 (U) Approval Requirements	18-78
18.6.4.3.4 (U) Limitations on Use of Administrative Subpoenas	18-79
18.6.4.3.5 (U) Compliance/Monitoring.....	18-82
18.6.5 (U) Investigative Method: Grand Jury Subpoenas (compulsory process)	18-85
18.6.5.1 (U) Overview of Compulsory Process.....	18-85
18.6.5.2 (U) Application.....	18-85
18.6.5.3 (U) Federal Grand Jury Subpoena	18-85
18.6.5.3.1 (U) Legal Authorities.....	18-85
18.6.5.3.2 (U) Scope	18-86
18.6.5.3.3 (U) Approval Requirements	18-86
18.6.5.3.4 (U) Duration of Approval.....	18-86
18.6.5.3.5 (U) Specific Procedures.....	18-86
18.6.5.3.6 (U) Notice and Reporting Requirements	18-87
18.6.5.3.7 (U) Grand Jury Proceedings—Generally	18-87
18.6.6 (U) Investigative Method: National Security Letter (compulsory process).....	18-97
18.6.6.1 (U) Overview of Compulsory Process.....	18-97
18.6.6.2 (U) Application.....	18-97
18.6.6.3 (U) National Security Letters	18-97
18.6.6.3.1 (U) Legal Authority	18-97
18.6.6.3.2 (U) Definition of Method.....	18-98
18.6.6.3.3 (U) Approval Requirements	18-98
18.6.6.3.4 (U) Standards for Issuing NSLs	18-99
18.6.6.3.5 (U) Special Procedures for Requesting Communication Subscriber Information	18-100
18.6.6.3.6 (U) Duration of Approval.....	18-100
18.6.6.3.7 (U) Specific Procedures.....	18-100
18.6.6.3.8 (U) Notice and Reporting Requirements	18-104
18.6.6.3.9 (U) Receipt of NSL Information	18-104
18.6.6.3.10 (U) Electronic Service and Electronic Returns of NSLs.....	18-106
18.6.6.3.11 (U) Dissemination of NSL Material.....	18-107

Domestic Investigations and Operations Guide

18.6.6.3.12	(U) Special Procedures for Handling Right to Financial Privacy Act Information	18-108
18.6.6.3.13	(U) Payment for NSL-Derived Information.....	18-108
18.6.7	(U) Investigative Method: FISA Order for Business Records (compulsory process)	18-109
18.6.7.1	(U) Overview of Compulsory Process.....	18-109
18.6.7.2	(U) Application.....	18-109
18.6.7.3	(U) Business Records Under FISA.....	18-109
18.6.7.3.1	(U) Legal Authority	18-109
18.6.7.3.2	(U) Definition of Method.....	18-109
18.6.7.3.3	(U) Approval Requirements	18-110
18.6.7.3.4	(U) Duration of Court Approval.....	18-110
18.6.7.3.5	(U) Notice and Reporting Requirements	18-110
18.6.7.3.6	(U) Compliance Requirements.....	18-110
18.6.7.3.7	(U) FISA Overcollection.....	18-110
18.6.8	(U) Investigative Method: Stored Wire or Electronic Communications and Transactional Records	18-111
18.6.8.1	(U) Summary.....	18-111
18.6.8.2	(U) Application.....	18-111
18.6.8.2.1	(U) Stored Data.....	18-111
18.6.8.2.2	(U) Legal Process	18-112
18.6.8.2.3	(U) Retrieval	18-112
18.6.8.2.4	(U) Basic Subscriber Information	18-112
18.6.8.2.5	(U) Preservation of Stored Data	18-112
18.6.8.2.6	(U) Cost reimbursement.....	18-113
18.6.8.3	(U) Legal Authority.....	18-113
18.6.8.4	(U) ECPA Disclosures	18-113
18.6.8.4.1	(U) Definitions	18-114
18.6.8.4.2	(U) Compelled Disclosure	18-114
18.6.8.4.3	(U) Voluntary Disclosure.....	18-120
18.6.8.5	(U) Voluntary Emergency Disclosure.....	18-123
18.6.8.5.1	(U) Scope	18-123
18.6.8.5.2	(U) Duration of Approval.....	18-124
18.6.8.5.3	(U) Specific Procedures.....	18-124
18.6.8.5.4	(U) Cost Reimbursement.....	18-125
18.6.8.5.5	(U) Notice and Reporting Requirements	18-125
18.6.8.5.6	(U) Reporting Voluntary Emergency disclosures	18-125
18.6.8.5.7	(U) Roles/Responsibilities.....	18-125
18.6.8.6	(U) Other Applicable Policies.....	18-126
18.6.9	(U) Investigative Method: Pen Registers and Trap/Trace Devices (PR/TT).....	18-127

ACLU EC-112

18.6.9.1	(U) Summary.....	18-127
18.6.9.2	(U) Application.....	18-127
18.6.9.3	(U) Legal Authority.....	18-127
18.6.9.4	(U) Definition of Investigative Method	18-127
18.6.9.5	(U) Standards for Use and Approval Requirements for Investigative Method ..	18-127
18.6.9.5.1	(U) Pen Register/Trap and Trace under FISA	18-127
18.6.9.5.2	(U) Criminal Pen Register/Trap and Trace under Title 18.....	18-129
18.6.9.6	(U) Duration of Approval.....	18-131
18.6.9.7	(U) Specific Procedures	18-131
18.6.9.8	(U) Use of FISA Derived Information in Other Proceedings.....	18-132
18.6.9.9	(U) Congressional Notice and Reporting Requirements	18-132
18.6.9.9.1	(U) Criminal Pen Register/Trap and Trace- Annual Report.....	18-132
18.6.9.9.2	(U) National Security Pen Registers and Trap and Trace – Semi-Annual Report.....	18-133
18.6.9.10	(U) Post Cut-Through Dialed Digits (PCTDD)	18-133
18.6.9.10.1	(U) Overview	18-133
18.6.9.10.2	(U) Collection of PCTDD.....	18-134
18.6.9.10.3	(U) Use of PCTDD.....	18-134
18.6.9.10.4	(U) What constitutes PCTDD content.....	18-135
18.6.9.11	(U//FOUO) [REDACTED] b7E	18-136
18.6.9.11.1	(U//FOUO) To Locate a Known Phone Number	18-136
18.6.9.11.2	(U//FOUO) To Identify an Unknown Target Phone Number	18-137
18.6.9.11.3	(U) PR/TT Order Language	18-138
18.6.10	(U) Investigative Method: Mail Covers.....	18-139
18.6.10.1	(U) Summary.....	18-139
18.6.10.2	(U) Application.....	18-139
18.6.10.3	(U) Legal Authority.....	18-139
18.6.10.4	(U) Definition of Investigative Method	18-139
18.6.10.5	(U) Standard for Use and Approval Requirements for Investigative Method	18-140
18.6.10.6	(U) Duration of Approval.....	18-142
18.6.10.7	(U) Storage of Mail Cover Information.....	18-142
18.6.10.8	(U) Return of Mail Cover Information to USPS	18-142
18.6.10.9	(U) Compliance and Monitoring	18-143
18.6.11	(U) Investigative Method: Polygraph Examinations.....	18-145
18.6.11.1	(U) Summary.....	18-145
18.6.11.2	(U) Application.....	18-145
18.6.11.3	(U) Legal Authority.....	18-145

18.6.11.4	(U) Standards for Use and Approval Requirements for Investigative Method ..	18-145
18.6.11.5	(U) Duration of Approval.....	18-145
18.6.11.6	(U) Specific Procedures.....	18-146
18.6.11.7	(U) Compliance and Monitoring	18-146
18.6.12	(U) Investigative Method: Trash Covers (Searches that Do Not Require a Warrant or Court Order)	18-147
18.6.12.1	(U) Summary.....	18-147
18.6.12.2	(U) Application.....	18-147
18.6.12.3	(U) Legal Authority.....	18-147
18.6.12.4	(U) Definition of Investigative Method	18-147
18.6.12.4.1	(U) Distinction between “Trash Covers” and Searches of Abandoned Property or Trash	18-147
18.6.12.4.2	(U) Determination of an Area of Curtilage Around a Home.....	18-148
18.6.12.5	(U) Standards for Use and Approval Requirements for Investigative Method ..	18-148
18.6.13	(U) Investigative Method: Undercover Operations.....	18-149
18.6.13.1	(U) Summary.....	18-149
18.6.13.2	(U) Legal Authority.....	18-149
18.6.13.3	(U) Definition of Investigative Method	18-149
18.6.13.3.1	(U) Distinction Between Sensitive Circumstance and Sensitive Investigative Matter	18-150
18.6.13.4	(U//FOUO) Standards for Use and Approval Requirements for Investigative Method.....	18-150
18.6.13.4.1	(U) Standards for Use of Investigative Method	18-150
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)	18-150
18.6.13.4.3	(U//FOUO) Approval Requirements for UCOs [REDACTED]	18-151
18.6.13.5	(U) Duration of Approval.....	18-152
18.6.13.6	(U) Additional Guidance.....	18-152
18.6.13.7	(U) Compliance and Monitoring, and Reporting Requirements.....	18-152
18.7	(U) Authorized Investigative Methods in Full Investigations	18-153
18.7.1	(U) Investigative Method: Searches – With a Warrant or Court Order (reasonable expectation of privacy)	18-155
18.7.1.1	(U) Summary.....	18-155
18.7.1.2	(U) Legal Authority.....	18-155
18.7.1.3	(U) Definition of Investigative Method	18-156
18.7.1.3.1	(U) Requirement for Reasonableness	18-156
18.7.1.3.2	(U) Reasonable Expectation of Privacy	18-156

18.7.1.3.3	(U) Issuance of Search Warrant.....	18-156
18.7.1.3.4	(U) Property or Persons That May be Seized with a Warrant	18-157
18.7.1.4	(U) Approval Requirements for Investigative Method.....	18-161
18.7.1.5	(U) Duration of Approval.....	18-161
18.7.1.6	(U) Specific Procedures.....	18-161
18.7.1.6.1	(U) Obtaining a Warrant under FRCP Rule 41.....	18-161
18.7.1.6.2	(U) Obtaining a FISA Warrant	18-164
18.7.2	(U) Investigative Method: Electronic Surveillance – Title III.....	18-169
18.7.2.1	(U) Summary.....	18-169
18.7.2.2	(U) Legal Authority.....	18-169
18.7.2.3	(U) Definition of Investigative Method	18-169
18.7.2.4	(U) Title III Generally	18-169
18.7.2.5	(U) Standards for Use and Approval Requirements for Non-Sensitive Title IIIs.....	18-170
18.7.2.6	(U) Standards for Use and Approval Requirements for Sensitive Title IIIs.....	18-170
18.7.2.7	(U) Procedures For Emergency Title III Interceptions	18-171
18.7.2.7.1	(U) Obtaining Emergency Authorization	18-172
18.7.2.7.2	(U) Post-Emergency Authorization.....	18-173
18.7.2.8	(U) Pre-Title III Electronic Surveillance (ELSUR) Search Policy	18-174
18.7.2.9	(U) Duration of Approval for Title III.....	18-175
18.7.2.10	(U) Specific Procedures for Title III Affidavits.....	18-175
18.7.2.11	(U) Dispute Resolution for Title III Applications	18-176
18.7.2.12	(U) Notice and Reporting Requirements – Title III.....	18-176
18.7.3	(U) Investigative Method: Electronic Surveillance – FISA and FISA Title VII (acquisition of foreign intelligence information).....	18-179
18.7.3.1	(U) Summary.....	18-179
18.7.3.2	(U) Foreign Intelligence Surveillance Act (FISA).....	18-179
18.7.3.2.1	(U) Legal Authority	18-179
18.7.3.2.2	(U) Definition of Investigative Method.....	18-179
18.7.3.2.3	(U) Standards for Use and Approval Requirements for FISA.....	18-180
18.7.3.2.4	(U) Duration of Approval for FISA.....	18-181
18.7.3.2.5	(U//FOUO) Specific Procedures for FISA	18-181
18.7.3.2.6	(U) Notice and Reporting Requirements for FISA.....	18-183
18.7.3.2.7	(U) Compliance and Monitoring for FISA	18-183
18.7.3.2.8	(U) Special Circumstances for FISA.....	18-184
18.7.3.2.9	(U) FISA Overcollection.....	18-184
18.7.3.2.10	(U) Other Applicable Policies.....	18-184
18.7.3.3	(U) FISA Title VII (acquisition of foreign intelligence information)	18-184
18.7.3.3.1	(U) Summary	18-184

(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) [blank]

Appendix L: (U) On-Line Investigations

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

Appendix N: (U) Tax Return information

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

(U) PREAMBLE

August 17, 2011

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

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

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

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

(U) Thank you for your outstanding service!

Robert S. Mueller, III

Director

ACLU EC-117

xxix

1 (U) SCOPE AND PURPOSE

1.1 (U) SCOPE

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

- A) (U) *The Attorney General's Guidelines for Extraterritorial FBI Operations and Criminal Investigations;*
- B) (U) *The Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection (those portions which were not superseded by The Attorney General Guidelines for Domestic FBI Operations);*
- C) (U) *The Attorney General Guidelines on the Development and Operation of FBI Criminal Informants and Cooperative Witnesses in Extraterritorial Jurisdictions;*
- D) (U) *The Attorney General Procedure for Reporting and Use of Information Concerning Violations of Law and Authorization for Participation in Otherwise Illegal Activity in FBI Foreign Intelligence, Counterintelligence or International Terrorism Intelligence Investigations (August 8, 1988; and*
- E) (U) *Memorandum of Understanding Concerning Overseas and Domestic Activities of the Central Intelligence Agency and the Federal Bureau of Investigation (2005).*

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

1.2 (U) PURPOSE

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

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

(U) In addition to this policy document, each FBI Headquarters (FBIHQ) operational division has a Policy Implementation Guide (PG) or several PGs that supplement the DIOG. No policy or PG may contradict, alter, or otherwise modify the standards of the DIOG. Requests for DIOG modifications can be made to the Corporate Policy office (CPO) pursuant to DIOG Section 3.2.2 paragraphs (A), (B), (C) and (D). As a result, numerous FBI manuals, electronic communications, letterhead memoranda, and other policy documents are incorporated into the DIOG and operational division PGs, thus, consolidating FBI policy guidance.

ACLU EC-118

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

18.5.4 (U) On-line services and resources.

18.5.5 (U) CHS use and recruitment.

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

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

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

18.5.9 (U) Grand jury subpoenas – for telephone or electronic mail subscriber information only.

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) Trash Covers (Searches that do not require a warrant or court order).

ACLU EC-119

§18

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)

(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 – for telephone or electronic mail subscriber information only in Type 1 & 2 Assessments. (Section 18.5.9)

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

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

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

(U) Mail covers. (Section 18.6.10)

(U) National Security Letters. (Section 18.6.6)

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

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

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

(U) Polygraph examinations. (Section 18.6.11)

ACLU EC-120

18-2

- (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)
- (U) Searches – with a warrant or court order. (Section 18.7.1)
- (U) Stored wire and electronic communications and transactional records. (Section 18.6.8)
- (U) Trash Covers (Searches that do not require a warrant or court order). (Section 18.6.12)
- (U) Undercover Operations. (Section 18.6.13)

18.1.3 (U) GENERAL OVERVIEW

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

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

18.2 (U) LEAST INTRUSIVE METHOD

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

(U) Selection of the least intrusive means is a balancing test as to which FBI employees must use common sense and sound judgment to effectively execute their duties while mitigating the potential negative impact on the privacy and civil liberties of all people encompassed within the Assessment or Predicated Investigation, including targets, witnesses, and victims. This principle is not intended to discourage investigators from seeking relevant and necessary intelligence, information, or evidence, but rather is intended to encourage investigators to choose the least

ACLU EC-121

18.6 (U) AUTHORIZED INVESTIGATIVE METHODS IN PRELIMINARY INVESTIGATIONS

(U) See AGG-Dom, Part II.B and Part V.A.1-10.

(U) In Preliminary Investigations the authorized methods include the following:

- A) (U) The investigative methods authorized for Assessments:
 - 1) (U) Public information. (See Section 18.5.1)
 - 2) (U) Records or information - FBI and DOJ. (See Section 18.5.2)
 - 3) (U) Records or information - Other federal, state, local, tribal, or foreign government agency. (See Section 18.5.3)
 - 4) (U) On-line services and resources. (See Section 18.5.4)
 - 5) (U) CHS use and recruitment. (See Section 18.5.5)
 - 6) (U) Interview or request information from the public or private entities. (See Section 18.5.6)
 - 7) (U) Information voluntarily provided by governmental or private entities. (See Section 18.5.7)
 - 8) (U) Physical Surveillance (not requiring a court order). (See Section 18.5.8)
- B) (U) Consensual monitoring of communications, including electronic communications. (See Section 18.6.1)
- C) (U) Intercepting the communications of a computer trespasser. (See Section 18.6.2)
- D) (U) Closed-circuit television/video surveillance, direction finders, and other monitoring devices. (See Section 18.6.3)
- E) (U) Administrative subpoenas. (See Section 18.6.4)
- F) (U) Grand jury subpoenas. (See Section 18.6.5)
- G) (U) National Security Letters. (See Section 18.6.6)
- H) (U) FISA Order for business records. (See Section 18.6.7)
- I) (U) Stored wire and electronic communications and transactional records. (See Section 18.6.8)¹⁶
- J) (U) Pen registers and trap/trace devices. (See Section 18.6.9)
- K) (U) Mail covers. (See Section 18.6.10)
- L) (U) Polygraph examinations. (See Section 18.6.11)
- M)(U) Trash Covers (Searches that do not require a warrant or court order). (See Section 18.6.12)
- N) (U) Undercover operations. (See Section 18.6.13)

¹⁶ (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)

18.6.1 (U) INVESTIGATIVE METHOD: CONSENSUAL MONITORING OF COMMUNICATIONS, INCLUDING ELECTRONIC COMMUNICATIONS

18.6.1.1 (U) SUMMARY

(U) Monitoring of wire, oral or electronic communications based on the consent of one party to the communication is referred to as consensual monitoring. The consent exception applies to the interception of wire, oral, and electronic communications. Consensual monitoring requires review by the CDC or the OGC. (AGG-Dom, Part V.A.4)

18.6.1.2 (U) APPLICATION

(U//FOUO) [Redacted] b7E

(U//FOUO) [Redacted] b7E

(U//FOUO) The law of the state or territory where the consenting party is located when making the recording will govern whether OIA approval is needed.

(U//FOUO) See the OGC website for a list of all-party consent states. See also DIOG Section 18.6.1.6, below.

18.6.1.3 (U) LEGAL AUTHORITY

- A) (U) The Fourth Amendment to the United States Constitution and case law interpreting the same;
- B) (U) The Wiretap Statute, 18 U.S.C. § 2511-2522, prohibits the intentional interception and use of wire, voice, or electronic communications absent an exception;
- C) (U) The consensual monitoring exceptions, 18 U.S.C. § 2511(2)(c) & (d), require one party to the communication to consent to monitoring; and
- D) (U) The Foreign Intelligence Surveillance Act of 1978 (FISA), 50 U.S.C. §§ 1801 et seq. provides that if a party to the communication has consented to monitoring, a FISA court order is not required.

18.6.1.4 (U) DEFINITION OF INVESTIGATIVE METHOD

(U) Generally, the Wiretap Statute (also referred to as Title III), 18 U.S.C. §§ 2510-2522, prohibits the intentional interception of wire, oral, or electronic communications unless one of several exceptions applies. One such exception is based on the consent of a party to the communication. Two other statutory exceptions to the general prohibition include 1) the
ACLU EC-123

warrant or court order exception, and 2) the computer trespasser exception. This section discusses the monitoring of communications under the consent exception.

(U) Consensual monitoring is the monitoring of communications based on the consent of a party to the communication. (AGG-Dom, Part VII.A.) For purposes of this policy, at least one of the parties to the communication must be located, or the interception of the consensual communication must occur, within the United States or the United States territories. The consensual monitoring of communications is subject to legal review by the CDC or OGC, as applicable. (AGG-Dom, Part V.A.4). Consensual monitoring includes the interception of the content of communications and typically falls into one of three general categories:

- A) (U) Wire communications, which include conventional telephone communications or other means of transmitting the human voice through cable, wire, radio frequency (RF), voice over Internet Protocol (VoIP), or other similar connections;
- B) (U) Oral communications, typically intercepted through the use of devices that monitor and record oral conversations (e.g., a body transmitter or recorder or a fixed location transmitter or recorder used during face-to-face communications in which a person would have a reasonable expectation of privacy but for the consent of the other party); and
- C) (U) Electronic communications, which include any transfer of signs, signals, writing, images, sounds, data, or intelligence by a wire, radio, electronic, or optical system or network (e.g., e-mail, instant message, chat sessions, text messaging, non-voice peer-to-peer communications), as that term is defined in 18 U.S.C. § 2510(12)(14) and (17), which are intercepted and recorded at the time of transmission. The monitoring of electronic communications based on one party consent is sometimes referred to as "consensual computer monitoring." "Consensual computer monitoring" applies to "real time" electronic surveillance based on consent and does not include retrieving or obtaining records of communications that have been stored on the computer or elsewhere after the communication has occurred.

(U) Note regarding electronic communications monitoring: Agents seeking to consensually monitor electronic communications (specifically, communications to, through, or from a computer) must consider whether the party who has consented is a party to all of the communications they want to monitor or whether some of the communications involve a computer trespasser, as defined by the computer trespasser exception. (See DIOG Section 18.6.2) The trespasser exception and the consensual monitoring of communications exceptions are related, but separate, exceptions to the Wiretap Statute. The owner, operator, and authorized users of a protected computer or computer network can consent to the monitoring of only those communications they send or receive (i.e., to which they are a party), which typically does not include a trespasser's communications. The trespasser exception allows the interception of the communications transmitted to or from the trespasser.

(U) When applicable, the exceptions to the Wiretap Statute can be used together, permitting the interception of the communications of both authorized users and trespassers on the protected computer. This is particularly useful when it is difficult to discern the trespasser communications from other communications. If it is possible to obtain consent to monitor the communications of the authorized users, use of both the consent and trespasser exceptions together can mitigate the risk of over or under collection of the trespasser's communications.

18.6.1.5 (U) STANDARDS AND APPROVAL REQUIREMENTS FOR CONSENSUAL MONITORING

18.6.1.5.1 (U) GENERAL APPROVAL REQUIREMENTS

(U//FOUO) Except as provided below, an SSA may approve the consensual monitoring of communications if the information likely to be obtained is relevant to an ongoing Predicated Investigation. SSA approval, documented through the FD-759, is conditioned on the following criteria being met and documented on the FD-759 and other supporting documentation:

18.6.1.5.1.1 (U) REASONS FOR MONITORING

(U//FOUO) The synopsis must include sufficient factual information supporting the need for the monitoring. It must provide the relationship between the monitoring and the investigative purpose (e.g., obtain evidence of drug trafficking, public corruption, etc.).

18.6.1.5.1.2 (U) DOCUMENTED CONSENT OF A PARTY TO THE COMMUNICATION TO BE MONITORED

(U//FOUO) Consent must be obtained from one of the parties to be monitored, and the consent must be documented to the appropriate investigative ELSUR sub-file. Having the consent of one of the parties provides an exception to the Title III statute. The requirement to obtain and document consent also applies to the monitoring of computer communications. See DIOG Section 18.6.1.8 for specific procedures.

18.6.1.5.1.3 (U) SUBJECT

(U//FOUO) Agents conducting consensual monitoring must not intentionally intercept third-parties who are not of interest to the investigation except for unavoidable or inadvertent overhears.

18.6.1.5.1.4 (U) LOCATION OF DEVICE

(U//FOUO) Consensual monitoring can only be approved if appropriate safeguards are in place to ensure that the consenting party remains a party to the communication throughout the course of monitoring. For example, if a fixed-location monitoring device is being used, the consenting party must be admonished and agree to be present during the duration of the monitoring. If practicable, technical means must be used to activate monitoring only when the consenting party is present.

18.6.1.5.1.5 (U) NOTICE OF CONSENSUAL MONITORING TO OTHER FIELD OFFICES

(U//FOUO) If an employee, CHS, or non-confidential third party is operationally tasked to conduct consensual monitoring outside the field office's territory, the FBI employee requesting approval to conduct the monitoring must provide notice to the SSA who is responsible for the investigative program in the field office where the monitoring occurs. This notice must be documented in the appropriate investigative file b7E

ACLU EC-125

18-51

[Redacted]

(U//FOUO)

[Redacted] b7E

18.6.1.5.1.6 (U) DURATION OF APPROVAL

(U//FOUO) The request for approval must state the length of time needed for monitoring. Unless otherwise warranted, approval may be granted for the duration of the investigation, subject to a substantial change of circumstances. If one or more sensitive monitoring circumstances is present, DOJ may limit its approval to a shorter duration. See DIOG Section 18.6.1.6.3 below.

18.6.1.5.1.7 (U) LEGAL REVIEW

(U//FOUO) Prior to the opening of consensual monitoring, the CDC or OGC must concur that, given the facts of the investigation, the consensual monitoring is legal. Although AUSA concurrence is no longer required for consensual monitoring, providing notice to the AUSA is encouraged.

18.6.1.5.1.8 (U) CHANGE OF MONITORING CIRCUMSTANCES

(U//FOUO) Whenever the monitoring circumstances change substantially, a new FD-759 must be executed, and the CDC or OGC must be recontacted to obtain new concurrence. (AGG-Dom, Part V.A.4.) The following are examples of substantial changes in monitoring circumstances which require a new FD-759: a different consenting party, a change in the location of a fixed monitoring device, or the addition of a new computer system. If any of these or other monitoring circumstances substantially change, the FBI employee must immediately contact the CDC or OGC.

18.6.1.5.1.9 (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.

ACLU EC-126

(U//FOUO) Consensual monitoring conducted by a non-confidential party (e.g., witness, victim, etc.) will be controlled by the agency that is primarily responsible for the non-confidential party. In a joint investigation, the employees should reach an understanding as to which agency is responsible for the non-confidential party; that agency's policies will govern approval and documentation requirements for consensual monitoring.

18.6.1.6 (U) CONSENSUAL MONITORING SITUATIONS REQUIRING ADDITIONAL APPROVAL

18.6.1.6.1 (U) PARTY LOCATED OUTSIDE THE UNITED STATES

(U//FOUO)

[Redacted]

b7E

(U//FOUO)

[Redacted]

b7E

(U//FOUO)

[Redacted]

b7E

(U//FOUO)

[Redacted]

b7E

See DIOG Section 13.

18.6.1.6.2 (U) CONSENT OF MORE THAN ONE PARTY REQUIRED FOR CONSENSUAL MONITORING

(U//FOUO) For those state, local and tribal governments that require all-party consent ^{and do} not sanction or provide a law enforcement exception [Redacted] b7E

[Redacted]

ACLU EG-127

[Redacted] b7E

(U//FOUO) The law of the state or territory where the monitoring will take place will govern whether OIA approval is needed.

(U//FOUO) Consensual monitoring authority and OIA in all-party consent states with no law enforcement exception for FBI employees and [Redacted] b7E
[Redacted] and the authorization must be appropriately documented. As noted in DIOG Section 17.4 above, OIA authority for a CHS must be approved in conformity with the AGG-CHS and the FBI CHSPG.

(U//FOUO) [Redacted] b7E

(U//FOUO) [Redacted] b7E

(U//FOUO) See the OGC website for a list of all-party consent states. See, also DIOG Section 18.6.2, below.

18.6.1.6.3 (U) SENSITIVE MONITORING CIRCUMSTANCE

(U) Requests to monitor communications when a sensitive monitoring circumstance is involved must be approved by the DOJ Criminal Division, or, if the investigation concerns a threat to the national security or foreign intelligence collection, by the DOJNSD. (AGG-Dom, Part V.A.4) A “sensitive monitoring circumstance” is defined in the AGG-Dom, Part VII.O, to include the following:

- A) (U) Investigation of a member of Congress, a federal judge, a member of the Executive Branch at Executive Level IV or above, or a person who has served in such capacity within the previous two years (Executive Levels I through IV are defined in 5 U.S.C. §§ 5312-5315);

- B) (U) Investigation of the Governor, Lieutenant Governor, or Attorney General of any state or territory, or a judge or justice of the highest court of any state or territory, concerning an offense involving bribery, conflict of interest, or extortion related to the performance of official duties;
- C) (U) The Attorney General, the Deputy Attorney General, or an Assistant Attorney General has requested that the FBI obtain prior approval for the use of consensual monitoring in a specific investigation;
- D) (U) A party to the communication is in the custody of the Bureau of Prisons (BOP) or the United States Marshal Service (USMS) or is being or has been afforded protection in the Witness Security Program.

[Redacted] b7E

- E) (U//FOUO) [Redacted]

[Redacted] b7E

1) (U//FOUO) [Redacted] b7E

2) (U//FOUO) [Redacted] b7E

[Redacted]

3) (U//FOUO) [Redacted] b7E

[Redacted]

4) (U//FOUO) [Redacted] b7E

5) (U//FOUO) [Redacted] b7E

6) (U//FOUO) [Redacted] b7E

[Redacted]

7) (U//FOUO) [Redacted] b7E

8) (U//FOUO) [Redacted] b7E

[Redacted]

9) (U//FOUO) [Redacted] b7E

[Redacted]

10) (U//FOUO) [Redacted] b7E

[Redacted]

11) (U//FOUO) [Redacted] b7E

12) (U//FOUO) [Redacted]

ACLU EC-129

§18

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

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

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

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

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

(U//FOUO) [redacted] b7E

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

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

C) (U//FOUO) See the classified provisions in DIOG Appendix G for additional information regarding consensual monitoring.

(U//FOUO) ***Procedure for Obtaining DOJ Approval For a Sensitive Monitoring Circumstance:*** [redacted]

[redacted] b7E

(U//FOUO) ***Emergency requests involving Sensitive Monitoring Circumstances:*** [redacted]

[redacted] b7E

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

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

(U//FOUO) [redacted] b7E

[redacted]

(U//FOUO) [Redacted] b7E

(U//FOUO) [Redacted] b7E

18.6.1.7 (U) DURATION OF APPROVAL

(U//FOUO) [Redacted] b7E

18.6.1.8 (U) SPECIFIC PROCEDURES

(U//FOUO) The following procedures apply when obtaining consent.

18.6.1.8.1 (U) DOCUMENTING CONSENT TO MONITOR/RECORD

(U//FOUO) [Redacted] b7E

(U//FOUO) [Redacted] b7E

§18

18.6.1.8.1 (U) CONSENSUAL MONITORING OF COMPUTERS

(U//FOUO)

[Redacted]

b7E

[Redacted] the CDC or OGC must review the document at issue to ensure that the implied consent is legally sufficient.

18.6.1.8.2 (U) DOCUMENTING APPROVAL

(U//FOUO)

[Redacted]

b7E

18.6.1.8.3 (U) RETENTION OF CONSENSUALLY MONITORED COMMUNICATIONS

(U//FOUO)

[Redacted]

b7E

18.6.1.8.4 (U) MULTIPLE COMMUNICATIONS

(U//FOUO)

[Redacted]

b7E

18.6.1.8.5 (U) INVESTIGATION SPECIFIC APPROVAL

(U//FOUO)

[Redacted]

b7E

18.6.1.9 (U) COMPLIANCE AND MONITORING

(U//FOUO) Case agents and supervisors must regularly monitor the use of this method to ensure that the continued interception of communications is warranted and lawfully obtained by virtue of consent, express or implied, from a party to the communication. Such monitoring shall include a review of the investigative file to ensure that consent and authorization forms are in the appropriate investigative ELSUR sub-file and properly completed by the requesting agent. ELSUR program personnel must review all submitted FD-759s and consent forms (FD-

ACLU EC-132

472 and FD-1071) to ensure proper approval is documented for the consensual monitoring of communications

ACLU EC-133

18.6.2 (U) INVESTIGATIVE METHOD: INTERCEPTING THE COMMUNICATIONS OF A COMPUTER TRESPASSER

18.6.2.1 (U) SUMMARY

(U) The wire or electronic communications of a computer trespasser to, from, or through a protected computer may be intercepted and collected during a Predicated Investigation. Use of this method requires SSA approval and review by the CDC or the OGC. (AGG-Dom, Part V.A.4)

18.6.2.2 (U) APPLICATION

(U//FOUO) 

b7E

18.6.2.3 (U) LEGAL AUTHORITY

- A) (U) The Fourth Amendment to the United States Constitution and case law interpreting the same;
- B) (U) The Wiretap Statute, 18 U.S.C. § 2511, prohibits the intentional interception and use of wire, oral, or electronic communications absent an exception;
- C) (U) Computer Trespasser Exception, 18 U.S.C. § 2511(2)(i); and
- D) (U) The Foreign Intelligence Surveillance Act of 1978 (FISA), 50 U.S.C. §§ 1801 et seq., requires court authorization for “electronic surveillance.” FISA specifically provides, however, that the acquisition of computer trespasser communications that would be permissible under 18 U.S.C. § 2511(2)(i) are not subject to the FISA court order requirement for electronic surveillance of wire communication under section 101(f)(2) of FISA. 50 U.S.C. § 1801(f)(2).

18.6.2.4 (U) DEFINITION OF THE COMMUNICATIONS OF A COMPUTER TRESPASSER

(U) Generally, the Wiretap Statute (also referred to as Title III), 18 U.S.C. §§ 2510-2522, prohibits the intentional interception of wire, oral, or electronic communications unless one of several exceptions applies. One such exception is the interception of a computer trespasser's wire or electronic communications to, through or from a protected computer based on the authorization of the owner or operator of that computer. Another statutory exception is based on the consent of a party to the communication. This section relates specifically to the computer trespasser exception; the policy on consensual recording of computer communications can be found at DIOG Section 18.6.1.

(U) The computer trespasser exception to the Wiretap Statute, 18 U.S.C. § 2511(2)(i), permits a person acting under color of law to intercept the wire or electronic communications of a computer trespasser that are transmitted to, through, or from a protected computer when the owner or operator of that computer authorizes the interception. The use of this method does not include retrieving or obtaining records of communications that have been stored on the computer or elsewhere after the communication has occurred.

ACLU EC-134

§18

(U) The statute requires:

- A) (U) The owner or operator of the protected computer to authorize the interception of the trespasser's communications on the protected computer;
- B) (U) The person acting under color of law to be engaged in a lawful investigation;
- C) (U) The person acting under color of law to have reasonable grounds to believe that the contents of the trespasser's communications will be relevant to the investigation; and
- D) (U) The interception is limited to the communications transmitted to or from the trespasser.

(U) The case agent is responsible for documenting the basis for the conclusion that the person who provided authorization to intercept the trespasser's communications is either the owner or operator of the protected computer. The "owner or operator" must have sufficient authority over the protected computer/computer network system to authorize access across the entire system. This could be a corporate officer, CIO, or system administrator, if the system administrator has authority across the entire system. In any instance in which the identification of the owner or operator is not plainly evident, the case agent must seek the assistance of the CDC or the OGC to identify the proper owner or operator.

(U) A "protected computer," defined in 18 U.S.C. § 1030(e), has been generally interpreted to be any computer or computer network device connected to the Internet, although it also includes most computers used by a financial institution or the United States Government regardless of whether the computer is connected to the Internet.

(U) A "computer trespasser" is a person who accesses a protected computer without authorization and thus has no reasonable expectation of privacy in any communication transmitted to, from, or through the protected computer. The definition of computer trespasser does not include a person known by the owner or operator to have exceeded their authority or to have an existing contractual relationship with the owner or operator for access to all or part of the computer. (18 U.S.C. § 2510(21))

(U) The trespasser exception and the consensual monitoring of communications exception are related, but separate, exceptions to the Wiretap Statute. The owner, operator, and authorized users of a protected computer can consent to the monitoring of only those communications they send or receive (i.e., communications to which they are a party), which do not include a trespasser's communications. (See DIOG Section 18.6.1) In comparison, under the trespasser exception, the owner or operator may only authorize the interception of the communications of a trespasser transmitted to, through or from the protected computer.

(U) When applicable, the computer trespasser and consensual monitoring of communications exceptions to the Wiretap Statute can be used together, permitting the interception of communications of both authorized users and trespassers on the protected computer. This is particularly useful when it is difficult to discern the trespasser communications from other communications. If it is possible to obtain consent to monitor the communications of the authorized users, using the consent and trespasser exceptions together can mitigate the risk of over or under collection of the trespasser's communications. See DIOG Section 18.6.1 for the policy regarding consensual monitoring of computer communications.

ACLU EC-135

18-62

18.6.2.5 (U//FOUO) USE AND APPROVAL REQUIREMENTS FOR INTERCEPTING THE COMMUNICATIONS OF A COMPUTER TRESPASSER

18.6.2.5.1 (U) GENERAL APPROVAL REQUIREMENTS

(U//FOUO) An SSA may approve the use of the computer trespasser exception, subject to CDC or OGC review. Approval is conditioned on the following criteria being met and documented on the FD-759 and through other supporting documentation in the investigative file:

18.6.2.5.1.1 (U) REASONS FOR THE INTERCEPTION

(U//FOUO) The synopsis portion of the FD-759 must include sufficient facts to support the need for the interception and to explain how the contents of the trespasser's communications will be relevant to the investigative purpose.

18.6.2.5.1.2 (U) OWNER OR OPERATOR AUTHORIZATION

(U//FOUO) The authorization of the owner or operator of the protected computer (who may be the system administrator, as stated above) to a person acting under color of law to intercept the trespasser communications on the protected computer system or network must be documented using the FD-1070, Authorization to Intercept the Communications of a Computer Trespasser. The steps the case agent takes to ensure that the person providing the authorization is the actual or appropriate owner or operator of the protected computer must be documented in the investigative file. See 18.6.2.6 below for specific procedures.

18.6.2.5.1.3 (U) ACQUIRING ONLY TRESPASSER COMMUNICATIONS

(U//FOUO) When intercepting communications under the computer trespasser exception alone (i.e., not in conjunction with consensual monitoring of electronic communications), the collection must not intentionally acquire communications other than those to or from the trespasser. This can often be technically complicated to accomplish depending on the use and configuration of the protected computer and the sophistication of the trespasser. The steps to be taken to identify trespasser communications and to isolate such communications from those of authorized users must be considered by the approving and reviewing officials and documented in the investigative file. See DIOG Section 18.6.2.6 below for specific procedures.

18.6.2.5.1.4 (U) OWNER OR OPERATOR COLLECTION

(U//FOUO) The interception of trespasser communications may be conducted by the FBI or by the owner or operator of the protected computer at the FBI's request. In either instance, the interception is being conducted under color of law. If the collection is not being conducted by the FBI, the case agent must document that he or she has informed the person conducting the interception that it must be accomplished in conformity with the statute.

ACLU EC-136

18-63

§18

18.6.2.5.1.5 (U) LOCATION OF INTERCEPT

(U//FOUO) If the intercept or collection of the trespasser communications will occur outside of the field office of the approving official, the SAC or ASAC of the field office within which the interception will occur must be notified, and the notification must be documented in the investigative file.

18.6.2.5.1.6 (U) DURATION

(U//FOUO) The request for approval (FD-759) must state the length of time needed for the interception. Unless otherwise warranted, approval may be granted for the duration of the investigation, subject to a substantial change of circumstances, as described in DIOG Section 18.6.2.6, below.

18.6.2.5.1.7 (U) LEGAL REVIEW

(U//FOUO) Prior to the opening of the interception, the CDC or OGC must concur that, given the facts of the investigation, the interception appears to be lawful under the computer trespasser exception. Whenever the factors surrounding the use of the approved technique change substantially, a new FD-759 must be executed. The newly executed FD-759 must include refreshed concurrence of the CDC or OGC. (AGG-Dom, Part V.A.4.) The following are examples of substantial changes in the circumstances of the interception that require a new FD-759: a change in owner or operator, a change in the method of collection, or the change or addition of a protected computer system. On the other hand, technical changes in the collection system for the purpose of improving or refining the interception are usually not substantial changes to the circumstances of the interception.

18.6.2.5.1.8 (U) JOINT INVESTIGATIONS

(U//FOUO) In joint investigations, if the FBI is the lead investigating agency, FBI policies and guidance regarding the interception of computer trespasser communications must be followed. If the FBI is not the lead investigating agency, the policies of the lead investigating agency must be followed and documented to the appropriate FBI investigative file.

18.6.2.5.1.9 (U) EXTRATERRITORIAL CONSIDERATIONS

(U//FOUO)

[REDACTED]

b7E

ACLU EC-137

18-64

18.6.2.6 (U) DURATION OF APPROVAL FOR INTERCEPTING THE COMMUNICATIONS OF A COMPUTER TRESPASSER

(U//FOUO) The interception and collection of computer trespasser communications under the computer trespasser exception may be approved for a specified length of time or for the duration of the particular investigation.

18.6.2.7 (U) SPECIFIC PROCEDURES FOR INTERCEPTING THE COMMUNICATIONS OF A COMPUTER TRESPASSER

(U//FOUO) The following procedures apply when obtaining authorization.

18.6.2.7.1 (U) DOCUMENTING AUTHORIZATION TO INTERCEPT

(U//FOUO) Whenever possible, written authorization must be obtained from the owner or operator of the protected computer and documented on an FD-1070, Authorization to Intercept the Communications of a Computer Trespasser.

(U//FOUO) If the authorization from the owner or operator is provided orally, at least one FBI agent and another law enforcement or intelligence officer should witness the authorization, and the authorization must be memorialized in an FD-302. The fact that the authorizing party has declined or was unable to give written authorization must also be recorded on the FD-1070, Authorization to Intercept the Communications of a Computer Trespasser form. This form should then be executed in all respects with the exception of the authorizing party's signature.

(U//FOUO) The case agent must document to the file (i.e., FD-302 or EC) the facts that establish that the person providing the authorization is a proper party to provide authorization for the anticipated interception.

(U//FOUO) If the case agent is seeking approval for the FBI to engage in both consensual monitoring and an interception of the computer trespasser on the same computer system separate forms --

[Redacted] b7E

18.6.2.7.2 (U) ACQUIRING ONLY THE TRESPASSER COMMUNICATIONS

(U//FOUO) The computer trespasser exception permits the FBI to intercept only trespasser communications. Prior to seeking approval to intercept computer trespasser communications, the case agent must coordinate the use of the method with the Field Office Technical Advisor by submission of an Electronic Technical Request (ETR). On receipt of the ETR, the Technical Advisor must ensure that the technical equipment and expertise necessary to lawfully implement the interception are timely provided following approval to use this investigative method.

(U//FOUO) Many of the technical challenges and risks associated with accurately isolating the trespasser communications can be mitigated by also obtaining consent to monitor the computer or a court order. The possibility of using the authority to intercept trespasser

ACLU EC-138

communications in conjunction with consent should be raised at the time of the ETR submission or as soon thereafter as the case agent determines that the authorized users of the protected computer will consent to FBI monitoring.

(U//FOUO) When intercepting trespasser communications, the case agent must prepare an FD-302 or EC detailing the steps taken to identify trespasser communications and to isolate such communications from those of authorized users. For example: "reviewed system logs provided by the system administrator and identified a trespasser accessing the system at the following dates and times via IP address xxx or port xxx." Additionally, any subsequent review or revision of the steps needed to identify and isolate the trespasser's communications must also be documented to the investigative file by an EC or FD-302, as appropriate.

18.6.2.7.3 (U) REVIEWING THE ACCURACY OF THE INTERCEPTION

(U//FOUO) At the opening of interception and collection of computer trespasser communications, the Technical Advisor or designated technically trained agent (TTA) coordinating the implementation of the interception and collection device shall ensure that appropriate collection parameters are implemented as required by OTD policy and procedures.

(U//FOUO) The case agent shall ensure a timely initial review of the collected information to verify that the interception and collection are limited to communications authorized for interception and collection under the trespass authority or other lawful exception. Following this initial review, the case agent shall ensure that a similar review and evaluation is repeated at appropriate intervals throughout the duration of the interception to ensure that the interception and collection remain within the scope of the trespasser or other lawful exceptions. Factors that may impact the frequency of reviews include, but are not limited to: volume of data to be reviewed, complexity and nature of data collected, and complexity of the trespassed system.

(U//FOUO) Any FBI employee who identifies interception and collection of communications that may be outside the scope of the trespasser or other lawful exception shall immediately notify the case agent and the operational SSA of the possible unauthorized interception and collection of communications. Upon the determination that communications have been unlawfully intercepted or collected, the interceptions and collection must be halted immediately. The case agent must consult with a TTA to determine whether collection may be resumed in a manner that assures further unlawful collections will not occur. If the SSA determines that unlawful collection can be reliably prevented, that determination must be documented to the file before lawful interceptions and collection may resume.

(U//FOUO) The content of communications determined to have been unlawfully collected cannot be used in any manner and shall be removed promptly from all FBI systems and destroyed. A memorandum documenting the removal and destruction shall be filed in the main investigation file and the appropriate investigative ELSUR sub-file.

18.6.2.7.4 (U) REVIEWING THE RELEVANCY OF THE INTERCEPTION

(U//FOUO) The trespasser exception requires the FBI to have a reasonable belief that the contents of the trespasser's communications will be relevant to the investigation. Following opening of the interception and collection of the trespasser communication, the case agent must ensure that the collected communications are reviewed, at appropriate intervals throughout the duration of the interception, to determine whether the interception is and continues to be relevant to the authorized investigation. Factors that may impact the frequency of reviews include, but are not limited to: volume of data to be reviewed, complexity and nature of data collected, and complexity of the trespassed system.

18.6.2.7.5 (U) DURATION OF APPROVAL

(U//FOUO) Authorization to intercept trespasser communications remains valid until such time as the authorizing party, orally or in writing, revokes the authorization or on the termination date of the authorization, whichever comes first.

18.6.2.7.6 (U) ELSUR REQUIREMENTS

(U//FOUO) The information obtained from the collection must be retained in conformity with the ELSUR Policies (See ELSUR Guide, Electronic Surveillance Manual, and Electronic Surveillance Issues located in the OGC Main Law Library) or other applicable policies.

18.6.2.7.7 (U) MULTIPLE COMMUNICATIONS

(U//FOUO) In investigations in which various modes of communication may be intercepted (e.g., telephonic, non-telephonic, electronic communications, etc., or the use of consensual computer monitoring in conjunction with the interception of trespasser communications), one FD-759 may be used to document approval, provided that each mode of communication to be monitored is being used in the same investigative file and all facts required on the FD-759 are the same. If the material facts on the FD-759 vary (e.g., different periods of authority, etc.), separate FD-759s must be executed.

18.6.2.7.8 (U) INVESTIGATION SPECIFIC APPROVAL

(U//FOUO) Approval for intercepting a computer trespasser's communications is investigation specific and is not transferable to any other investigation, unless the investigative file under which the authority was granted is consolidated or reclassified. Investigation specific approval must be obtained for any spin-off investigation(s) that arises out of the original investigation.

18.6.2.8 (U) COMPLIANCE AND MONITORING

(U//FOUO) Case agents must regularly monitor the use of this method to ensure that the continued interception of trespasser communications is warranted and being lawfully conducted. Such monitoring shall include a review of the investigative file to ensure that consent and authorization forms have been properly executed and filed. ELSUR program personnel must review all submitted FD-759s and FD-1070 (Authorization to Intercept the

ACLU EC-140

§18

Communications of a Computer Trespasser form) to ensure proper approval has been documented for the interception of computer trespasser communications.

ACLU EC-141

18-68

Version Dated:
October 15, 2011

18.6.6 (U) INVESTIGATIVE METHOD: NATIONAL SECURITY LETTER (COMPULSORY PROCESS)

18.6.6.1 (U) OVERVIEW OF COMPULSORY PROCESS

(U//FOUO)

[Redacted]

b7E

(U)

[Redacted]

b7E

18.6.6.2 (U) APPLICATION

(U//FOUO) National Security Letters (NSLs) may be used in a national security Predicated Investigation. This method may not be used for assistance to other agencies, unless relevant to an already open FBI authorized investigation.

18.6.6.3 (U) NATIONAL SECURITY LETTERS

18.6.6.3.1 (U) LEGAL AUTHORITY

- A) (U) 12 U.S.C. § 3414(a)(5)(A);
- B) (U) 15 U.S.C. §§ 1681u and 1681v;
- C) (U) 18 U.S.C. § 2709;
- D) (U) 50 U.S.C. § 436;
- E) (U) AGG-Dom, Part V; and
- F) (U) A National Security Letter (NSL) may be used only to request:
 - 1) (U) Financial Records: The Right to Financial Privacy Act (RFPA), 12 U.S.C. § 3414(a)(5);
 - 2) (U) Identity of Financial Institutions: Fair Credit Reporting Act (FCRA), 15 U.S.C. § 1681u(a);
 - 3) (U) Consumer Identifying Information: FCRA, 15 U.S.C. § 1681u(b);
 - 4) (U) Identity of Financial Institutions and Consumer Identifying Information: FCRA, 15 U.S.C. §§ 1681u(a) and (b);
 - 5) (U) Full Credit Reports in International Terrorism Investigations: FCRA, 15 U.S.C. § 1681v; and

ACLU EC-142

§18

- 6) (U) Telephone Subscriber Information, Toll Billing Records, Electronic Communication Subscriber Information, and Electronic Communication Transactional Records: Electronic Communications Privacy Act (ECPA), 18 U.S.C. § 2709.

18.6.6.3.2 (U) DEFINITION OF METHOD

(U) A National Security Letter (NSL) is an administrative demand for documents or records that are relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities. Sample NSLs are available. [REDACTED] b7E

18.6.6.3.3 (U) APPROVAL REQUIREMENTS

(U//FOUO) The process for creating an NSL involves two documents: the NSL itself and the EC approving the issuance of the NSL. The authority to sign NSLs has been delegated to the Deputy Director, Executive Assistant Director, and Associate EAD for the National Security Branch; Assistant Directors and all DADs for CT/CD/Cyber; General Counsel; Deputy General Counsel for the National Security Law Branch; Assistant Directors in Charge in NY, WFO, and LA; and all SACs. This delegation includes FBI officials properly designated to serve in these positions in an acting capacity. No other delegations are permitted. The following requirements for designating an acting official are particular to NSLs and are more restrictive than the Succession and Delegation Policy set forth in DIOG Section 3:

A) (U//FOUO) [REDACTED]

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

C) (U//FOUO) [REDACTED]

(U) [REDACTED]

(U//FOUO) In addition to being signed by a statutorily-required approver, every NSL must be reviewed and approved by a CDC, ADC (or attorney acting in that capacity), or an NSLB attorney.

18.6.6.3.4 (U) STANDARDS FOR ISSUING NSLS

(U) [Redacted]
[Redacted] b7E

(U//FOUO) [Redacted]
[Redacted]

(U//FOUO) [Redacted]
[Redacted] b7E

(U//FOUO) [Redacted]
[Redacted]

(U//FOUO) [Redacted]
[Redacted]

ACLU-EC 144

[Redacted]

(U//FOUO) As with all investigative methods, before requesting an NSL, the employee initiating the request should consider whether an NSL is the least intrusive and reasonable means based upon the circumstances of the investigation to obtain the needed information. See DIOG Section 4.4.

b7E

18.6.6.3.5 (U) SPECIAL PROCEDURES FOR REQUESTING COMMUNICATION SUBSCRIBER INFORMATION

(U//FOUO) [Redacted]

(U//FOUO) [Redacted]

[Redacted]

b7E

(U//FOUO) [Redacted] the investigator should also consider whether an NSL is the least intrusive and reasonable means to obtain the information [Redacted]

b7E

[Redacted]

18.6.6.3.6 (U) DURATION OF APPROVAL

(U) [Redacted]

18.6.6.3.7 (U) SPECIFIC PROCEDURES

(U//FOUO) [Redacted]

[Redacted]

b7E

(U//FOUO) [Redacted]

[Redacted]

(U//FOUO)

[Redacted]

A) (U//FOUO)

b7E

[Redacted]

B) (U//FOUO)

[Redacted]

C) (U//FOUO)

b7E

[Redacted]

D) (U//FOUO)

[Redacted]

E) (U//FOUO)

[Redacted]

F) (U//FOUO)

[Redacted]

b7E

(U//FOUO)

[Redacted]

ACLU EC-146

18-101

§18

(U//FOUO) [Redacted]
[Redacted] b7E

(U//FOUO) [Redacted]
[Redacted] b7E

(U//FOUO) [Redacted]
[Redacted]

18.6.6.3.7.1 (U) COVER EC

(U//FOUO) [Redacted]
[Redacted]

(U//FOUO) [Redacted] b7E
[Redacted]

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

B) (U//FOUO) [Redacted]
[Redacted]

C) (U//FOUO) [Redacted]
[Redacted]

D) (U//FOUO) [Redacted] b7E
[Redacted]

E) (U//FOUO) [Redacted]
[Redacted]

F) (U//FOUO) [Redacted]
[Redacted]

G) (U//FOUO) [Redacted]
[Redacted]

ACLU-EC 147

H) (U//FOUO) [REDACTED]

I) (U//FOUO) [REDACTED]

J) (U//FOUO) [REDACTED] b7E

K) (U//FOUO) [REDACTED]

(U//FOUO) This list is not exhaustive. [REDACTED]

18.6.6.3.7.2 (U) COPY OF NSL

(U//FOUO) A copy of the signed NSL must be retained in the investigative file and be serialized under the appropriate NSL document type in the FBI's central recordkeeping system. Documented proof of service of NSLs must also be maintained in the NSL sub-file.

18.6.6.3.7.3 (U) SECOND-GENERATION INFORMATION

(U//FOUO) [REDACTED] b7E

18.6.6.3.7.4 (U) CONTACT WITH MEMBERS OF THE NEWS MEDIA BY A [REDACTED]

(U//FOUO) [REDACTED] b7E

18.6.6.3.7.5 (U) EMERGENCY CIRCUMSTANCES

(U//FOUO) ECPA protects subscriber or communications transactional information from disclosure by providers of telephone or other electronic communication services. Generally, an NSL, grand jury subpoena, or another form of legal process must be used to compel a communication service provider to disclose subscriber or transactional information. In emergency circumstances, however, the provider may voluntarily disclose information to the FBI if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person exists and requires

ACLU EC-148

disclosure without delay. As a matter of FBI policy, when there is a danger of death or serious physical injury that does not permit the proper processing of an NSL, an administrative subpoena (if permissible), a grand jury subpoena, or a letter to the provider citing 18 U.S.C. § 2702 may be used to request emergency disclosure, if approved by a SAC, ASAC, or FBIHQ Section Chief. If time does not permit the issuance of an emergency letter citing 18 U.S.C. § 2702, an oral request to the provider may be made, but the oral request must be followed-up with a letter to the particular provider. In either situation, an [redacted] Form, which automatically generates the letter, must be completed.

(U//FOUO) [redacted] b7E

(U//FOUO) [redacted] b7E

18.6.6.3.8 (U) NOTICE AND REPORTING REQUIREMENTS

(U//FOUO) The National Security Law Branch at FBIHQ compiles NSL statistics for reporting to Congress. The NSL subsystem [redacted] automatically records the information needed for Congressional reporting. If the NSL is created outside the subsystem, the EC must include all information necessary for NSLB to report NSL statistics accurately. The EC must delineate the number of targeted phone numbers/e-mail accounts/financial accounts that are addressed to each NSL recipient. For example, if there are three targets, ten accounts, and six recipients of an NSL, the EC must state how many accounts are the subject of the NSL as to Recipient 1, Recipient 2, etc. It is not sufficient to indicate only that there are ten accounts and six recipients.

(U//FOUO) In addition, the FBI must report the USPER status of the subject of all NSLs (as opposed to the target of the investigation), other than NSLs that seek only subscriber information. While the subject is often the target of the investigation, that is not always the case. The EC must reflect the USPER status of the subject of the request – the person whose information the FBI is seeking. If the NSL is seeking information about more than one person, the EC must reflect the USPER status of each person. (See the model ECs on the NSLB website.)

18.6.6.3.9 (U) RECEIPT OF NSL INFORMATION

(U//FOUO) [redacted] b7E

ACLU EC-149

[Redacted]

b7E

(U//FOUO) [Redacted]

[Redacted]

b7E

(U//FOUO) [Redacted]

[Redacted]

b7E

(U//FOUO) [Redacted]

[Redacted]

b7E

(U//FOUO) [Redacted]

[Redacted]

b7E

ACLU EC-150

§18

[Redacted]

b7E

(U//FOUO)

[Redacted]

b7E

(U//FOUO)

[Redacted]

b7E

(U//FOUO)

[Redacted]

b7E

18.6.6.3.10 (U) ELECTRONIC SERVICE AND ELECTRONIC RETURNS OF NSLS

(U//FOUO)

[Redacted]

b7E

(U//FOUO)

[Redacted]

b7E

(U//FOUO)

[Redacted]

b7E

ACLU EC-151

[Redacted]

(U//FOUO) [Redacted]

[Redacted]

A) (U//FOUO) [Redacted]

[Redacted]

B) (U//FOUO) [Redacted]

[Redacted]

b7E

(U//FOUO) [Redacted]

[Redacted]

(U//FOUO) [Redacted]

[Redacted]

(U//FOUO) [Redacted]

[Redacted]

18.6.6.3.11 (U) DISSEMINATION OF NSL MATERIAL

(U//FOUO) Subject to certain statutory limitations, information obtained in response to an NSL may be disseminated according to general dissemination standards in the AGG-Dom. The ECPA (telephone and electronic communications transactional records) and RFPA (financial records) permit dissemination if consistent with the AGG-Dom and the information is clearly relevant to the responsibilities of the recipient agency. FCRA permits dissemination of identity of financial institutions and consumer identifying information to other federal agencies as may be necessary for the approval or conduct of a foreign counterintelligence investigation. FCRA imposes no special rules for dissemination of full credit reports.

(U//FOUO) [Redacted]

[Redacted] NSLs are not classified nor is the material received in return classified. [Redacted]

b7E

[Redacted]

§18

18.6.6.3.12 (U) SPECIAL PROCEDURES FOR HANDLING RIGHT TO FINANCIAL PRIVACY ACT INFORMATION

(U//FOUO) [Redacted]

(U//FOUO) [Redacted] b7E

(U//FOUO) [Redacted]

(U//FOUO) [Redacted]

18.6.6.3.13 (U) PAYMENT FOR NSL-DERIVED INFORMATION

(U//FOUO) No legal obligation exists for the FBI to compensate recipients of NSLs issued pursuant to ECPA (telephone and electronic communications transactional records) or FCRA, 15 U.S.C. § 1681v (full credit reports in international terrorism investigations), and therefore no payment should be made in connection with those NSLs. See EC, 319X-HQ-A1487720-OGC, serial 222, for a form letter to be sent in response to demands for payment concerning these NSLs.

(U//FOUO) Compensation is legally required for NSLs issued pursuant to RFP (financial records) and FCRA § 1681u (identity of financial institutions and consumer identifying information). A fee schedule has been adopted under 12 C.F.R. § 219.3, Appendix A, and should be reviewed for the current reimbursement provisions. A copy of this fee schedule is available on the OGC website at:

[Redacted] b7E

ACLU EC-153

18.6.8 (U) INVESTIGATIVE METHOD: STORED WIRE OR ELECTRONIC COMMUNICATIONS AND TRANSACTIONAL RECORDS

18.6.8.1 (U) SUMMARY

(U//FOUO) FBI employees may acquire the contents of stored wire or electronic communications and associated transactional records—including basic subscriber information—as provided in 18 U.S.C. §§ 2701-2712 (Electronic Communications Privacy Act (ECPA)). Requests for voluntary disclosure under the emergency authority of 18 U.S.C. § 2702 require prior approval from the field office ASAC or FBIHQ Section Chief when appropriate.

(U//FOUO) All requests for information from electronic communication service providers (e.g., telephone companies, internet service providers) pertaining to a subscriber or customer must comply with ECPA. As used in ECPA, the term “information pertaining to a subscriber or customer” should be read broadly. It includes, for example, information regarding whether a particular individual has an account with a covered provider. Thus, unless done in accordance with ECPA, an FBI employee may not ask a telephone company or internet service provider whether John Smith has an account with the company (i.e., the FBI employee may not informally seek information that is statutorily protected prior to the issuance of appropriate process or the existence of an exception to ECPA). In addition, based on a November 5, 2008 interpretation of ECPA from the Office of Legal Counsel, the FBI may not ask a telephone company whether a given telephone number that the company services has been assigned to an individual. In short, in order to obtain any information specific to the subscriber from a telephone company or electronic communication service provider, the FBI must provide legal process pursuant to 18 U.S.C. §§ 2703 or 2709 or the request must fall within the limited exceptions established in 18 U.S.C. § 2702, and discussed below.

(U//FOUO) [Redacted] b7E

18.6.8.2 (U) APPLICATION

(U//FOUO) [Redacted] b7E

18.6.8.2.1 (U) STORED DATA

(U) The Electronic Communications Privacy Act (ECPA)—18 U.S.C. §§ 2701-2712—governs the disclosure of two broad categories of information: (i) the contents of wire or

ACLU EC-154

electronic communications held in “electronic storage” by providers of “electronic communication service” or contents held by those who provide “remote computing service” to the public; and (ii) records or other information pertaining to a subscriber to or customer of such services. The category of “records or other information” can be subdivided further into subscriber records (listed in 18 U.S.C. § 2703(c)(2)) and stored traffic data or other records.

(U) Records covered by ECPA include all records that are related to the subscriber, including buddy lists, “friend” lists (MySpace), and virtual property owned (Second Life). These other sorts of records are not subscriber records and cannot be obtained with a subpoena under 18 U.S.C. § 2703(c)(2) or an NSL under 18 U.S.C. § 2709.

18.6.8.2.2 (U) LEGAL PROCESS

(U) The legal process for obtaining disclosure will vary depending on the type of information sought and whether the information is being voluntarily provided under 18 U.S.C. § 2702 (e.g., with consent or when emergency circumstances require disclosure) or the provider is being compelled to provide the information under 18 U.S.C. § 2703, as outlined below. The process for compelling production under 18 U.S.C. § 2709 is discussed in the NSL section above.

18.6.8.2.3 (U) RETRIEVAL

(U) Contents held in “electronic storage” by a provider of “electronic communication service” for 180 days or less can only be obtained with a search warrant based on probable cause. Accordingly, such records may only be obtained during a Full Investigation.

(U) Contents held by those who provide “remote computing service” to the public and contents held in “electronic storage” for more than 180 days by an “electronic communication service” provider can be obtained with: a warrant; a subpoena with prior notice to the subscriber or customer; or an order issued by a court under 18 U.S.C. § 2703(d) when prior notice has been provided to the customer or subscriber (unless the court has authorized delayed notice).

(U) Title 18 U.S.C. § 2705 establishes the standard to delay notice for an initial period of up to 90 days. Records or other information pertaining to a subscriber to or customer of such services, including basic subscriber information, can be obtained with a search warrant or an 18 U.S.C. § 2703(d) order without notice.

18.6.8.2.4 (U) BASIC SUBSCRIBER INFORMATION

(U) Basic subscriber information, as described in 18 U.S.C. § 2703(c)(2), can be compelled by a grand jury or administrative subpoena without notice.

18.6.8.2.5 (U) PRESERVATION OF STORED DATA

(U) The government is authorized under 18 U.S.C. § 2703(f) to direct a provider to preserve records or other information (stored records or communications) in its possession for 90 days (which may be extended for an additional 90-days) pending issuance of applicable legal

ACLU EC-155

process for disclosure. To make a preservation request, the FBI must believe that the records will subsequently be sought by appropriate legal process.

18.6.8.2.6 (U) COST REIMBURSEMENT

(U) 18 U.S.C. § 2706 requires the government to reimburse for costs incurred in providing the contents of communications, records, or other information obtained under 18 U.S.C. §§ 2702, 2703, or 2704, except that reimbursement is not required for records or other information maintained by a communications common carrier that relate to telephone toll records and telephone listings obtained under 18 U.S.C. § 2703. In essence, the government does not have to reimburse for the cost of producing records that the provider maintains in the ordinary course of its business.

18.6.8.3 (U) LEGAL AUTHORITY

(U) 18 U.S.C. §§ 2701-2712

(U) AGG-Dom, Part V.9

(U) ECPA—18 U.S.C. §§ 2701-2712— creates statutory privacy rights for the contents of communications in “electronic storage” and records or other information pertaining to a subscriber to or customer of an “electronic communication service” and a “remote computing service.” The statutory protections protect the privacy of an individual’s electronic data contained in a networked account—that may otherwise fall outside the scope of the protections afforded by the Fourth Amendment—when such account or its service is owned or managed by a third-party provider.

(U) ECPA generally: (i) prohibits access to the contents of wire or electronic communications while in “electronic storage” unless authorized (18 U.S.C. § 2701); (ii) prohibits a provider of service to the public from disclosing the contents of wire or electronic communications while held in “electronic storage,” and prohibits divulging to the government any information pertaining to a subscriber to or customer of such service unless authorized (18 U.S.C. § 2702); and (iii) authorizes the government to compel disclosure from a provider of stored contents of a wire or electronic communication and records or other information pertaining to a subscriber to or customer (18 U.S.C. § 2703). ECPA provides for reimbursement of costs incurred in providing the information acquired.

(U) [REDACTED] b7E

18.6.8.4 (U) ECPA DISCLOSURES

(U) ECPA authorities can be divided into two categories: (i) compelled disclosure—legal process to compel providers to disclose the contents of stored wire or electronic communications (including e-mail and voice mail—opened and unopened) and other information, such as account records and basic subscriber information; and (ii) voluntary disclosure of such information from service providers. Each of these authorities is discussed below.

ACLU EC-156

18-113

18.6.8.4.1 (U) DEFINITIONS

- A) (U) ***Electronic Storage***: is "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof," or "any storage of such communication by an electronic communication service for purposes of backup protection of such communication." 18 U.S.C. § 2510(17). In short, "electronic storage" refers only to temporary storage, made in the course of transmission, by a provider of an electronic communication service.
- B) (U) ***Remote Computing Service (RCS)***: is a service that provides "to the public" computer storage or processing services by means of an electronic communications system. 18 U.S.C. § 2711(2). In essence, a remote computing service is an off-site computer that stores or processes data for a customer.
- C) (U) ***Electronic Communications System***: is "any wire, radio, electromagnetic, photooptical or photoelectronic facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications." 18 U.S.C. § 2510(14).
- D) (U) ***Electronic Communication Service (ECS)***: is "any service that provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15). For example, telephone companies and electronic mail companies generally act as providers of electronic communication services.

18.6.8.4.2 (U) COMPELLED DISCLOSURE

(U) 18 U.S.C. § 2703 lists five types of legal process that the government can use to compel a provider to disclose certain kinds of information. The five mechanisms, in descending order of required threshold showing are as follows:

- A) (U) Search warrant;
- B) (U) 18 U.S.C. § 2703(d) court order with prior notice to the subscriber or customer;
- C) (U) 18 U.S.C. § 2703(d) court order without prior notice to the subscriber or customer;
- D) (U) Subpoena with prior notice to the subscriber or customer; and
- E) (U) Subpoena without prior notice to the subscriber or customer.

(U)

[Redacted]

b7E

(U)

[Redacted]

b7E

ACLU EC-157

18-114

18.6.8.4.2.1 (U//FOUO) NOTICE—ORDERS NOT TO DISCLOSE THE EXISTENCE OF A WARRANT, SUBPOENA, OR COURT ORDER

(U//FOUO) FBI employees may obtain a court order directing network service providers not to disclose the existence of compelled process if the government has no legal duty to notify the customer or subscriber of the process. If an 18 U.S.C. § 2703(d) order or 18 U.S.C. § 2703(a) warrant is being used, a request for a non-disclosure order can be included in the application and proposed order or warrant. If a subpoena is being used to obtain the information, a separate application to a court for a non-disclosure order must be made.

18.6.8.4.2.2 (U) LEGAL STANDARD

(U//FOUO) A court may order an electronic communications service provider or remote computing service not to disclose the existence of a warrant, subpoena, or court order for such period as the court deems appropriate. The court must enter such an order if it determines that there is reason to believe that notification of the existence of the warrant, subpoena, or court order will result in:

- A) (U) Endangering the life or physical safety of an individual;
- B) (U) Flight from prosecution;
- C) (U) Destruction of or tampering with evidence;
- D) (U) Intimidation of potential witnesses; or
- E) (U) Otherwise seriously jeopardizing an investigation or unduly delaying a trial. 18 U.S.C. § 2705(b).

18.6.8.4.2.3 (U) SEARCH WARRANT

(U//FOUO) Investigators can obtain the full contents of a network account with a search warrant issued pursuant to FRCP Rule 41. However, FRCP Rule 41 search warrant may not be issued in Preliminary Investigations. See DIOG Section 18.7.1.3.4.4.

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

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

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

ACLU EC-158

18-115

§18

- A) (U) "The contents of a wire or electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days." 18 U.S.C. § 2703(a).
- B) (U) "The contents of any wire or electronic communication" held by a provider of remote computing service "on behalf of . . . a subscriber or customer of such remote computing service," 18 U.S.C. §§ 2703(b)(1)(B)(ii), 2703 (b)(2); and
- C) (U) Everything that can be obtained using a 18 U.S.C. § 2703(d) court order without notice.

(U) [Redacted] b7E

(U) [Redacted] b7E

18.6.8.4.2.4.1 (U) LEGAL STANDARD

(U) To order delayed notice, the court must find that "there is reason to believe that notification of the existence of the court order may... endanger the life or physical safety of an individual; [lead to] flight from prosecution; [lead to] destruction of or tampering with evidence; [lead to] intimidation of potential witnesses; or . . . otherwise seriously jeopardiz[e] an investigation or unduly delay[] a trial." 18 U.S.C. §§ 2705(a)(1)(A) and 2705(a)(2). The applicant must satisfy this standard anew each time an extension of the delayed notice is sought.

18.6.8.4.2.4.2 (U) NATIONWIDE SCOPE

(U) Federal court orders under 18 U.S.C. § 2703(d) have effect outside the district of the issuing court. Orders issued pursuant to 18 U.S.C. § 2703(d) may compel providers to disclose information even if the information is stored outside the district of the issuing court. See 18 U.S.C. § 2703(d) ("any court that is a court of competent jurisdiction" may issue a 18 U.S.C. § 2703(d) order); 18 U.S.C. § 2711(3) (court of competent jurisdiction includes any federal court having jurisdiction over the offense being investigated without geographic limitation).

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

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

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

- A) (U) All "record(s) or other information pertaining to a subscriber to or customer of such service (not including the contents of communications [held by providers of electronic communications service and remote computing service])," and
- B) (U) Basic subscriber information that can be obtained using a subpoena without notice. 18 U.S.C. § 2703(c)(1).

18.6.8.4.2.5.1 (U) TYPES OF TRANSACTIONAL RECORDS

(U) The broad category of transactional records includes all records held by a service provider that pertain to the subscriber beyond the specific records listed in 2703(c)(2)

[Redacted]

(U//FOUO) [Redacted] b7E

[Redacted]

18.6.8.4.2.5.2 (U) CELL SITE AND SECTOR INFORMATION

(U) Cell site and sector information is considered "a record or other information pertaining to a subscriber" and therefore, production of historical and prospective cell site and sector information may be compelled by a court order under 18 U.S.C. § 2703(d). Requests made pursuant to 18 U.S.C. § 2703(d) for disclosure of prospective cell site and sector information—which is delivered to law enforcement under Communications Assistance for Law Enforcement Act (CALEA) at the beginning and end of calls—must be combined with an application for pen register/trap and trace device. Some judicial districts will require a showing of probable cause before authorizing the disclosure of prospective cell site and sector information.

18.6.8.4.2.5.3 (U) [Redacted]

[Redacted]

(U) [Redacted]

[Redacted] b7E

ACLU EC-160

§18

[Redacted]

(U//FOUO)

[Redacted]

b7E

(U)

[Redacted]

(U)

[Redacted]

18.6.8.4.2.5.4 (U) LEGAL STANDARD

(U) A court order under 18 U.S.C. § 2703(d) is known as an "articulable facts" court order or simply a "d" order. This section imposes an intermediate standard to protect on-line transactional records. It is a standard higher than a subpoena, but not a probable cause warrant.

(U) In applying for an order pursuant to 18 U.S.C. § 2703 (d), the FBI must state sufficient specific and articulable facts for the court to find that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation.

b7E

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

(U//FOUO) Investigators can subpoena opened e-mail from a provider if they give prior notice to the subscriber or comply with the delayed notice provisions of 18 U.S.C. §

ACLU EC-161

18-118

2705(a)– [redacted] that there is reason ^{b7E}
to believe notification of the existence of the subpoena may have an adverse result.

(U) FBI employees who obtain a subpoena and give prior notice to the subscriber or comply with the delayed notice provisions of 18 U.S.C. § 2705(a) may obtain:

- A) (U) "The contents of any wire or electronic communication" held by a provider of remote computing service "on behalf of . . . a subscriber or customer of such remote computing service." 18 U.S.C. § 2703(b)(1)(B)(i), § 2703(b)(2);
- B) (U) "The contents of a wire or electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days." 18 U.S.C. § 2703(a); and
- C) (U) Basic subscriber information listed in 18 U.S.C. § 2703(c)(2).

(U) As a practical matter, this means that [redacted]

[redacted]

(U) *Notice:* [redacted]

[redacted] ^{b7E}

(U) **Legal standards for delaying notice:** The supervisory official must certify in writing that "there is reason to believe that notification of the existence of the court order may... endanger[] the life or physical safety of an individual; [lead to] flight from prosecution; [lead to] destruction of or tampering with evidence; [lead to] intimidation of potential witnesses; or... otherwise seriously jeopardiz[e] an investigation or unduly delay[] a trial." 18 U.S.C. §§ 2705(a)(1)(A), 2705(a)(2). This standard must be satisfied anew every time an extension of the delayed notice is sought. This documentation must be placed with the subpoena in the appropriate investigative file.

18.6.8.4.2.7 (U) SUBPOENA WITHOUT PRIOR NOTICE TO THE SUBSCRIBER OR CUSTOMER

(U//FOUO) Without notice to the subscriber or customer, investigators can subpoena basic subscriber information:

(U) name; address; local and long distance telephone connection records, or records of session times and durations; length of service (including start date) and types of service used; telephone or instrument number or other subscriber number or identity, including

ACLU EC-162

18-119

§18

any temporarily assigned network address; and means and source of payment for such service (including any credit card or bank account number)[.]” 18 U.S.C. § 2703(c)(2).

(U)

b7E

A) (U) ***Legal Standard:*** The legal threshold for issuing a subpoena is relevance to the investigation. Courts are reluctant to review the “good faith” issuance of subpoenas as long as they satisfy the following factors¹⁷: (i) the investigation is conducted pursuant to a legitimate purpose; (ii) the information requested under the subpoena is relevant to that purpose; (iii) the agency does not already have the information it is seeking with the subpoena; and (iv) the agency has followed the necessary administrative steps in issuing the subpoena.

(U//FOUO) In the event that a federal grand jury subpoena is used, however, appropriate protections against disclosure must be followed in compliance with FRCP Rule 6(e).

B) (U//FOUO)

b7E

C) (U) ***Members of the News Media:*** Approval of the Attorney general must be obtained prior to seeking telephone billing records of a member of the news media. (See DIOG Section 18.6.5.1.5)

18.6.8.4.3 (U) VOLUNTARY DISCLOSURE

(U)

b7E

A) (U) ***Service NOT Available to the Public:*** ECPA does not apply to providers of services that are not available “to the public;” accordingly such providers may freely disclose both contents and other records relating to stored communications. Andersen Consulting v. UOP, 991 F. Supp. 1041 (N.D. Ill. 1998) (giving hired consulting firm employees access to UOP’s e-mail system is not equivalent to providing e-mail to the public).

B) (U) ***Services That ARE Available to the Public:*** If the provider offers services to the public, then ECPA governs the disclosure of contents and other records.

¹⁷ (U) United States v. Morton Salt Co., 338 U.S. 632, 642-43 (1950).

- C) (U) If the provider is authorized to disclose the information to the government under 18 U.S.C. § 2702 and is willing to do so voluntarily, law enforcement does not need to obtain a legal order or provide other legal process to compel the disclosure.
- D) (U) If a provider voluntarily discloses under the statute, there is no follow-up legal process required or available. If the provider, on the other hand, either may not or will not disclose the information voluntarily, FBI employees must rely on compelled disclosure provisions and obtain the appropriate legal orders.
- 1) (U) **Voluntary Disclosure of Stored Contents** - ECPA authorizes the voluntary disclosure of stored contents when:
- a) (U) The originator, addressee, intended recipient, or the subscriber (in the case of opened e-mail) expressly or impliedly consents, 18 U.S.C. § 2702(b)(3);
 - b) (U) The disclosure "may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service," 18 U.S.C. § 2702(b)(5);
 - c) (U) The provider "in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of information relating to the emergency," 18 U.S.C. § 2702(b)(8);
 - d) (U//FOUO) An emergency disclosure under this statutory exception is justified when the circumstances demand action without delay to prevent death or serious bodily injury; the statute does not depend on the immediacy of the risk of danger itself. For example,
 b7E
 - e) (U) The disclosure is made to the National Center for Missing and Exploited Children, in connection with a report submitted thereto under Section 227 of the Victims of Child Abuse Act of 1990. (42 U.S.C. § 13032 and 18 U.S.C. § 2702[b][6]); or
 - f) (U) The contents are inadvertently obtained by the service provider and appear to pertain to the commission of a crime. Such disclosures can only be made to a law enforcement agency. 18 U.S.C. § 2702(b)(7)
- 2) (U) **Voluntary Disclosure of Non-Content Customer Records** - ECPA permits a provider to voluntarily disclose non-content customer records to the government when:
- a) (U) The customer or subscriber expressly or impliedly consents, 18 U.S.C. § 2702(c)(2);
 - b) (U) The disclosure "may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service," 18 U.S.C. § 2702(c)(3);
 - c) (U) The provider "in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of information relating to the emergency," 18 U.S.C. § 2702(c)(4); or



ACLU EC-164

18-121

- d) (U//FOUO) *Note:* An emergency disclosure under this statutory exception is justified when the circumstances demand immediate action (i.e., obtaining/disclosing information "without delay") to prevent death or serious bodily injury; the statute does not depend on the immediacy of the risk of danger itself. For example, an e-mail that discusses a planned terrorist attack but not the timing of the attack would constitute an emergency that threatens life or limb and requires immediate action, even though the timing of the attack is unknown. It is the need for immediate action to prevent the serious harm threatened rather than the immediacy of the threat itself that provides the justification for voluntary disclosures under this exception. H.R. Rep. No. 107-497 at 13-14 (2002) accompanying The Cyber Security Enhancement Act of 2002, H.R. 3482, which passed as part of the comprehensive Homeland Security Act of 2002, Pub. L. No. 107-296, § 225 116 Stat. 2135 (2002).
 - e) (U) The disclosure is to the National Center for Missing and Exploited Children, in connection with a report submitted thereto under Section 227 of the Victims of Child Abuse Act of 1990. (42 U.S.C. § 13032 and 18 U.S.C. § 2702[c][5])
- 3) (U) **Preservation of Evidence under 18 U.S.C. § 2703(f)** - [REDACTED]
- [REDACTED] b7E
- a) (U) [REDACTED]
[REDACTED] A governmental entity is authorized to direct providers to preserve stored records and communications pursuant to 18 U.S.C. § 2703(f). Once a preservation request is made, ECPA requires that the provider must retain the records for 90 days, renewable for another 90-day period upon a government request. See 18 U.S.C. § 2703 (f)(2).
 - b) (U) There is no legally prescribed format for 18 U.S.C. § 2703(f) requests [REDACTED] b7E
[REDACTED]
 - c) (U) FBI employees who send 18 U.S.C. § 2703(f) letters to network service providers should be aware of two limitations. First, the authority to direct providers to preserve records and other evidence is not prospective. Thus, 18 U.S.C. § 2703(f) letters can order a provider to preserve records that have already been created but cannot order providers to preserve records not yet made. If FBI employees want providers to record information about future electronic communications, they must comply with the electronic surveillance statutes. A second limitation of 18 U.S.C. § 2703(f) is that some providers may be unable to comply effectively with 18 U.S.C. § 2703(f) requests
[REDACTED] b7E
- 4) (U) **Video Tape Rental or Sales Records** - 18 U.S.C. § 2710 makes the unauthorized disclosure of records by any person engaged in the rental, sale, or delivery of prerecorded video cassette tapes or similar audiovisual materials unlawful and provides an exclusionary rule to prohibit personally identifiable information otherwise obtained from being admissible as evidence in any court proceeding. Personally identifiable information is defined as "information that identifies a person as having requested or obtained specific video material or services"


ACLU EC-165

18-122

- a) (U) The disclosure to law enforcement of “personally identifiable information” is permitted only when the law enforcement agency:
 - (i) (U) Has the written consent of the customer;
 - (ii) (U) Obtains a search warrant issued under Rule 41, FRCP or equivalent state warrant; or
 - (iii) (U) Serves a grand jury subpoena;
- b) (U) 
 b7E
- c) (U) This type of information was specifically not included in the definition of "personally identifiable information" to allow law enforcement to obtain information about individuals during routine investigations such as neighborhood investigations.
- d) (U//FOUO) The disclosure of “personally identifiable information” in a national security investigation may be compelled through use of the above legal processes or pursuant to a business records order issued under 50 U.S.C. § 1861.

18.6.8.5 (U) VOLUNTARY EMERGENCY DISCLOSURE

18.6.8.5.1 (U) SCOPE

(U//FOUO) ECPA protects subscriber and transactional information regarding communications from disclosure by providers of remote computing services or telephone or other electronic communication services to the public (remote computing services, telephone and other electronic communications services are hereafter collectively referred to as “electronic communications service providers” or “providers”). Generally, an NSL, grand jury subpoena, or other form of legal process must be used to compel the communication service provider to disclose such information. 

 b7E

(U//FOUO) 

 b7E

§18

(U//FOUO) [Redacted]
[Redacted] b7E

(U//FOUO) [Redacted]
[Redacted]

(U//FOUO) The use of the [Redacted] is designed to capture all the information the FBI needs to satisfy statutory annual Congressional reporting requirements.

(U//FOUO) [Redacted]
[Redacted] b7E

18.6.8.5.2 (U) DURATION OF APPROVAL

(U) As authorized by statute (e.g., for as long as the emergency necessitating usage exists and only in those circumstances when it is impracticable to obtain other legal process such as a subpoena or NSL) and applicable court order or warrant.

18.6.8.5.3 (U) SPECIFIC PROCEDURES

A) (U//FOUO) *Required Form:* [Redacted]
[Redacted] b7E

ACLU EC-167

B) (U//FOUO) *Filing requirements*

[Redacted]

b7E

C) (U//FOUO) *Contact with Providers*

[Redacted]

18.6.8.5.4 (U) COST REIMBURSEMENT

(U) Policy and procedures regarding cost reimbursement are described in the following:

A) (U) Standardized payment procedures may be found at

[Redacted]

B) (U) Cost Reimbursement Guidance can also be found in 18 U.S.C. § 2706

b7E

[Redacted]

18.6.8.5.5 (U) NOTICE AND REPORTING REQUIREMENTS

18.6.8.5.6 (U) REPORTING VOLUNTARY EMERGENCY DISCLOSURES

(U) 18 U.S.C. § 2702(d) requires the Attorney General to report annually to Congress information pertaining to the receipt of voluntary disclosures of the contents of stored wire or electronic communications in an emergency under 18 U.S.C. § 2702(b)(8), specifically:

A) (U) The number of accounts from which the FBI received voluntary emergency disclosures; and

B) (U) A summary of the basis for the emergency disclosure in those investigations that were closed without the filing of criminal charges.

(U) The [Redacted] Form will capture information required to meet these reporting requirement.

18.6.8.5.7 (U) ROLES/RESPONSIBILITIES

b7E

(U) The [Redacted] that hosts the [Redacted] will, when necessary, follow-up with e-mail notifications to the issuing employee to ensure that the information included in the report to DOJ (which it uses to prepare the required Congressional report) is current. It is the responsibility of the FBI employee to respond to these requests for information as soon as practicable but no later than ten (10) business days. Failure to do so may be considered “substantial non-compliance” pursuant to Section 3.

(U) OGC/ILB is assigned the administrative responsibility to complete the following by December 31 of each year:

A) (U) Tabulate the number of voluntary disclosures of stored contents received under the authority of 18 U.S.C. § 2702(b)(8) for the calendar year;

ACLU EC-168

18-125

§18

- B) (U) Prepare a report summarizing the basis for disclosure in those instances in which the relevant investigation was closed without the filing of criminal charges; and
- C) (U) Submit the report to the General Counsel for review and submission to DOJ according to the statutory requirement for annual report by the Attorney General.

18.6.8.6 (U) OTHER APPLICABLE POLICIES

(U) See the



b7E

ACLU EC-169

18-126

18.6.9 (U) INVESTIGATIVE METHOD: PEN REGISTERS AND TRAP/TRACE DEVICES (PR/TT)

18.6.9.1 (U) SUMMARY

(U) Pen register and trap and trace (PR/TT) devices enable the prospective collection of non-content traffic information associated with wire and electronic communications, such as: the phone numbers dialed from or to a particular telephone, including electronic communications; messages sent from or to a particular telephone; or the internet protocol (IP) address of communications on the Internet and other computer networks.

18.6.9.2 (U) APPLICATION

(U//FOUO)

[Redacted]

b7E

18.6.9.3 (U) LEGAL AUTHORITY

(U) 18 U.S.C. §§ 3121 et seq. and 50 U.S.C. §§ 1842 et seq. regulate the use of PR/TT devices. PR/TT orders authorize the collection of phone number dialed from or to a particular telephone, IP addresses, port numbers and the “To” and “From” information from e-mail; they cannot intercept the content of a communication, such as telephone conversations or the words in the “subject line” or the body of an e-mail.

18.6.9.4 (U) DEFINITION OF INVESTIGATIVE METHOD

(U) A pen register device or process records or decodes dialing, routing, addressing or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided that such information must not include the contents of any communication. See 18 U.S.C. § 3127(3).

(U) A trap and trace device or process captures the incoming electronic or other impulses that identify the originating number or other dialing, routing, addressing or signaling information reasonably likely to identify the source of a wire or electronic communication, provided that such information does not include the contents of any communication. See 18 U.S.C. § 3127(4).

18.6.9.5 (U) STANDARDS FOR USE AND APPROVAL REQUIREMENTS FOR INVESTIGATIVE METHOD

18.6.9.5.1 (U) PEN REGISTER/TRAP AND TRACE UNDER FISA

(U) Applications for authority to use a PR/TT device can be made to the FISC in national security investigations. See 50 U.S.C. § 1842.

18.6.9.5.1.1 (U) LEGAL STANDARD

(U) Applications to the FISC are to be under oath and must include:

- A) (U) The identity of the federal officer making the application; and
- B) (U) A certification by the applicant that the information likely to be obtained is foreign intelligence information not concerning an USPER or is information that is relevant to an ongoing investigation to protect the United States against international terrorism or clandestine intelligence activities; and that such investigation, if of an USPER, is not conducted solely upon the basis of activities protected by the First Amendment to the Constitution.

18.6.9.5.1.2 (U) PROCEDURES

(U//FOUO) Requests for opening or renewal of FISA PR/TT must be made using

[Redacted]

b7E

[Redacted] will route the request to appropriate parties for their review and approval of the request [Redacted] Routing a paper copy for signatures is not required.

18.6.9.5.1.3 (U) EMERGENCY AUTHORITY—FISA: 50 U.S.C. § 1843

(U//FOUO) Under the provisions of FISA, the Attorney General may grant Emergency Authority (EA) for PR/TT. Requests for Emergency Authority must be referred to the appropriate FBIHQ division.

(U//FOUO) [Redacted]

[Redacted]

b7E

- A) (U) The Attorney General may authorize the installation and use of a PR/TT upon a determination that an emergency exists and that the factual basis exists for a court order. The FISC must be informed at the time of the authorization and an application for a court order must be made to the court as soon as practicable, but no more than seven (7) days after the authorization. If the court does not issue an order approving the use of a PR/TT, an emergency-authorized PR/TT use must terminate at the earliest of when the information sought is obtained, when the FISC denies the application, or seven (7) days after the Attorney General authorization is given.
- B) (U) If the FISC denies the application after an emergency PR/TT device has been installed, no information collected as a result may be used in any manner, except with the approval of the Attorney General upon a showing that the information indicates a threat of death or serious bodily harm to any person..

ACLU EC-171

(U) Notwithstanding the foregoing, the President, acting through the Attorney General, may authorize the use of a PR/TT, without a court order, for a period not to exceed 15 calendar days, following a declaration of war by Congress. See 50 U.S.C. § 1844.

(U//FOUO) For an emergency authorization to use a PR/TT surveillance [redacted] b7E
[redacted] at any time.

18.6.9.5.1.4 (U) FISA OVERCOLLECTION

(U//FOUO) In accordance with Foreign Intelligence Surveillance Court (FISC) Rule of Procedure 15, information acquired outside of the scope of the FISA authorization (“FISA overcollection”) will no longer be sequestered with the FISC, absent extraordinary circumstances. Contact NSLB for further guidance regarding the handling of any FISA overcollection.

18.6.9.5.2 (U) CRIMINAL PEN REGISTER/TRAP AND TRACE UNDER TITLE 18

(U) Applications for the installation and use of a PR/TT device may be made to a “court of competent jurisdiction”—i.e., “any district court of the United States (including a magistrate judge of such a court) or any United States court of appeals having jurisdiction over the offense being investigated, or any court of general criminal jurisdiction of a State authorized by the law of that State to enter orders authorizing the use of a pen register or trap and trace device.” See 18 U.S.C. § 3127(2).

18.6.9.5.2.1 (U) LEGAL STANDARD

(U) Applications for authorization to install and use a PR/TT device must include:

- A) (U) The identity of the attorney for the government or the state law enforcement or investigative officer making the application and the identity of the law enforcement agency conducting the investigation; and
- B) (U) A certification by the applicant that the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by that agency.

18.6.9.5.2.2 (U//FOUO) PROCEDURES

(U//FOUO) An SSA must approve a request for opening or renewal of PR/TT use prior to submission of the request to an attorney for the government. Before approving such a request, the SSA should consider of the following:

- A) (U//FOUO) The use of resources based on the investigative purpose set forth;
- B) (U//FOUO) Whether there is sufficient factual basis for the certification to be made in the application (i.e., is the information likely to be obtained relevant to an ongoing criminal investigation);
- C) (U//FOUO) Whether the customer or subscriber has consented to the use of a PR/TT, see 18 U.S.C. § 3121(b)(3); or

ACLU EC-172

18-129

§18

D) (U//FOUO) Whether the use of a PR/TT is the least intrusive method if reasonable based upon the circumstances of the investigation.

(U//FOUO) A copy of the approving EC must be maintained in the pen register sub-file “PEN.”

(U//FOUO) A PR/TT order is executable anywhere within the United States and, upon service, the order applies to any person or entity providing wire or electronic communication service in the United States whose assistance may facilitate the execution of the order. Whenever such an order is served on any person or entity not specifically named in the order, upon request of such person or entity, the attorney for the government or law enforcement or investigative officer that is serving the order must provide written or electronic certification that the order applies to the person or entity being served.

18.6.9.5.2.3 (U) EMERGENCY AUTHORITY—CRIMINAL: 18 U.S.C. § 3125

(U) The Attorney General, the Deputy Attorney General, the Associate Attorney General, any Assistant Attorney General, any acting Assistant Attorney General, or any Deputy Assistant Attorney General may specially designate any investigative or law enforcement officer to reasonably determine whether an emergency situation exists that requires the installation and use of a PR/TT device before an order authorizing such installation and use can, with due diligence, be obtained and there are grounds upon which an order could be entered authorizing the installation and use of a PR/TT.

(U) An emergency situation as defined in this section involves:

- A) (U) Immediate danger of death or serious bodily injury to any person;
- B) (U) Conspiratorial activities characteristic of organized crime;
- C) (U) An immediate threat to a national security interest; or
- D) (U) An ongoing attack on a protected computer (as defined in 18 U.S.C. § 1030) that constitutes a crime punishable by a term of imprisonment greater than one year.

(U) Only DOJ officials have the authority to authorize the emergency installation of a PR/TT. The FBI does not have this authority. If the DOJ authorizes the emergency installation of a PR/TT, the government has 48 hours after the installation to apply for and obtain a court order according to 18 U.S.C. § 3123. It is a violation of law to fail to apply for and obtain a court order within this 48 hour period. Use of the PR/TT shall immediately terminate when the information sought is obtained, when the application for a court order is denied, or if no court order has been obtained 48 hours after the installation of the PR/TT device in emergency situations.

(U//FOUO) As with requesting authorization for an emergency Title III

b7E

Once that

ACLU EC-173

approval has been obtained, the DOJ attorney will advise the AUSA that the emergency use has been approved and that the law enforcement agency may proceed with the installation and use of the PR/TT. The DOJ attorney will send a verification memorandum, signed by the authorizing official, to the AUSA. The AUSA will include an authorization memorandum with the application for the court order approving the emergency use.

(U//FOUO) If an emergency situation arises after regular business hours [redacted]
[redacted] b7E
During regular business hours [redacted]
[redacted]

18.6.9.6 (U) DURATION OF APPROVAL

- A) (U) *FISA*: The use of a PR/TT device may be authorized by the FISC for a period of time not to exceed 90 days in investigations targeting an USPER. Extensions may be granted for periods not to exceed 90 days upon re-application to the court. In investigations in which the applicant has certified that the information likely to be obtained is foreign intelligence information not concerning a U.S. person (USPER), an order or extension may be for a period of time not to exceed one year.
- B) (U) *Criminal*: The installation and use of a PR/TT device may be authorized by court order under 18 U.S.C. § 3123 for a period not to exceed 60 days, which may be extended for additional 60-day periods.

18.6.9.7 (U) SPECIFIC PROCEDURES

(U//FOUO) Prior to installing and using a PR/TT device (whether issued in a criminal or national security matter), the case agent must:

- A) (U//FOUO) [redacted]
- B) (U//FOUO) [redacted] b7E
- C) (U//FOUO) [redacted]
- D) (U//FOUO) [redacted]

ACLU EC-174

18-131

§18

(U//FOUO) [REDACTED] b7E

18.6.9.8 (U) USE OF FISA DERIVED INFORMATION IN OTHER PROCEEDINGS

(U//FOUO) There are statutory (50 U.S.C. Sections 1806, 1825, and 1845) and Attorney General (AG) policy restrictions on the use of information derived from a FISA ELSUR, physical search, or PR/TT. These restrictions apply to and must be followed by anyone “who may seek to use or disclose FISA information in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States. . . .” See DIOG Appendix E for the AG Memo, Revised Policy on the Use or Disclosure of FISA Information, dated 01-10-2008. The guidance in the AG’s Memo establishes notification/approval procedures which must be strictly followed. Though not contained in the AG Memo, FBI policy requires that [REDACTED] b7E [REDACTED] Questions concerning the FISA use policy or requests for assistance in obtaining FISA use authority from the AG should be directed to NSLB’s Classified Litigation Support Unit.

(U//FOUO) The United States must, prior to the trial, hearing, or other proceeding or at a reasonable time prior to an effort to disclose or use that information or submit it into evidence, notify the “aggrieved person” [as defined in 50 U.S.C. Sections 1801(k), 1821(2), or 1841(2)], and the court or other authority in which the information is to be disclosed or used, that the United States intends to disclose or use such information. See 50 U.S.C. Sections 1806(c), 1825(d), and 1845(c).

18.6.9.9 (U) CONGRESSIONAL NOTICE AND REPORTING REQUIREMENTS

18.6.9.9.1 (U) CRIMINAL PEN REGISTER/TRAP AND TRACE- ANNUAL REPORT

(U) The Attorney General is required to make an annual report to Congress on the number of criminal PR/TT orders applied for by DOJ law enforcement agencies. See 18 U.S.C. § 3126. The report must include the following information:

- A) (U) The period of interceptions authorized by the order, and the number and duration of any extensions;
- B) (U) The offense specified in the order or application, or extension;
- C) (U) The number of investigations involved;
- D) (U) The number and nature of the facilities affected; and
- E) (U) The identity, including the district, of the applying agency making the application and the person authorizing the order.

(U//FOUO) DOJ, Criminal Division, OEO requires the FBI to provide quarterly reports on pen register usage. To satisfy DOJ data requirements and standardize and simplify field reporting, court-ordered pen register usage must be reported to FBIHQ [REDACTED] b7E [REDACTED] within five (5) workdays after the expiration date of an original order and any extensions, or denial of an application for an order. For all criminal PR/TT orders or extensions issued on or after January 1, 2009, the

ACLU EC-175

18-132

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

18.6.9.9.2 (U) NATIONAL SECURITY PEN REGISTERS AND TRAP AND TRACE – SEMI-ANNUAL REPORT

(U) The Attorney General must inform the House Permanent Select Committee on Intelligence, Senate Select Committee on Intelligence, Committee of the Judiciary of the House Representatives, and Committee of the Judiciary of the Senate concerning all uses of PR/TT devices pursuant to 50 U.S.C. § 1846. This report is coordinated through DOJ NSD. A semi-annual report must be submitted that contains the following information:

- A) (U) The total number of applications made for orders approving the use of PR/TT devices;
- B) (U) The total number of such orders either granted, modified, or denied; and
- C) (U) The total number of PR/TT devices whose installation and use was authorized by the Attorney General on an emergency basis and the total number of subsequent orders approving or denying the installation and use of such PR/TT devices.

18.6.9.10 (U) POST CUT-THROUGH DIALED DIGITS (PCTDD)

18.6.9.10.1 (U) OVERVIEW

(U//FOUO) Telecommunication networks provide users the ability to engage in extended dialing and/or signaling (also known as "post cut-through dialed digits" or PCTDD), which in some circumstances are simply call-routing information and, in others, are call content. For example, non-content PCTDD may be generated when a party places a calling card, credit card, or collect call by first dialing a long-distance carrier access number and then, after the initial call is "cut through," dialing the telephone number of the destination party. In other instances, PCTDD may represent call content, such as when a party calls an automated banking service and enters an account number, calls a pharmacy's automated prescription refill service and enters prescription information, or enters a call-back number when prompted by a voice mail service. See United States Telecom Assn v. Federal Communications Commission, 227 F.3d 450, 462 (D.C. Cir. 2000).

[REDACTED] b7E

(U//FOUO) The definition of both a pen register device and a trap and trace device provides that the information collected by these devices "shall not include the contents of any communication." See 18 U.S.C. § 3127(3) and (4). In addition, 18 U.S.C. § 3121(e) makes explicit the requirement to "use technology reasonably available" that restricts the collection of information "so as not to include the contents of any wire or electronic communications." "Content" includes any information concerning the substance, purport, or meaning of a communication. See 18 U.S.C. § 2510(8). When the pen register definition is read in conjunction with the limitation provision, however, it suggests that although a PR/TT device may not be used for the express purpose of collecting content, the incidental collection of content may occur despite the use of "reasonably available" technology to minimize, to the

§18

extent feasible, any possible over collection of content while still allowing the device to collect all of the dialing and signaling information authorized.

(U//FOUO) *DOJ Policy:* In addition to this statutory obligation, DOJ has issued a directive in [redacted] to all DOJ agencies requiring that no affirmative investigative use may be made of PCTDD incidentally collected that constitutes content, except in cases of emergency—to prevent an immediate danger of death, serious physical injury, or harm to the national security.

(U//FOUO) [redacted] b7E

18.6.9.10.2 (U) COLLECTION OF PCTDD

(U//FOUO) [redacted]

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

B) (U//FOUO) [redacted]

18.6.9.10.3 (U) USE OF PCTDD

(U//FOUO) [redacted] b7E

A) (U//FOUO) [redacted]

ACLU EC-177

1) (U//FOUO) [Redacted]

2) (U//FOUO) [Redacted]

3) (U//FOUO) [Redacted]

4) (U//FOUO) [Redacted]

5) (U//FOUO) [Redacted] b7E

B) (U//FOUO) [Redacted]

1) (U//FOUO) [Redacted]

2) (U//FOUO) [Redacted]

18.6.9.10.4 (U) WHAT CONSTITUTES PCTDD CONTENT

(U//FOUO) In applying the above, the term “content” is interpreted to mean “any information concerning the substance, purport, or meaning of a communication” as defined in 18 U.S.C. § 2510. Questions concerning whether specific PCTDD are content as opposed to dialing, routing, addressing, or signaling information should be addressed to the CDC or OGC for coordination with DOJ as necessary.

ACLU EC-178

§18

(U//FOUO) [Redacted] b7E

18.6.9.11 (U//FOUO) [Redacted]

(U//FOUO) [Redacted] b7E

18.6.9.11.1 (U//FOUO) To LOCATE A KNOWN PHONE NUMBER

A) (U//FOUO) Authority: A standard PR/TT order issued pursuant to 18 U.S.C. § 3127 is adequate to authorize the use of this technology to determine the location of a known targeted phone, provided that the language authorizes FBI employees to install or cause to be installed and use a pen register device, without geographical limitation, at any time of day or night within (X) days from the date the order is signed, to record or decode dialing, routing, addressing, or signaling information transmitted by the “Subject Telephone.” Due to varying and often changing court interpretations of the requirements for obtaining cell site location information, agents contemplating legal process to obtain such information should consult as necessary with their CDC and/or AUSA for the legal requirements in their particular jurisdiction. The application and order should generally also request authority to compel disclosure of cell site location data on an ongoing basis under 18 U.S.C. § 2703(d)—or probable cause, if such is required by the particular district court—as such information may assist in determining the general location of the targeted phone. [Redacted]

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

C) (U//FOUO) [Redacted]

ACLU EC-179

[Redacted]

[Redacted] Under Kyllo v. United States, 533 U.S. 27 (2001), the use of equipment not in general public use to acquire data that is not otherwise detectable that emanates from a private premise implicates the Fourth Amendment. [Redacted]

[Redacted]

D) (U//FOUO)

b7E

[Redacted]

18.6.9.11.2 (U//FOUO) To IDENTIFY AN UNKNOWN TARGET PHONE NUMBER

(U//FOUO) *Authority*

[Redacted]

[Redacted]

b7E

(U//FOUO)

[Redacted]

[Redacted]

b7E

ACLU EC-180

§18

A) (U//FOUO) [Redacted]

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

18.6.9.11.3 (U) PR/TT ORDER LANGUAGE

(U) The language in the order should state that "the pen register will be implemented unobtrusively and with minimum interference with the services accorded to customers of such service."

18.7 (U) AUTHORIZED INVESTIGATIVE METHODS IN FULL INVESTIGATIONS

(U) See AGG-Dom, Part V.A.11-13.

(U) In Full Investigations, to include Enterprise Investigations, the authorized investigative methods include:

- A) (U) The investigative methods authorized for Assessments.
 - 1) (U) Public information. (See Section 18.5.1)
 - 2) (U) Records or information - FBI and DOJ. (See Section 18.5.2)
 - 3) (U) Records or information - Other federal, state, local, tribal, or foreign government agency. (See Section 18.5.3)
 - 4) (U) On-line services and resources. (See Section 18.5.4)
 - 5) (U) CHS use and recruitment. (See Section 18.5.5)
 - 6) (U) Interview or request information from the public or private entities. (See Section 18.5.6)
 - 7) (U) Information voluntarily provided by governmental or private entities. (See Section 18.5.7)
 - 8) (U) Physical Surveillance (not requiring a court order). (See Section 18.5.8)
- B) (U) The investigative methods authorized for Preliminary Investigations.
 - 1) (U) Consensual monitoring of communications, including electronic communications. (See Section 18.6.1)
 - 2) (U) Intercepting the communications of a computer trespasser. (See Section 18.6.2)
 - 3) (U) Closed-circuit television/video surveillance, direction finders, and other monitoring devices. (See Section 18.6.3)
 - 4) (U) Administrative subpoenas. (See Section 18.6.4)
 - 5) (U) Grand jury subpoenas. (See Section 18.6.5)
 - 6) (U) National Security Letters. (See Section 18.6.6)
 - 7) (U) FISA Order for business records. (See Section 18.6.7)
 - 8) (U) Stored wire and electronic communications and transactional records. (See Section 18.6.8)¹⁸
 - 9) (U) Pen registers and trap/trace devices. (See Section 18.6.9)
 - 10) (U) Mail covers. (See Section 18.6.10)
 - 11) (U) Polygraph examinations. (See Section 18.6.11)
 - 12) (U) Trash Covers (Searches that do not require a warrant or court order). (See Section 18.6.12)
 - 13) (U) Undercover operations. (See Section 18.6.13)

¹⁸ (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)

§18

- C) (U) Searches – with a warrant or court order (reasonable expectation of privacy). (See Section 18.7.1 below)
- D) (U) Electronic surveillance – Title III. (See Section 18.7.2 below)
- E) (U) Electronic surveillance – FISA and FISA Title VII (acquisition of foreign intelligence information). (See Section 18.7.3 below)

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

ACLU EC-183

Version Dated:
October 15, 2011

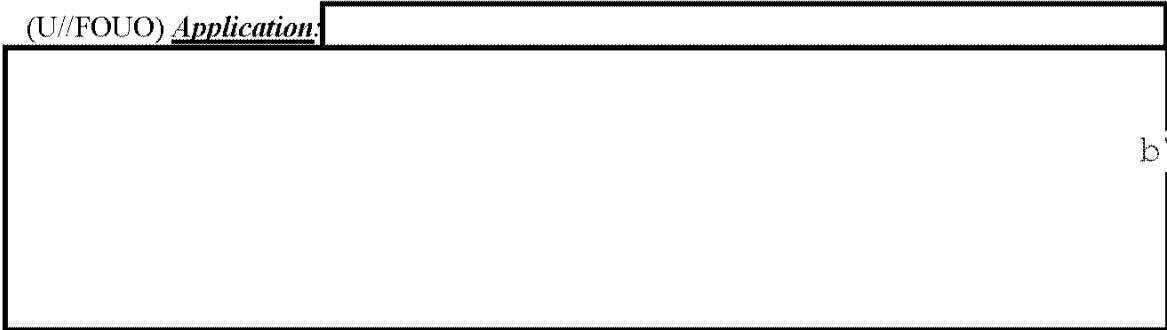
18.7.1 (U) INVESTIGATIVE METHOD: SEARCHES – WITH A WARRANT OR COURT ORDER (REASONABLE EXPECTATION OF PRIVACY)

(U) See AGG-Dom, Part V.A.12 and the Attorney General's Guidelines On Methods Of Obtaining Documentary Materials Held By Third Parties, Pursuant to Title II, Privacy Protection Act of 1980 (Pub. L. 96-440, Sec. 201 et seq.; 42 U.S.C. § 2000aa-11, et seq.).

18.7.1.1 (U) SUMMARY

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

(U//FOUO) Application:



b7E

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

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

18.7.1.2 (U) LEGAL AUTHORITY

(U) Searches conducted by the FBI must be in conformity with FRCP Rule 41; FISA, 50 U.S.C. §§ 1821-1829; or E.O. 12333 § 2.5.

ACLU EC-184

18-155

18.7.1.3 (U) DEFINITION OF INVESTIGATIVE METHOD

(U) ***Physical Search defined:*** A physical search constitutes any physical intrusion within the United States into premises or property (including examination of the interior of property by technical means) that is intended to result in the seizure, reproduction, inspection, or alteration of information, material, or property, under circumstances in which a person has a reasonable expectation of privacy.

(U) A physical search requiring a warrant does not include: (i) electronic surveillance as defined in FISA or Title III; or (ii) the acquisition by the United States Government of foreign intelligence information from international foreign communications, or foreign intelligence activities conducted according to otherwise applicable federal law involving a foreign electronic communications system, using a means other than electronic surveillance as defined in FISA.

18.7.1.3.1 (U) REQUIREMENT FOR REASONABLENESS

(U) By the terms of the Fourth Amendment, a search must be reasonable at its inception and reasonable in its execution.

[REDACTED]

b7E

18.7.1.3.2 (U) REASONABLE EXPECTATION OF PRIVACY

(U) The right of privacy is a personal right, not a property concept. It safeguards whatever an individual reasonably expects to be private. The protection normally includes persons, residences, vehicles, other personal property, private conversations, private papers and records. The Supreme Court has determined that there is no reasonable expectation of privacy in certain areas or information. As a result, government intrusions into those areas do not constitute a search and, thus, do not have to meet the requirements of the Fourth Amendment. These areas include: (i) open fields; (ii) prison cells; (iii) public access areas; and (iv) vehicle identification numbers. The Supreme Court has also determined that certain governmental practices do not involve an intrusion into a reasonable expectation of privacy and, therefore, do not amount to a search. These practices include: (i) aerial surveillance conducted from navigable airspace; (ii) field test of suspected controlled substance; and (iii) odor detection. A reasonable expectation of privacy may be terminated by an individual taking steps to voluntarily relinquish the expectation of privacy, such as abandoning property or setting trash at the edge of the curtilage or beyond for collection.

18.7.1.3.3 (U) ISSUANCE OF SEARCH WARRANT

(U) Under FRCP Rule 41, upon the request of a federal law enforcement officer or an attorney for the government, a search warrant may be issued by:

- A) (U) a federal magistrate judge, or if none is reasonably available, a judge of a state court of record within the federal district, for a search of property or for a person within the district;

- B) (U) a federal magistrate judge for a search of property or for a person either within or outside the district if the property or person is within the district when the warrant is sought but might move outside the district before the warrant is executed;
- C) (U) a federal magistrate judge in any district in which activities related to the terrorism may have occurred, for a search of property or for a person within or outside the district, in an investigation of domestic terrorism or international terrorism (as defined in 18 U.S.C. § 2331); and
- D) (U) a magistrate with authority in the district to issue a warrant to install a tracking device. The warrant may authorize use of the device to track the movement of a person or property located within the district, outside, or both.

(U) Physical searches related to a national security purpose may be authorized by the FISC. (50 U.S.C. §§ 1821-1829)

18.7.1.3.4 (U) PROPERTY OR PERSONS THAT MAY BE SEIZED WITH A WARRANT

(U) A warrant may be issued to search for and seize any: (i) property that constitutes evidence of the commission of a criminal offense; (ii) contraband, the fruits of crime, or things otherwise criminally possessed; or (iii) property designed or intended for use or that is or has been used as the means of committing a criminal offense. In addition to a conventional search conducted following issuance of a warrant, examples of search warrants include:

18.7.1.3.4.1 (U) ANTICIPATORY WARRANTS

(U) As the name suggests, an anticipatory warrant differs from other search warrants in that it is not supported by probable cause to believe that contraband exists at the premises to be searched at the time the warrant is issued. Instead, an anticipatory search warrant is validly issued where there is probable cause to believe that a crime has been or is being committed, and that evidence of such crime will be found at the described location at the time of the search, but only after certain specified events transpire. These conditions precedent to the execution of an anticipatory warrant, sometimes referred to as "triggering events," are integral to its validity. Because probable cause for an anticipatory warrant is contingent on the occurrence of certain expected or "triggering" events, typically the future delivery, sale, or purchase of contraband, the judge making the probable cause determination must take into account the likelihood that the triggering event will occur on schedule and as predicted. Should these triggering events fail to materialize, the anticipatory warrant is void.

18.7.1.3.4.2 (U) SNEAK AND PEEK SEARCH WARRANTS

(U) A sneak and peek search warrant allows law enforcement agents to surreptitiously enter a location such as a building, an apartment, garage, storage shed, etc. for the purpose of looking for and documenting evidence of criminal activity.

[Redacted]

b7E

ACLU EC-186

18-157

18.7.1.3.4.3 (U) MAIL OPENINGS

(U) Mail in United States postal channels may be searched only pursuant to court order, or presidential authorization. United States Postal Service regulations governing such activities must be followed. A search of items that are being handled by individual couriers, or commercial courier companies, under circumstances in which there is a reasonable expectation of privacy, or have been sealed for deposit into postal channels, and that are discovered within properties or premises being searched, must be carried out according to unconsented FISA or FRCP Rule 41 physical search procedures.

18.7.1.3.4.4 (U) COMPELLED DISCLOSURE OF THE CONTENTS OF STORED WIRE OR ELECTRONIC COMMUNICATIONS

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

18.7.1.3.4.4.1 (U) SEARCH WARRANT

(U//FOUO) Investigators can obtain the full contents of a network account with a search warrant. ECPA does not require the government to notify the customer or subscriber when it obtains information from a provider using a search warrant. Warrants issued under 18 U.S.C. § 2703 must either comply with FRCP Rule 41 or be an equivalent state warrant. Warrants issued pursuant to 18 U.S.C. § 2703 do not require personal service on the customer; the warrants are only be served on the electronic communication service or a remote computing service. FRCP Rule 41 requires a copy of the warrant be left with the provider, and a return and inventory be made. Federal courts have nationwide jurisdiction to issue these search warrants (see below).

(U) With a search warrant issued based on probable cause pursuant to FRCP Rule 41 or an equivalent state warrant, the government may obtain:

ACLU EC-187

18-158

A) (U) The contents of a wire or electronic communication that has been in electronic storage in an electronic communications system for one hundred and eighty days or less, and

B) (U) Everything that can be obtained using a 18 U.S.C. § 2703(d) court order with notice.

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

18.7.1.3.4.4.2 (U) NATIONWIDE SCOPE

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

18.7.1.3.4.4.3 (U) SERVICE OF PROCESS

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

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

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

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

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

§18

Domestic Investigations and Operations Guide

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

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

(U) [Redacted]

(U) [Redacted] b7E

18.7.1.3.4.4.5 (U) LEGAL STANDARD

(U) To order delayed notice, the court must find that "there is reason to believe that notification of the existence of the court order may... endanger the life or physical safety of an individual; [lead to] flight from prosecution; [lead to] destruction of or tampering with evidence; [lead to] intimidation of potential witnesses; or . . . otherwise seriously jeopardiz[e] an investigation or unduly delay[] a trial." 18 U.S.C. §§ 2705(a)(1)(A) and 2705(a)(2). The applicant must satisfy this standard anew each time an extension of the delayed notice is sought.

18.7.1.3.4.4.6 (U) NATIONWIDE SCOPE

(U) Federal court orders under 18 U.S.C. § 2703(d) have effect outside the district of the issuing court. Orders issued pursuant to 18 U.S.C. § 2703(d) may compel providers to disclose information even if the information is stored outside the district of the issuing court. See 18 U.S.C. § 2703(d) ("any court that is a court of competent jurisdiction" may issue a 18 U.S.C. § 2703[d] order); 18 U.S.C. § 2711(3) (court of competent jurisdiction includes any federal court having jurisdiction over the offense being investigated without geographic limitation).

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

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

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

ACLU EC-189

18-160

- A) (U) All "record(s) or other information pertaining to a subscriber to or customer of such service (not including the contents of communications [held by providers of electronic communications service and remote computing service])," and
- B) (U) Basic subscriber information that can be obtained using a subpoena without notice. 18 U.S.C. § 2703(c)(1).

18.7.1.4 (U) APPROVAL REQUIREMENTS FOR INVESTIGATIVE METHOD

- A) (U//FOUO) ***Search warrants issued under authority of FRCP Rule 41:*** A warrant to search is issued by a federal magistrate (or a state court judge if a federal magistrate is not reasonably available). Coordination with the USAO or DOJ is required to obtain the warrant.
- B) (U//FOUO) ***FISA:*** In national security investigations, field office requests for FISA authorized physical searches must be submitted to FBIHQ using the FBI FISA Request Form. Field office requests for FISA approval are tracked through [redacted] This form should be completed by the case agent. b7E
- C) (U//FOUO) ***Sensitive Investigative Matters (SIM):*** Notice to the appropriate FBIHQ operational Unit Chief and Section Chief is required if the matter under investigation is a sensitive investigative matter. Notice to DOJ is also required, as described in DIOG Section 10.

18.7.1.5 (U) DURATION OF APPROVAL

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

18.7.1.6 (U) SPECIFIC PROCEDURES

18.7.1.6.1 (U) OBTAINING A WARRANT UNDER FRCP RULE 41

18.7.1.6.1.1 (U) PROBABLE CAUSE

(U//FOUO) After receiving an affidavit or other information, a magistrate judge or a judge of a state court of record must issue the warrant if there is probable cause to search for and seize a person or property under FRCP Rule 41(c). Probable cause exists where "the facts and circumstances within the FBI employee's knowledge, and of which they had reasonably trustworthy information are sufficient in themselves to warrant a person of reasonable caution in the belief that..." a crime has been or is being committed, and that sizable property can be found at the place or on the person to be searched. Probable cause is a reasonable belief grounded on facts. In judging whether a reasonable belief exists, the test is whether such a belief would be engendered in a prudent person with the officer's training and experience. To establish probable cause, the affiant must demonstrate a basis for knowledge and belief that the facts are true and that there is probable cause to believe the items listed in the affidavit will be found at the place to be searched.

18.7.1.6.1.2 (U) REQUESTING A WARRANT IN THE PRESENCE OF A JUDGE

- A) (U) ***Warrant on an Affidavit:*** When a federal law enforcement officer or an attorney for the government presents an affidavit in support of a warrant, the judge may require the affiant to

ACLU EC-190

18-161

appear personally and may examine under oath the affiant and any witness the affiant produces.

- B) (U) **Warrant on Sworn Testimony**: The judge may wholly or partially dispense with a written affidavit and base a warrant on sworn testimony if doing so is reasonable under the circumstances.
- C) (U) **Recording Testimony**: Testimony taken in support of a warrant must be recorded by a court reporter or by a suitable recording device, and the judge must file the transcript or recording with the clerk, along with any affidavit.

18.7.1.6.1.3 (U) REQUESTING A WARRANT BY TELEPHONIC OR OTHER MEANS

- A) (U) **In General**: A magistrate judge may issue a warrant based on information communicated by telephone or other appropriate means, including facsimile transmission.
- B) (U) **Recording Testimony**: Upon learning that an applicant is requesting a warrant, a magistrate judge must: (i) place under oath the applicant and any person on whose testimony the application is based; and (ii) make a verbatim record of the conversation with a suitable recording device, if available, or by a court reporter, or in writing.
- C) (U) **Certifying Testimony**: The magistrate judge must have any recording or court reporter's notes transcribed, certify the transcription's accuracy, and file a copy of the record and the transcription with the clerk. Any written verbatim record must be signed by the magistrate judge and filed with the clerk.
- D) (U) **Suppression Limited**: Absent a finding of bad faith, evidence obtained from a warrant issued under FRCP Rule 41(d)(3)(A) is not subject to suppression on the ground that issuing the warrant in that manner was unreasonable under the circumstances.

18.7.1.6.1.4 (U) ISSUING THE WARRANT

(U) In general, the magistrate judge or a judge of a state court of record must issue the warrant to an officer authorized to execute it. The warrant must identify the person or property to be searched, identify any person or property to be seized, and designate the magistrate judge to whom it must be returned. The warrant must command the officer to: (i) execute the warrant within a specified time no longer than 10 days; (ii) execute the warrant during the daytime, unless the judge for good cause expressly authorizes execution at another time; and (iii) return the warrant to the magistrate judge designated in the warrant.

18.7.1.6.1.5 (U) WARRANT BY TELEPHONIC OR OTHER MEANS

(U) If a magistrate judge decides to proceed under FRCP Rule 41(d)(3)(A), the following additional procedures apply:

- A) (U) **Preparing a Proposed Duplicate Original Warrant**: The applicant must prepare a "proposed duplicate original warrant" and must read or otherwise transmit the contents of that document verbatim to the magistrate judge.
- B) (U) **Preparing an Original Warrant**: The magistrate judge must enter the contents of the proposed duplicate original warrant into an original warrant.

- C) (U) **Modifications:** The magistrate judge may direct the applicant to modify the proposed duplicate original warrant. In that case, the judge must also modify the original warrant.
- D) (U) **Signing the Original Warrant and the Duplicate Original Warrant:** Upon determining to issue the warrant, the magistrate judge must immediately sign the original warrant, enter on its face the exact time it is issued, and direct the applicant to sign the judge's name on the duplicate original warrant.

18.7.1.6.1.6 (U) EXECUTING AND RETURNING THE WARRANT

- A) (U) **Noting the Time:** The officer executing the warrant must enter on its face the exact date and time it is executed.
- B) (U) **Inventory:** An officer present during the execution of the warrant must prepare and verify an inventory of any property seized. The officer must do so in the presence of another officer and the person from whom, or from whose premises, the property was taken. If either one is not present, the officer must prepare and verify the inventory in the presence of at least one other credible person.
- C) (U) **Receipt:** The officer executing the warrant must: (i) give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken; or (ii) leave a copy of the warrant and receipt at the place where the officer took the property.
- D) (U) **Return:** The officer executing the warrant must promptly return it — together with a copy of the inventory — to the magistrate judge designated on the warrant. The judge must, on request, give a copy of the inventory to the person from whom, or from whose premises, the property was taken and to the applicant for the warrant.

18.7.1.6.1.7 (U) FORWARDING PAPERS TO THE CLERK

(U) The magistrate judge to whom the warrant is returned must attach to the warrant a copy of the return, the inventory, and all other related papers and must deliver them to the clerk in the district where the property was seized. (FRCP Rule 41)

18.7.1.6.1.8 (U) WARRANT FOR A TRACKING DEVICE

- A) (U) **Noting the Time:** The officer executing a tracking device warrant must enter on it the exact date and time the device was installed and the period during which it was used.
- B) (U) **Return:** Within 10 calendar days after the use of the tracking device has ended, the officer executing the warrant must return it to the judge designated in the warrant.
- C) (U) **Service:** Within 10 calendar days after use of the tracking device has ended, the officer executing the warrant must serve a copy of the warrant on the person who was tracked. Service may be accomplished by delivering a copy to the person who, or whose property was tracked; or by leaving a copy at the person's residence or usual place of abode with an individual of suitable age and discretion who resides at that location and by mailing a copy to the person's last known address. Upon request of the government, the judge may delay notice as provided in FRCP Rule 41(f)(3).

18.7.1.6.1.9 (U) DELAYED NOTICE

(U) Upon the government's request, a magistrate judge—or if authorized by FRCP Rule 41(b), a judge of a state court of record—may delay any notice required by FRCP Rule 41 if the delay is authorized by statute.

18.7.1.6.2 (U) OBTAINING A FISA WARRANT

(U) Applications for court-authorized physical search pursuant to FISA must be made by a federal officer in writing upon oath or affirmation and with the specific approval of the Attorney General. (See 50 U.S.C. § 1823).

18.7.1.6.2.1 (U) CERTIFICATE BY THE DIRECTOR OF THE FBI

(U) Each FISA application must be accompanied by a Certification by the Director of the FBI or one of nine other individuals authorized by Congress or the President to provide such certifications that: the information being sought is foreign intelligence information; that a significant purpose of the search is to obtain foreign intelligence information; that such information cannot reasonably be obtained by normal investigative techniques; that the information sought is "foreign intelligence information" as defined by FISA. The certification must include a statement explaining the certifier's basis for the certification.

(U) 50 U.S.C. § 1823 specifies the Assistant to the President for National Security Affairs; E.O. 12139 as amended by E.O. 13383 specifies the Director of the FBI, Deputy Director of the FBI, the Director of National Intelligence, the Principal Deputy Director of National Intelligence, the Director of the Central Intelligence Agency, the Secretary of State, the Deputy Secretary of State, the Secretary of Defense, and the Deputy Secretary of Defense as appropriate officials to make certifications required by FISA. The FBI Director has represented to Congress that the FBI deputy Director will only certify FISA's when the FBI Director is not available to do so.

18.7.1.6.2.2 (U) LENGTH OF PERIOD OF AUTHORIZATION FOR FISC ORDERS

(U) Generally, a FISC Order approving an unconsented physical search will specify the period of time during which physical searches are approved and provide that the government will be permitted the period of time necessary to achieve the purpose, or for 90 days, whichever is less, except that authority may be:

- A) (U) For no more than one year for "Foreign Power" targets (establishments); or
- B) (U) For no more than 120 days for a non-USPER agent of a foreign power, with renewals for up to one.

18.7.1.6.2.3 (U) EXTENSION OF PHYSICAL SEARCH AUTHORITY

(U//FOUO) An extension of physical search authority may be granted on the same basis as the original order upon a separate application for an extension and upon new findings made in the same manner as the original order.

18.7.1.6.2.4 (U) EMERGENCY FISA AUTHORITY

A) (U) The Attorney General may authorize an emergency physical search under FISA when he reasonably makes a determination that an emergency situation exists that precludes advance FISA court review and approval, and there exists a factual predication for the issuance of a FISA Court Order. In such instances, a FISC judge must be informed by the Attorney General or his designee at the time of the authorization and an application according to FISA requirements is submitted to the judge as soon as is practicable but not more than seven (7) days after the emergency authority has been approved by the Attorney General.

B) (U) If a court order is denied after an emergency authorization has been initiated, no information gathered as a result of the search may be used in any manner except if with the approval of the Attorney General, the information indicates a threat of death or serious bodily harm to any person.

C) (U//FOUO) For an emergency FISA for physical search [redacted]

b7E

18.7.1.6.2.5 (U) SPECIAL CIRCUMSTANCES

(U) The President through the Attorney General may also authorize a physical search under FISA without a court order for periods of up to one year, if the Attorney General certifies that the search will be solely directed at premises, information, material, or property that is used exclusively by or under the open and exclusive control of a foreign power; there is no substantial likelihood that the physical search will involve the premises, information, material, or property of a United States person (USPER); and there are minimization procedures that have been reported to the court and Congress. The FBI's involvement in such approvals is usually in furtherance of activities pursued according to E.O. 12333. Copies of such certifications are to be transmitted to the FISA Court. See 50 U.S.C. § 1822[a].

(U) Information concerning USPERs acquired through unconsented physical searches may only be used according to minimization procedures. See: 50 U.S.C. §§ 1824(d)(4) and 1825(a).

18.7.1.6.2.6 (U) REQUIRED NOTICE

(U) If an authorized search involves the premises of an USPER, and the Attorney General determines that there is no national security interest in continuing the secrecy of the search, the Attorney General must provide notice to the USPER that the premises was searched and the identification of any property seized, altered, or reproduced during the search.

18.7.1.6.2.7 (U//FOUO) FISA VERIFICATION OF ACCURACY PROCEDURES

(U//FOUO) [redacted]

b7E

§18

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

A) (U//FOUO) Each investigative file for which an application is or has been prepared for submission to the FISC must include [redacted]. This [redacted] sub-file must be used for copies of all of the supporting documentation relied upon when making the certifications contained on the [redacted] b7E

[redacted]
[redacted] must include:

1) (U//FOUO) [redacted]

[redacted]

2) (U//FOUO) [redacted]

[redacted] and

3) (U//FOUO) [redacted]

[redacted] b7E

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

18.7.1.6.2.8 (U) USE OF FISA DERIVED INFORMATION IN OTHER PROCEEDINGS

(U//FOUO) There are statutory (50 U.S.C. Sections 1806, 1825, and 1845) and Attorney General (AG) policy restrictions on the use of information derived from a FISA ELSUR, physical search, or PR/TT. These restrictions apply to and must be followed by anyone “who may seek to use or disclose FISA information in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States. . . .” See DIOG Appendix E for the AG Memo, Revised Policy on the Use or Disclosure of FISA Information, dated 01-10-2008. The guidance in the AG’s Memo establishes notification/approval procedures which must be strictly followed. Though not contained in the AG Memo, FBI policy requires that [redacted] b7E

[redacted] b7E

ACLU-EC 195

[Redacted] b7E

(U//FOUO) The United States must, prior to the trial, hearing, or other proceeding or at a reasonable time prior to an effort to disclose or use that information or submit it into evidence, notify the “aggrieved person” [as defined in 50 U.S.C. Sections 1801(k), 1821(2), or 1841(2)], and the court or other authority in which the information is to be disclosed or used, that the United States intends to disclose or use such information. See 50 U.S.C. Sections 1806(e), 1825(d), and 1845(c).

18.7.1.6.2.9 (U//FOUO) [Redacted]
[Redacted]

(U//FOUO) Each investigative file for which an application is or has been prepared for submission to the FISC will include a sub-file to be labeled [Redacted]. This [Redacted] sub-file is to contain copies of all applications to and orders issued by the FISC for the conduct of physical searches in the investigation. The following data must be included in this [Redacted] b7E

- A) (U//FOUO) [Redacted]
and
- B) (U//FOUO) [Redacted]

18.7.1.6.2.10 (U//FOUO) FISA RENEWALS

(U//FOUO) [Redacted]
[Redacted]

(U//FOUO) [Redacted]
[Redacted] b7E

(U//FOUO) [Redacted]
[Redacted]

18.7.1.6.2.10.1 (U) APPEALING THE DECISION OF THE REVIEW BOARD

(U//FOUO) [Redacted]
[Redacted]

ACLU EC-196

§18



18.7.1.6.2.11 (U) COMPLIANCE AND MONITORING FOR FISA

(U//FOUO)



b7E

18.7.1.6.2.12 (U) FISA OVERCOLLECTION



Contact NSLB for further guidance regarding the handling of any FISA overcollection.

18.7.2 (U) INVESTIGATIVE METHOD: ELECTRONIC SURVEILLANCE – TITLE III

18.7.2.1 (U) SUMMARY

(U//FOUO) Electronic Surveillance (ELSUR) under Title III is a valuable investigative method. It is, also, a very intrusive means of acquiring information relevant to the effective execution of the FBI's law enforcement. To ensure that due consideration is given to the competing interests between law enforcement and the effect on privacy and civil liberties, this section contains various administrative and management controls beyond those imposed by statute and DOJ guidelines. Unless otherwise noted, it is the responsibility of the case agent and his/her supervisor to ensure compliance with these instructions. [REDACTED] b7E

[REDACTED] Title III ELSUR requires: (i) administrative or judicial authorization prior to its use; (ii) contact with the field office ELSUR Technician to coordinate all necessary recordkeeping; and (iii) consultation with the Technical Advisor (TA) or a designated TTA to determine feasibility, applicability, and use of the appropriate equipment.

(U//FOUO) *Application:* [REDACTED]

b7E

18.7.2.2 (U) LEGAL AUTHORITY

(U) Title III ELSUR is authorized by chapter 119, 18 U.S.C. §§ 2510-2522 (Title III of the Omnibus and Safe Streets Act of 1968).

18.7.2.3 (U) DEFINITION OF INVESTIGATIVE METHOD

(U) Title III ELSUR is the non-consensual electronic collection of information (usually communications) under circumstances in which the parties have a reasonable expectation of privacy and court orders or warrants are required.

18.7.2.4 (U) TITLE III GENERALLY

(U) With the prior approval of the Attorney General, or Attorney General's designee, the United States Attorney, by and through an AUSA, or the Strike Force Attorney, may apply to a federal judge for a court order authorizing the interception of wire, oral, or electronic communications relating to one or more of the offenses listed in Title III (18 U.S.C. § 2516). Judicial oversight continues throughout the operational phase of the electronic surveillance including the installation, monitoring, and handling of recording media.

(U) For purposes of obtaining review and approval for use of the method, Title III applications are considered to be either "sensitive" or "non-sensitive." The requirements for each are set forth below.

ACLU EC-198

18-169

18.7.2.5 (U) STANDARDS FOR USE AND APPROVAL REQUIREMENTS FOR NON-SENSITIVE TITLE IIIs

(U//FOUO) An SAC is the authorizing official to approve all requests for “non-sensitive” Title III orders, including original, extension, and renewal applications. SAC approval of all extensions and renewals is required to ensure that field office managers will allocate the resources necessary to use this method. Any delegation of SAC approval authority to an ASAC under this section must be in writing (See DIOG Section 3.4.3).

(U//FOUO) Prior to SAC approval referred to above, CDC or OGC review is required for the initial “non-sensitive” Title III order. Extensions and renewals sought within 30 days after the expiration of the original Title III order in non-sensitive Title IIIs do not require CDC review, unless requested by the SAC or designee. The CDC must review renewals sought more than 30 days after the expiration of the original Title III order.

(U//FOUO) There may be situations or unusual circumstances requiring the FBI to adopt an already existing Title III from another federal law enforcement agency. Such adoptions may only be done on a case-by-case basis, in exceptional circumstances, and subject to the requirements set forth herein relating to CDC review and SAC approval. Should the Title III proposed for adoption involve sensitive circumstances, it must also be handled in accordance with the approval and review requirements set forth below.

18.7.2.6 (U) STANDARDS FOR USE AND APPROVAL REQUIREMENTS FOR SENSITIVE TITLE IIIs

(U//FOUO) All Title III applications involving one of the seven “sensitive circumstances,” listed below, including all extensions and renewals, must be reviewed by OGC and approved by FBIHQ. The SAC, with the recommendation of the CDC, must determine whether the request involves sensitive circumstances. The term “sensitive circumstances” as used in this section relating to electronic surveillance under Title III is different from the term “sensitive investigative matters,” as used in conjunction with approval requirements for opening Assessments and Predicated Investigations, and is different from the term “sensitive monitoring circumstances” as used in conjunction with the approval requirements for consensual monitoring.

(U//FOUO) The field office must include a copy of the completed CDC checklist (FD-926) when forwarding the initial sensitive Title III applications to OGC and FBIHQ for review. After the initial submission, the CDC checklist must be completed by the appropriate OGC unit for all subsequent extensions or renewals of sensitive Title IIIs.

(U//FOUO) Although ultimate approval for sensitive Title IIIs is at the FBIHQ level, the SAC or ASAC must continue to review and approve the use of the method for all sensitive Title III applications as it relates to the allocation of resources within their field office.

(U//FOUO) The following five sensitive circumstances require the approval of a Deputy Assistant Director (DAD) or a higher level official from the Criminal Investigative Division (CID), Cyber Division, Counterterrorism Division (CTD), Weapons of Mass Destruction Directorate (WMDD), or Counterintelligence Division (CD), as appropriate, and such approvals must be documented in an EC:

ACLU EC-199

18-170

- A) (U//FOUO) Significant privilege issues or First Amendment concerns (e.g., attorney-client privilege or other privileged conversations or interception of news media representatives);
- B) (U//FOUO) Significant privacy concerns are anticipated (e.g., placing a microphone in a bedroom or bathroom);
- C) (U//FOUO) Application is based on “relaxed specificity” (i.e., “roving” interception) under 18 U.S.C. § 2518(11)(a) and (b);
- D) (U//FOUO) Application concerns a Domestic Terrorism (DT), International Terrorism, or Espionage investigation; or
- E) (U//FOUO) Any situation deemed appropriate by the AD of CID or OGC.

(U//FOUO) The following two sensitive circumstances require the approval of the Director, the Acting Director, Deputy Director, or the Executive Assistant Director (EAD) for the Criminal Cyber Response and Services Branch or National Security Branch, or the respective Assistant Director for Criminal Investigative Division (CID), Cyber Division, Counterterrorism Division (CTD), Weapons of Mass Destruction Directorate (WMDD), or Counterintelligence Division (CD), and such approvals must be documented in an EC:

- A) (U//FOUO) "Emergency" Title III interceptions (i.e., interceptions conducted prior to judicial approval under 18 U.S.C. § 2518(7)); or
- B) (U//FOUO) It is anticipated that conversations of members of Congress, federal judges, high-level federal officials, high-level state executives, or members of a state judiciary or legislature will be intercepted.

(U//FOUO) “Sensitive circumstances” may develop at any point in time during the course of a Title III. For example, while an initial application for interceptions might not be considered sensitive, conversations intercepted thereafter of a high-level state executive would render any subsequent spinoffs, extensions, or renewals “sensitive” Title III requests.

(U//FOUO) Note: When drafting the Title III Affidavit, the agent must determine whether the proposed Title III intercept involves any of the DOJ-designated seven "sensitive circumstances" listed in DIOG Section 18.7.2.6. If the proposed Title III will involve one or more of the seven "sensitive circumstances," the agent must consult with the assigned AUSA to determine how the "sensitive circumstance(s)" will be addressed and how/when the federal judge will be notified.

18.7.2.7 (U) PROCEDURES FOR EMERGENCY TITLE III INTERCEPTIONS

(U//FOUO) 18 U.S.C. § 2518(7) provides that any investigative or law enforcement officer, specially designated by the Attorney General, Deputy Attorney General, or the Associate Attorney General, who reasonably determines that an emergency situation exists that requires communications to be intercepted before an order authorizing such interception can, with due diligence, be obtained, and there are grounds upon which an order could be entered authorizing interception, may intercept such communications.

(U//FOUO) Section 2518(7) postpones, rather than eliminates the need for judicial authorization. If the Attorney General, Deputy Attorney General, or the Associate Attorney General authorizes an appropriate FBI official to approve an emergency Title III interception, an after-the-fact application for an order approving the interception must be made in

ACLU EC-200

§18

accordance with Title III to the appropriate Court, and an order obtained, within 48 hours after the interception has occurred or begins to occur.

(U//FOUO) [Redacted]

b7E

(U) 18 U.S.C. § 2518(7) defines an emergency situation as one involving:

- A) (U) immediate danger of death or serious physical injury to any person,
- B) (U) conspiratorial activities threatening the national security interest, or
- C) (U) conspiratorial activities characteristic of organized crime.

(U//FOUO) In all but the most unusual circumstances, the only situations likely to constitute an emergency by the Department of Justice (DOJ) are those involving an imminent threat to life, e.g., a kidnapping, hostage taking, or imminent terrorist activity.

18.7.2.7.1 (U) OBTAINING EMERGENCY AUTHORIZATION

(U//FOUO) [Redacted]

A) (U//FOUO) [Redacted]

b7E

B) (U//FOUO) [Redacted]

b7E

ACLU EC-201

[Redacted]

C) (U//FOUO) During off-duty hours, requesting field offices should direct emergency Title III

[Redacted]

D) (U//FOUO) [Redacted]

(U//FOUO) [Redacted] b7E

[Redacted]

18.7.2.7.2 (U) POST-EMERGENCY AUTHORIZATION

(U//FOUO) Once the AG or his designee has authorized the Director, or his designee to make the determination whether to proceed with the emergency Title III, the government has 48 hours (including weekends and holidays) from the time the AG granted authorization to apply for a court order approving the interception. The field office, in coordination with the AUSA, must immediately begin preparing an affidavit, application and proposed order for court authorization.

(U//FOUO) The affidavit in support of the after-the-fact application to the court for an order approving the emergency interception must contain only those facts known to the AG or his designee at the time the emergency interception was approved. The application must be accompanied by the [Redacted] form, b7E which must reflect the date and time of the emergency authorization.

(U//FOUO) The government may also request, at the time it files for court-authorization for the emergency, court-authorization to continue the interception beyond the initial 48 hour period. If continued authorization is sought at the same time, one affidavit may be submitted in support of both requests. However, the affidavit must clearly indicate what information was communicated to the AG or his designee at the time the emergency interception was approved and what information was developed thereafter. Two separate applications and proposed orders should be submitted to the court in this situation – one set for the emergency and one set for the extension. If continued interceptions are not being sought, no further authorization is needed from OEO. The AUSA should, however, still submit the application, affidavit, and order to OEO for review. If continued interceptions are sought, that application, affidavit, and

ACLU EC-202

§18

order must be reviewed by OEO and approved by DOJ like any other Title III request. In either situation, the affidavit must also be submitted through the operational unit for OGC review, when time allows.

(U//FOUO) [Redacted]

b7E

(U//FOUO) Pursuant to 18 U.S.C. § 2518(7), in the absence of a court order, interception shall immediately terminate when the communication sought is obtained or when the application for the order is denied, whichever is earlier. In the event an application for approval is denied, or in any other case where the interception is terminated without an order having been issued, the contents of any wire, oral, or electronic communication intercepted shall be treated as having been obtained in violation of Title III, and an inventory shall be served on the person named in the application.

(U//FOUO) [Redacted]

- A) (U//FOUO) [Redacted]
- B) (U//FOUO) [Redacted]
- C) (U//FOUO) [Redacted]

(U//FOUO) [Redacted]

b7E

- A) (U//FOUO) [Redacted]
- B) (U//FOUO) [Redacted]
- C) (U//FOUO) [Redacted]

18.7.2.8 (U) PRE-TITLE III ELECTRONIC SURVEILLANCE (ELSUR) SEARCH POLICY

(U//FOUO) 18 U.S.C § 2518(1)(e) requires that each application for an order to intercept wire, oral, or electronic communications (hereinafter "Title III") contain a statement describing all previous applications for Title III surveillance of the same persons, facilities, or places named in the current application. [Redacted]

[Redacted]

b7E

ACLU EC-203

(U) For specific details on how to conduct and document such ELSUR searches, see DIOG Appendix H.

18.7.2.9 (U) DURATION OF APPROVAL FOR TITLE III

(U) Court orders issued pursuant to Title III are for a period not to exceed 30 days. An “extension” order may be sought to continue monitoring beyond the initial 30-day period without a lapse in time. When a break in coverage has occurred, a “renewal” order may be sought to continue monitoring the same interceptees and facilities identified in the original order. The affidavit and application in support of an extension or renewal must comply with all of the Title III requirements, including approval of the Attorney General or designee.

18.7.2.10 (U) SPECIFIC PROCEDURES FOR TITLE III AFFIDAVITS

(U//FOUO) The requirements in 18 U.S.C. § 2518 must be followed in the preparation of a Title III affidavit. The employee drafting the Title III affidavit and approving officials must consider the following requirements:

- A) (U//FOUO) The identity and qualifications of the affiant must be articulated;
- B) (U//FOUO) For the interception of wire or oral communications, the affidavit must establish probable cause to believe a violation of at least one of the offenses enumerated in 18 U.S.C. § 2516(1) has been, is being, or will be committed. For the interception of electronic communications, the affidavit must establish probable cause to believe that some federal felony has been, is being, or will be committed;
- C) (U//FOUO) The affidavit must set forth the identities of those persons, if known, for whom there is probable cause to believe they are committing the alleged offenses, even if it is not believed they will be intercepted over the target facility. This group of individuals is often referred to as the “Subjects.” “Interceptees” may be listed separately; “interceptee” are those Subjects who are expected to be intercepted;
- D) (U//FOUO) Probable cause must be current and relevant to the use of the particular facilities for which interception is sought;
- E) (U//FOUO) The necessity for the Title III must be articulated. There must be a factual basis for concluding that alternative investigative procedures have been tried and failed or a demonstration why these procedures appear to be unlikely to succeed or would be too dangerous if tried (“boilerplate” statements in this respect are unacceptable);
- F) (U//FOUO) Interceptions must be minimized, as statutorily required;
- G) (U//FOUO) The facility or premises to be intercepted must be described fully, including a diagram, if possible, if microphone installation is contemplated (surreptitious entries may not be conducted for the purpose of preparing a diagram); and
- H) (U//FOUO)

(U//FOUO) A statement describing all previous applications for Title III surveillance of the same persons (both subjects and interceptees), facilities or places named in the current affidavit. To comply with this requirement, a “search,” e.g., an automated indices search of the FBI’s ELSUR Data Application (EDA) system and the systems of other appropriate agencies, must be conducted prior to submitting the Title III affidavit to the DOJ OEO (non-sensitive circumstances) or to the responsible FBIHQ operational unit (sensitive circumstances). The squad SSA is responsible for verifying that pre-Title III ELSUR checks have been completed

ACLU EC-204

§18

Domestic Investigations and Operations Guide

before the affidavit is sent to the court. The ELSUR Operations Technician (EOT) and the ELSUR supervisor are responsible for confirming that ELSUR searches were properly conducted as set forth in the final affidavit submitted to the court.

(U//FOUO) **Note:** When drafting the Title III Affidavit, the agent must determine whether the proposed Title III intercept involves any of the DOJ-designated seven "sensitive circumstances" listed in DIOG Section 18.7.2.6. If the proposed Title III will involve one or more of the seven "sensitive circumstances," the agent must consult with the assigned AUSA to determine how the "sensitive circumstance(s)" will be addressed and how/when the federal judge will be notified.

(U//FOUO) **Note:** It is also recommended that the application include how the FBI will address any sensitive circumstances as listed in DIOG Section 18.7.2.6, if they exist.

(U//FOUO) At least 10 calendar days prior to submitting the original Title III request to DOJ OEO, the field office must forward an electronic communication to FBIHQ setting forth by separate subheading: a synopsis of the investigation; the priority of the investigation within the office; the anticipated manpower and/or linguistic requirements and outside support, if any, that will be needed; a synopsis of the probable cause supporting the Title III application; the prosecutive opinion of the USAO; and description of the interceptees. If a field office is unable to submit the EC 10 calendar days prior to submitting the request to DOJ OEO, the field office must advise the operational unit immediately and note the circumstances that prevent timely notification.

(U//FOUO) Case agents must use the [redacted] b7E
[redacted]

18.7.2.11 (U) DISPUTE RESOLUTION FOR TITLE III APPLICATIONS

(U//FOUO) When there are legal questions/concerns that cannot be resolved through discussions with reviewing officials at DOJ, the responsible FBIHQ operational division supervisors or executives must forward the application to OGC for its review, advice, and recommendation.

18.7.2.12 (U) NOTICE AND REPORTING REQUIREMENTS – TITLE III

(U//FOUO) The anticipated interception of conversations related to a "Sensitive Investigative Matter" as defined in the AGG-Dom, Part VII.N, requires notice to the appropriate FBIHQ Unit Chief and Section Chief, and DOJ Criminal Division. *Note:* A sensitive investigative matter (SIM) is not the same as a sensitive circumstance described above.

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

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

ACLU EC-205

18-176

(U//FOUO) [Redacted]

(U//FOUO) [Redacted]

[Redacted]

b7E

(U//FOUO) [Redacted]

18.7.3 (U) INVESTIGATIVE METHOD: ELECTRONIC SURVEILLANCE – FISA AND FISA TITLE VII (ACQUISITION OF FOREIGN INTELLIGENCE INFORMATION)

18.7.3.1 (U) SUMMARY

(U//FOUO) ELSUR conducted pursuant to the Foreign Intelligence Surveillance Act (FISA) is a valuable investigative method. It is, also, a very intrusive means of acquiring information relevant to the effective execution of the FBI's national security and intelligence missions. To ensure that due consideration is given to the competing interests between national security and the effect on privacy and civil liberties, this section contains various administrative and management controls beyond those imposed by statute and DOJ guidelines. Unless otherwise noted, it is the responsibility of the case agent and his/her supervisor to ensure compliance with these instructions. FISA ELSUR is only authorized as an investigative method in the conduct of Full Investigations. FISA ELSUR requires: (i) administrative or judicial authorization prior to its use; (ii) contact with the field office ELSUR Technician to coordinate all necessary recordkeeping; and (iii) consultation with the Technical Advisor (TA) or a designated TTA to determine feasibility, applicability, and use of the appropriate equipment.

(U//FOUO) Application:

b7E

(U) This section is divided below into FISA (18.7.3.2) and FISA Title VII (18.7.3.3).

18.7.3.2 (U) FOREIGN INTELLIGENCE SURVEILLANCE ACT (FISA)

18.7.3.2.1 (U) LEGAL AUTHORITY

(U) 50 U.S.C. §§ 1801-1811 (FISA) and E.O. 12333 § 2.5.

(U) FISA Amendments Act of 2008 (P.L.No. 110-261).

18.7.3.2.2 (U) DEFINITION OF INVESTIGATIVE METHOD

(U) FISA is the non-consensual electronic collection of information (usually communications) under circumstances in which the parties have a reasonable expectation of privacy and court orders or warrants are required.

18.7.3.2.3 (U) STANDARDS FOR USE AND APPROVAL REQUIREMENTS FOR FISA

18.7.3.2.3.1 (U) FISA REQUEST FORM

(U//FOUO) FBIHQ and field office requests for FISC ELSUR orders must use the FISA Request Form. Field office requests for FISA orders are submitted and tracked through [redacted] b7E. The FISA request forms, in a question and answer format, have been designed to ensure that all information needed for the preparation of a FISC application is provided to FBIHQ and to the DOJ.

18.7.3.2.3.2 (U) CERTIFICATE BY THE DIRECTOR OF THE FBI

(U) Each FISA application must be accompanied by a Certification by the Director of the FBI or one of nine other individuals authorized by Congress or the President to provide such certifications that: the information being sought is foreign intelligence information; that a significant purpose of the electronic surveillance is to obtain foreign intelligence information; that such information cannot reasonably be obtained by normal investigative techniques; that the information sought is "foreign intelligence information" as defined by FISA. The certification must include a statement explaining the certifier's basis for the certification.

(U) Title 50 of the United States Code Section 1804 specifies the Assistant to the President for National Security Affairs; E.O. 12139 as amended by E.O. 13383 specifies the Director of the FBI, Deputy Director of the FBI, the Director of National Intelligence, the Principal Deputy Director of National Intelligence, the Director of the Central Intelligence Agency, the Secretary of State, the Deputy Secretary of State, the Secretary of Defense, and the Deputy Secretary of Defense as appropriate officials to make certifications required by FISA. The FBI Director has represented to Congress that the FBI Deputy Director will only certify FISA's when the FBI Director is not available to do so.

18.7.3.2.3.3 (U) EMERGENCY FISA AUTHORITY (50 U.S.C. § 1805[F])

(U) The Attorney General, on request from the Director of the FBI or his/her designee, may authorize an emergency FISA for electronic surveillance when it is reasonably determined that an emergency situation exists that precludes advance FISC review and approval and that a factual predication for the issuance of a FISA Order exists. A FISC judge must be informed by DOJ at the time of the emergency authorization and an application must be submitted to that judge as soon as is practicable but not more than seven (7) days after the emergency authority has been approved by the Attorney General. If a court order is denied after an emergency surveillance has been opened, no information gathered as a result of the surveillance may be used as evidence or disclosed in any trial or other proceeding, and no information concerning any USPER acquired from such surveillance may be used or disclosed in any manner, except with the approval of the Attorney General if the information indicates a threat of death or serious bodily harm to any person.

(U//FOUO) [Redacted]

18.7.3.2.4 (U) DURATION OF APPROVAL FOR FISA

(U//FOUO) [Redacted] b7E

18.7.3.2.5 (U//FOUO) SPECIFIC PROCEDURES FOR FISA

(U//FOUO) FISA related initiation and renewal procedures are contained within the FISA Initiation Form which can be found within [Redacted] or on the Forms section of the [NSLB library](#).

18.7.3.2.5.1 (U//FOUO) FISA VERIFICATION OF ACCURACY PROCEDURES

(U//FOUO) [Redacted]

(U//FOUO) [Redacted]

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

(U//FOUO) [Redacted]

1) (U//FOUO) [Redacted]

2) (U//FOUO) [Redacted]

3) (U//FOUO) [Redacted]

ACLU-EG-209

§18

[Redacted]

b7E

By (U//FOUO)

[Redacted]

18.7.3.2.5.2 (U) USE OF FISA DERIVED INFORMATION IN OTHER PROCEEDINGS

(U//FOUO) There are statutory (50 U.S.C. Sections 1806, 1825, and 1845) and Attorney General (AG) policy restrictions on the use of information derived from a FISA ELSUR, physical search, or PR/TT. These restrictions apply to and must be followed by anyone “who may seek to use or disclose FISA information in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States. . . .” See DIOG Appendix E for the AG Memo, Revised Policy on the Use or Disclosure of FISA Information, dated 01-10-2008. The guidance in the AG’s Memo establishes notification/approval procedures which must be strictly followed. Though not contained in the AG Memo, FBI policy requires that [Redacted]

b7E

[Redacted]

(U//FOUO) The United States must, prior to the trial, hearing, or other proceeding or at a reasonable time prior to an effort to disclose or use that information or submit it into evidence, notify the “aggrieved person” [as defined in 50 U.S.C. Sections 1801(k), 1821(2), or 1841(2)], and the court or other authority in which the information is to be disclosed or used, that the United States intends to disclose or use such information. See 50 U.S.C. Sections 1806(c), 1825(d), and 1845(c).

18.7.3.2.5.3 (U//FOUO) FISA ELECTRONIC SURVEILLANCE ADMINISTRATIVE (“FISA ELSUR”) SUB-FILE

(U//FOUO)

[Redacted]

b7E

ACLU EC-210

A) (U//FOUO) [Redacted]

B) (U//FOUO) [Redacted]

18.7.3.2.5.4 (U//FOUO) FISA REVIEW BOARD

(U//FOUO) [Redacted]

b7E

(U//FOUO) [Redacted]

(U//FOUO) [Redacted]

18.7.3.2.5.4.1 (U) [Redacted]

b7E

(U//FOUO) [Redacted]

18.7.3.2.6 (U) NOTICE AND REPORTING REQUIREMENTS FOR FISA

(U//FOUO) [Redacted]

18.7.3.2.7 (U) COMPLIANCE AND MONITORING FOR FISA

b7E

(U//FOUO) [Redacted]

§18

18.7.3.2.8 (U) SPECIAL CIRCUMSTANCES FOR FISA

(U) Under 50 U.S.C. § 1802, the President, through the Attorney General, may authorize electronic surveillance under FISA without a court order for periods of up to one year, if the Attorney General certifies in writing under oath that the surveillance will be solely directed at acquiring communications that are transmitted by means that are exclusively between or among foreign powers and there is no substantial likelihood of the surveillance acquiring the contents of communications to which USPERs are parties.

18.7.3.2.9 (U) FISA OVERCOLLECTION

(U//FOUO)

[REDACTED]

[REDACTED]

[REDACTED] Contact NSLB for further guidance regarding the handling of any FISA overcollection.

b7E

18.7.3.2.10 (U) OTHER APPLICABLE POLICIES

18.7.3.2.10.1 (U) FISA

- A) (U//FOUO) CD Policy Guide
- B) (U//FOUO) CTD Policy Guide
- C) (U//FOUO) Investigative Law Unit Library
- D) (U//FOUO) Foreign Intelligence Surveillance Act (FISA) Unit

18.7.3.3 (U) FISA TITLE VII (ACQUISITION OF FOREIGN INTELLIGENCE INFORMATION)

18.7.3.3.1 (U) SUMMARY

(U) Titles I and III of the FISA (codified as 50 U.S.C. §§ 1801, et seq.) provide the standard, traditional methods of collection against agents of foreign powers (including USPERs and non-USPERs) and foreign establishments inside the United States. Title VII of FISA, “Additional Procedures Regarding Certain Persons Outside the United States,” provides the means to target non-USPERs reasonably believed to be located outside the United States.

18.7.3.3.2 (U) LEGAL AUTHORITY

- A) (U) FISA Amendments Act of 2008 (122 Stat 2436)
- B) (U) AGG-Dom, Part V.A.13

18.7.3.3.3 (U) DEFINITION OF INVESTIGATIVE METHOD

(U) Title VII may be used for conducting FISAs on certain persons located outside the United States.

ACLU EC-212

18-184

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

(U//FOUO) See requirements under DIOG Sections 18.7.1, 18.7.2, and 18.7.3 and requirements specified above.

18.7.3.3.5 (U) DURATION OF APPROVAL

(U//FOUO) See requirements under DIOG Sections 18.7.1, 18.7.2, and 18.7.3 above.

18.7.3.3.6 (U//FOUO) SPECIFIC COLLECTION PROCEDURES FOR TITLE VII

(U) The relevant procedures (or collections) under Title VII are:

18.7.3.3.6.1 (U) SECTION 702 - PROCEDURES FOR TARGETING NON-U.S. PERSONS (NON-USPERS) WHO ARE OUTSIDE THE UNITED STATES

(U//FOUO) Under Section 702, the Government has the authority to target non-USPERS who are located outside the United States if the collection is effected with the assistance of an electronic communication service provider, as that term is defined in FISA. This section does not require a traditional FISA request. Rather, under this section, the Attorney General and the Director of National Intelligence may authorize, for periods of up to one year, the targeting of non-United States persons reasonably believed to be located outside the United States to acquire foreign intelligence information, provided they execute a Certification that is submitted to and approved by the FISC. The Certifications are accompanied by an affidavit signed by the FBI Director. In addition, the FBI is required to file "Targeting Procedures" that ensure that only non-U.S. persons (non-USPERS) reasonably believed to be located outside the United States will be targeted for collection and "to prevent the intentional acquisition of any communications as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States." Additionally, the statute prohibits targeting any person reasonably believed to be located outside the United States for the purpose of obtaining the communications of a particular, known person reasonably believed to be in the United States. Finally, the FBI is also required to follow 702-specific minimization procedures.

18.7.3.3.6.2 (U) SECTION 703 - CERTAIN ACQUISITIONS INSIDE THE UNITED STATES TARGETING UNITED STATES PERSONS OUTSIDE THE UNITED STATES

(U//FOUO) Under Section 703, the Government has the authority to target USPERS who are reasonably believed to be located outside the United States if the collection is effected with the assistance of a United States provider and if the collection occurs inside the United States. This section only authorizes electronic surveillance or the acquisition of stored electronic communications or stored electronic data that requires a court order, e.g., non-consensual collection. FISA 703 is an alternative to traditional FISA electronic surveillance (Title I) or physical search (Title III) authority when the facts meet the 703 criteria. There are two notable differences between Section 703 and traditional FISA authorities. First, although the application must identify any electronic communication

ACLU EC-213

service provider necessary to effect the acquisition, the application is not required to identify the specific facilities, places, premises, or property at which the acquisition will be directed. Second, Section 703 allows for the targeting of a USPER who is “an officer or employee of a foreign power,” even if the target is not knowingly engaging in clandestine intelligence gathering activities, sabotage, or international terrorism. To obtain authority to collect information under this section, the FBI must submit a FISA request and obtain a FISC order and secondary orders, as needed. The process to obtain that order is the same as the standard FISA process. Refer to the FISA Unit's website for further information. Section 703 also allows for emergency authorization. Unlike traditional FISA orders, however, surveillance authorized pursuant to this section must cease immediately if the target enters the United States. If the FBI wishes to continue surveillance of the USPER while he or she is in the United States, the FBI must obtain a separate court order under Title I (electronic surveillance) and/or Title III (physical search) of FISA in order to conduct electronic surveillance or a physical search of that USPER while the person is located in the United States. The use of any information collected using FISA 703 authority must comply with the applicable minimization procedures.

18.7.3.3.6.3 (U) SECTION 704 - OTHER ACQUISITIONS TARGETING UNITED STATES PERSONS OUTSIDE THE UNITED STATES

(U//FOUO) Under Section 704, the Government has the authority to target USPERs who are reasonably believed to be located outside the United States if the collection occurs outside the United States (i.e., without the assistance of a United States’ electronic communication service provider). The statute requires that the FISA court issue an order finding probable cause to believe that the USPER target is a foreign power, an agent of a foreign power, or an officer or employee of a foreign power and is reasonably believed to be located outside the United States "under circumstances in which the targeted United States person has a reasonable expectation of privacy and a warrant would be required if the acquisition were conducted in the United States for law enforcement purposes." To obtain authority to collect information under this section, the FBI must submit a FISA request and obtain a FISC order (the order will not include secondary orders). The process to obtain a FISA 704 order is similar to, but more streamlined than, that for obtaining a traditional FISA under the standard FISA process. There are two notable differences between Section 704 and traditional FISA authorities. First, the application is not required to identify the specific facilities, places, premises, or property at which the acquisition will be directed. Second, Section 704 allows for the targeting of “an officer or employee of a foreign power” even if the target is not knowingly engaging in clandestine intelligence gathering activities, sabotage, or international terrorism. Refer to the FISA Unit's intranet website for further information. Section 704 also allows for emergency authorization. Unlike traditional FISA orders, however, surveillance authorized pursuant to this section must cease if the USPER enters the United States but may be re-started if the person is again reasonably believed to be outside the United States during the authorized period of surveillance. If there is a need to continue surveillance while the target is located inside the United States a separate court order must be obtained. The use of any information collected using FISA 704 authority must comply with the applicable minimization procedures.

ACLU EC-214

(U//FOUO) [REDACTED]

b7E

18.7.3.3.6.4 (U) SECTION 705 - JOINT APPLICATIONS AND CONCURRENT AUTHORIZATIONS

(U//FOUO) Section 705(a) “joint applications” allow the FISC, upon request of the FBI, to approve a joint application targeting an USPER under both Sections 703 and 704 (authority to collect both when the person is inside and outside the United States).

(U//FOUO) Section 705(b) provides that if an order has been obtained under Section 105 (electronic surveillance under Title I of FISA) or 304 (physical search under Title III of FISA), the Attorney General may authorize the targeting of the USPER target while such person is reasonably believed to be located outside the United States. The Attorney General has this authority under E.O. 12333 § 2.5. In other words, when the FISA Court authorizes surveillance of an USPER target, the Attorney General, under Section 705(b) and E.O 12333 § 2.5, can simultaneously authorize surveillance to continue if the target travels outside the United States during the authorized period of the surveillance. According to Section 705(b), there is no need for a separate order pursuant to Section 703 or 704. During the FISA drafting process, an FBI employee should determine whether surveillance or physical search may occur for purpose of acquiring foreign intelligence while the person is reasonably believed to be outside the United States. If so, the FBI employee should consult with an OGC or DOJ-NSD attorney to ensure that appropriate language is added to the application.

(U//FOUO) [REDACTED]

18.7.3.3.6.5 (U) FISA OVERCOLLECTION

b7E

(U//FOUO) [REDACTED]

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

ACLU EC-216

Version Dated:
October 15, 2011

THE ATTORNEY GENERAL'S GUIDELINES FOR DOMESTIC FBI OPERATIONS

ACLU EC-217

Version Dated:
October 15, 2011

PREAMBLE

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

TABLE OF CONTENTS

INTRODUCTION 5

- A. FBI RESPONSIBILITIES – FEDERAL CRIMES, THREATS TO THE NATIONAL SECURITY, FOREIGN INTELLIGENCE** 6
- B. THE FBI AS AN INTELLIGENCE AGENCY** 9
- C. OVERSIGHT** 10

I. GENERAL AUTHORITIES AND PRINCIPLES 12

- A. SCOPE** 12
- B. GENERAL AUTHORITIES** 12
- C. USE OF AUTHORITIES AND METHODS** 12
- D. NATURE AND APPLICATION OF THE GUIDELINES** 14

II. INVESTIGATIONS AND INTELLIGENCE GATHERING 16

- A. ASSESSMENTS** 19
- B. PREDICATED INVESTIGATIONS** 20
- C. ENTERPRISE INVESTIGATIONS** 23

III. ASSISTANCE TO OTHER AGENCIES 25

- A. THE INTELLIGENCE COMMUNITY** 25
- B. FEDERAL AGENCIES GENERALLY** 25
- C. STATE, LOCAL, OR TRIBAL AGENCIES** 27
- D. FOREIGN AGENCIES** 27
- E. APPLICABLE STANDARDS AND PROCEDURES** 28

IV. INTELLIGENCE ANALYSIS AND PLANNING 29

- A. STRATEGIC INTELLIGENCE ANALYSIS** 29
- B. REPORTS AND ASSESSMENTS GENERALLY** 29
- C. INTELLIGENCE SYSTEMS** 29

V. AUTHORIZED METHODS 31

- A. PARTICULAR METHODS** 31
- B. SPECIAL REQUIREMENTS** 32
- C. OTHERWISE ILLEGAL ACTIVITY** 33

VI. RETENTION AND SHARING OF INFORMATION 35

- A. RETENTION OF INFORMATION** 35
- B. INFORMATION SHARING GENERALLY** 35
- C. INFORMATION RELATING TO CRIMINAL MATTERS** 36
- D. INFORMATION RELATING TO NATIONAL SECURITY AND FOREIGN INTELLIGENCE MATTERS** 37

VII. DEFINITIONS 42

II. INVESTIGATIONS AND INTELLIGENCE GATHERING

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

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

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

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

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

In the course of activities under these Guidelines, the FBI may incidentally obtain information relating to matters outside of its areas of primary investigative responsibility. For example, information relating to violations of state or local law or foreign law may be

incidentally obtained in the course of investigating federal crimes or threats to the national security or in collecting foreign intelligence. These Guidelines do not bar the acquisition of such information in the course of authorized investigative activities, the retention of such information, or its dissemination as appropriate to the responsible authorities in other agencies or jurisdictions. Part VI of these Guidelines includes specific authorizations and requirements for sharing such information with relevant agencies and officials.

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

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

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

The methods authorized in assessments are generally those of relatively low intrusiveness, such as obtaining publicly available information, checking government records,

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

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

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

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

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

A. ASSESSMENTS

1. Purposes

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

2. Approval

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

3. Authorized Activities

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

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

4. Authorized Methods

Only the following methods may be used in assessments:

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

B. PREDICATED INVESTIGATIONS

1. Purposes

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

2. Approval

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

3. Circumstances Warranting Investigation

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

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

4. Preliminary and Full Investigations

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

a. Preliminary investigations

i. Predication Required for Preliminary Investigations

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

ii. Duration of Preliminary Investigations

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

iii. Methods Allowed in Preliminary Investigations

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

b. Full Investigations

i. Predication Required for Full Investigations

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

ii. Methods Allowed in Full Investigations

All lawful methods may be used in a full investigation.

5. Notice Requirements

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

- d. The FBI shall notify the Deputy Attorney General if FBI Headquarters disapproves a field office's initiation of a predicated investigation relating to a threat to the national security on the ground that the predication for the investigation is insufficient.

C. ENTERPRISE INVESTIGATIONS

1. Definition

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

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

2. Scope

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

3. Notice and Reporting Requirements

- a. The responsible Department of Justice component for the purpose of notification and reports in enterprise investigations is the National Security Division, except that, for the purpose of notifications and reports in an enterprise investigation relating to a pattern of racketeering activity that does not involve an offense or offenses described in 18 U.S.C. 2332b(g)(5)(B), the responsible Department of Justice component is the

V. AUTHORIZED METHODS

A. PARTICULAR METHODS

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

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

other subpoenas, National Security Letters (15 U.S.C. 1681u, 1681v; 18 U.S.C. 2709; 12 U.S.C. 3414(a)(5)(A); 50 U.S.C. 436), and Foreign Intelligence Surveillance Act orders for the production of tangible things (50 U.S.C. 1861-63).

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

B. SPECIAL REQUIREMENTS

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

1. Contacts with Represented Persons

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

2. Use of Classified Investigative Technologies

Inappropriate use of classified investigative technologies may risk the compromise of such technologies. Hence, in an investigation relating to activities in violation of federal criminal law that does not concern a threat to the national security or foreign intelligence, the use of such technologies must be in conformity with the Procedures for the Use of Classified Investigative Technologies in Criminal Cases.

C. OTHERWISE ILLEGAL ACTIVITY

1. Otherwise illegal activity by an FBI agent or employee in an undercover operation relating to activity in violation of federal criminal law that does not concern a threat to the national security or foreign intelligence must be approved in conformity with the Attorney General's Guidelines on Federal Bureau of Investigation Undercover Operations. Approval of otherwise illegal activity in conformity with those guidelines is sufficient and satisfies any approval requirement that would otherwise apply under these Guidelines.
2. Otherwise illegal activity by a human source must be approved in conformity with the Attorney General's Guidelines Regarding the Use of FBI Confidential Human Sources.
3. Otherwise illegal activity by an FBI agent or employee that is not within the scope of paragraph 1. must be approved by a United States Attorney's Office or a Department of Justice Division, except that a Special Agent in Charge may authorize the following:
 - a. otherwise illegal activity that would not be a felony under federal, state, local, or tribal law;
 - b. consensual monitoring of communications, even if a crime under state, local, or tribal law;
 - c. the controlled purchase, receipt, delivery, or sale of drugs, stolen property, or other contraband;
 - d. the payment of bribes;
 - e. the making of false representations in concealment of personal identity or the true ownership of a proprietary; and
 - f. conducting a money laundering transaction or transactions involving an aggregate amount not exceeding \$1 million.

APPENDIX P: (U) ACRONYMS

A/EAD	Associate Executive Assistant Director
AD	Assistant Director
ADD	Associate Deputy Director
ADIC	Assistant Director-in-Charge
AFID	Alias False Identification
AG	Attorney General
AGG	Attorney General Guidelines
AGG-CHS	Attorney General Guidelines Regarding the Use of FBI Confidential Human Sources
AGG-Dom	Attorney General’s Guidelines for Domestic FBI Operations
AGG-UCO	The Attorney General’s Guidelines on FBI Undercover Operations
AOR	Area of Responsibility
ARS	Assessment Review Standards
ASAC	Assistant Special Agent in Charge
ASC	Assistant Section Chief
ATF	Bureau of Alcohol, Tobacco, Firearms and Explosives
AUSA	Assistant United States Attorney
CALEA	Communications Assistance for Law Enforcement Act
CCRSB	Criminal Cyber Response and Services Branch
CD	Counterintelligence Division

UNCLASSIFIED – FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

CDC	Chief Division Counsel
C.F.R.	Code of Federal Regulations
CHS	Confidential Human Source
CHSPG	Confidential Human Source Policy Implementation Guide
CIA	Central Intelligence Agency
CID	Criminal Investigative Division
CMS	Collection Management Section
CPO	Corporate Policy Office
CUORC	Criminal Undercover Operations Review Committee
CyD	Cyber Division
DAD	Deputy Assistant Director
DD	Deputy Director
DEA	Drug Enforcement Administration
DGC	Deputy General Counsel
DI	Directorate of Intelligence
DLAT	Deputy Legal Attache
DNI	Director of National Intelligence
DOD	Department of Defense
DOJ	Department of Justice
DOJ OEO	Office of Enforcement Operations, DOJ
DOS	Department of State

ACLU EC-233

UNCLASSIFIED – FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

DPO	Division Policy Officer
b7E	
EAD	Executive Assistant Director
EC	Electronic Communication
ECF	Electronic Case File
ECPA	Electronic Communication Privacy Act
ECS	Electronic Communication Service
EDA	ELSUR Data Application
EI	Enterprise Investigation
ELSUR	Electronic Surveillance
EO	Executive Order
EOT	ELSUR Operations Technician
ERS	ELSUR Records System
ESU	DOJ OEO, Electronic Surveillance Unit
ETR	Electronic Technical Request
FBIHQ	FBI Headquarters
FGJ	Federal Grand Jury
FGUSO	Field Guide for Undercover and Sensitive Operations
FICP	Foreign Intelligence Collection Program
FIG	Field Intelligence Group
FISA	Foreign Intelligence Surveillance Act

ACLU EC-234

UNCLASSIFIED – FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

FISC	Foreign Intelligence Surveillance Court
	b7E
FRCP	Federal Rules of Criminal Procedure
GC	General Counsel
HIPAA	Health Insurance Portability and Accountability Act
HSC	Homeland Security Council
ICE	Department of Homeland Security Immigration and Customs Enforcement
ICM	Investigative Case Management
IINI	Innocent Images National Initiative
ILB	Investigative Law Branch
ILU	Investigative Law Unit
IOB	Intelligence Oversight Board
IOD	International Operations Division
IP Address	Internet Protocol Address
IPG	Intelligence Policy Implementation Guide
ISP	Internet Service Provider
ITSMV	Interstate Transportation of Stolen Motor Vehicles
JDA	Juvenile Delinquency Act
JTTF	Joint Terrorism Task Force
LEGAT	Legal Attaché

ACLU EC-235

UNCLASSIFIED – FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

LHM	Letterhead Memorandum
LO	Lead Office
MAR	Monthly Administrative Report
MLAT	Mutual Legal Assistance Treaties
MOU/MOA	Memorandum of Understanding/Agreement
MSIN	Mobile Station Identification Number
MST	Mobile Surveillance Team
MST-A	Mobile Surveillance Team—Armed
NARA	National Archives and Records Administration
NCMEC	National Center for Missing and Exploited Children
NISS	National Information Sharing Strategy
NSB	National Security Branch
NSC	National Security Council
NSD	National Security Division, DOJ
NSL	National Security Letter
NSLB	National Security Law Branch
NSSE	National Special Security Events
NSUCOPG	National Security Undercover Operations Policy Implementation Guide
OCA	Office of Congressional Affairs
OCRS	Organized Crime and Racketeering Section, DOJ
OGC	Office of the General Counsel

ACLU EC-236

P-5

UNCLASSIFIED – FOR OFFICIAL USE ONLY

Version Dated:
October 15, 2011

UNCLASSIFIED – FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

OIA	Otherwise Illegal Activity
OIC	Office of Integrity and Compliance
OIO	Office of Operations, DOJ
OLC	Office of Legal Counsel, DOJ
OO	Office of Origin
OPA	Office of Public Affairs
OTD	Operational Technology Division
PBDM	Pattern Based Data Mining
PCHS	Potential CHS
PCLU	Privacy and Civil Liberties Unit
PCTDD	Post Cut-through Dialed Digits
PFI	Positive Foreign Intelligence
PG	Policy Implementation Guide
PI	Preliminary Investigation
PIA	Privacy Impact Assessment
PIAB	President's Intelligence Advisory Board
PSA	Performance Summary Assessments
PTA	Privacy Threshold Analysis
RA	Resident Agency
	b7E
RF	Radio Frequency

ACLU EC-237

UNCLASSIFIED – FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

RFPA	Right to Financial Privacy Act
RICO	Racketeer Influenced and Corrupt Organizations
RIG	Regional Intelligence Group
RMD	Records Management Division
SA	Special Agent
SAC	Special Agent-in-Charge
SC	Section Chief
SIA	Supervisory Intelligence Analyst
SIM	Sensitive Investigative Matter
SORC	Sensitive Operations Review Committee
SSA	Supervisory Special Agent
SSRA	Supervisory Senior Resident Agent
TFM	Task Force Member
TFO	Task Force Officer
TFP	Task Force Participant
TMD	Technical Management Database
TTA	Technically Trained Agent
UC	Unit Chief
UCE	Undercover Employee
UCFN	Universal Case File Number
UCO	Undercover Operation

ACLU EC-238

UNCLASSIFIED – FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

UCRC	Undercover Review Committee
UDP	Undisclosed Participation
UNI	Universal Index
USA	United States Attorney
USAO	United States Attorney's Office
U.S.C.	United States Code
USG	United States Government
USIC	United States Intelligence Community
USIC	United States Intelligence Community
USIC	United States Intelligence Community
USPER	United States Person, United States Persons, US PER, USPERs, US Person, US Persons, U.S. Person, U.S. Persons
USPS	United States Postal Service
USSS	United States Secret Service
VICAP	Violent Criminal Apprehension Program
VS	Victim Specialist services
WITT	Wireless Intercept Tracking Technology
WMD	Weapons of Mass Destruction
WMDD	Weapons of Mass Destruction Directorate

APPENDIX Q: (U) DEFINITIONS

(U//FOUO) Academic Nexus SIM: [REDACTED]

b7E

(U) Aggrieved Person: [REDACTED]

(U//FOUO) Assessments: The AGG-Dom authorizes as an investigative activity called an “Assessment” which requires an authorized purpose and articulated objective(s). The DIOG defines five types of Assessments that may be carried out to detect, obtain information about, or prevent or protect against federal crimes or threats to the national security or to collect foreign intelligence. Although “no particular factual predication” is required, the basis of an Assessment cannot be arbitrary or groundless speculation, nor can an Assessment be based solely on the exercise of First Amendment protected activities or on the race, ethnicity, national origin or religion of the subject, or a combination of only those factors.

(U//FOUO) Closed Circuit Television (CCTV): a fixed-location video camera that is typically concealed from view or that is placed on or operated by a consenting party.

(U) Consensual Monitoring: Monitoring of communications for which a court order or warrant is not legally required because of the consent of a party to the communication.

(U) Electronic Communication Service: Any service that provides to users thereof the ability to send or receive wire or electronic communications. For example, telephone companies and electronic mail companies generally act as providers of electronic communication services.

(U) Electronic Communications System: Any wire, radio, electromagnetic, photooptical or photoelectronic facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications.

(U) Electronic Storage: Any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof, or any storage of such communication by an electronic communication service for purposes of backup protection of such communication. In short, “electronic storage” refers only to temporary storage, made in the course of transmission, by a provider of an electronic communication service.

(U//FOUO) Electronic Tracking Device: [REDACTED]

b7E

ACLU EC-240

Q-1

UNCLASSIFIED – FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

(U//FOUO) Employee: For purposes of the AGG-Dom and DIOG, an “FBI employee” includes, but not limited to, an operational/administrative professional support person, intelligence analyst, special agent, task force officer (TFO), task force member (TFM), task force participant (TFP), detailee, and FBI contractor. An FBI employee is bound by the AGG-Dom and DIOG. The FBI employee definition excludes a confidential human source (CHS).

(U//FOUO) Enterprise: The term “enterprise” includes any individual, partnership, corporation, association, or other legal entity, and any union or group of individuals associated in fact although not a legal entity.

(U//FOUO) Enterprise Investigation: An Enterprise Investigation (EI) examines the structure, scope, and nature of the group or organization including: its relationship, if any, to a foreign power; the identity and relationship of its members, employees, or other persons who may be acting in furtherance of its objectives; its finances and resources; its geographical dimensions; its past and future activities and goals; and its capacity for harm. (AGG-Dom, Part II.C.2)

(U//FOUO) Enterprise Investigations are a type of Full Investigation and are subject to the same requirements that apply to Full Investigations described in Section 7. Enterprise Investigations focus on groups or organizations that may be involved in the most serious criminal or national security threats to the public, as described in Section 8. Enterprise Investigations cannot be conducted as Preliminary Investigations or Assessments, nor may they be conducted for the sole purpose of collecting foreign intelligence. [REDACTED]



b7E

(U//FOUO) Extraterritorial Guidelines: The guidelines for conducting investigative activities outside of the United States are currently contained in: (i) *The Attorney General's Guidelines for Extraterritorial FBI Operations and Criminal Investigations*; (ii) *The Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection*; and (iii) *The Attorney General Guidelines on the Development and Operation of FBI Criminal Informants and Cooperative Witnesses in Extraterritorial Jurisdictions* (collectively, the Extraterritorial Guidelines); (iv) *The Attorney General Procedure for Reporting and Use of Information Concerning Violations of Law and Authorization for Participation in Otherwise Illegal Activity in FBI Foreign Intelligence, Counterintelligence or International Terrorism Intelligence Investigations* (August 8, 1988); and (v) the *Memorandum of Understanding*

ACLU EC-241

UNCLASSIFIED – FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

Concerning Overseas and Domestic Activities of the Central Intelligence Agency and the Federal Bureau of Investigation (2005).

(U//FOUO) FISA: The Foreign Intelligence Surveillance Act of 1978, as amended. The law establishes a process for obtaining judicial approval of electronic surveillance, physical searches, pen register and trap and trace devices, and access to certain business records for the purpose of collecting foreign intelligence.

(U) For or On Behalf of a Foreign Power: The determination that activities are for or on behalf of a foreign power shall be based on consideration of the extent to which the foreign power is involved in control or policy direction; financial or material support; or leadership, assignments, or discipline.

(U) Foreign Computer Intrusion: The use or attempted use of any cyber-activity or other means, by, for, or on behalf of a foreign power to scan, probe, or gain unauthorized access into one or more United States-based computers.

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

(U) Foreign Intelligence Requirements:

- A) (U//FOUO) National intelligence requirements issued pursuant to authorization by the Director of National Intelligence, including the National Intelligence Priorities Framework and the National HUMINT Collection Directives, or any successor directives thereto;
- B) (U//FOUO) Requests to collect foreign intelligence by the President or by Intelligence Community officials designated by the President; and
- C) (U//FOUO) Directions to collect foreign intelligence by the Attorney General, the Deputy Attorney General, or an official designated by the Attorney General.

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

(U) Full Investigation: A Full Investigation may be opened if there is an “articulable factual basis” for the investigation that reasonably indicates one of the following circumstances exists:

(U) An activity constituting a federal crime or a threat to the national security has or may have occurred, is or may be occurring, or will or may occur and the investigation may obtain information relating to the activity or the involvement or role of an individual, group, or organization in such activity;

- A) (U) An individual, group, organization, entity, information, property, or activity is or may be a target of attack, victimization, acquisition, infiltration, or recruitment in connection with criminal activity in violation of federal law or a threat to the national security and the
ACLU EC-242

UNCLASSIFIED – FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

investigation may obtain information that would help to protect against such activity or threat;
or

B) (U) The investigation may obtain foreign intelligence that is responsive to a PFI requirement, as defined in DIOG Section 7.4.3.

(U) All lawful investigative methods may be used in a Full Investigation.

(U) A Full Investigation of a group or organization may be opened as an Enterprise Investigation if there is an articulable factual basis for the investigation that reasonably indicates the group or organization may have engaged, or may be engaged in, or may have or may be engaged in planning or preparation or provision of support for:

A) (U) Racketeering Activity:

1) (U) A pattern of racketeering activity as defined in 18 U.S.C. § 1961(5);

B) (U) International Terrorism:

1) (U) International terrorism, as defined in the AGG-Dom, Part VII.J, or other threat to the national security;

C) (U) Domestic Terrorism:

1) (U) Domestic terrorism as defined in 18 U.S.C. § 2331(5) involving a violation of federal criminal law;

2) (U) Furthering political or social goals wholly or in part through activities that involve force or violence and a violation of federal criminal law; or

3) (U) An offense described in 18 U.S.C. § 2332b(g)(5)(B) or 18 U.S.C. § 43.

(U) Human Source: A Confidential Human Source as defined in the Attorney General's Guidelines Regarding the Use of FBI Confidential Human Sources.

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

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

(U//FOUO) National Security Letters: an administrative demand for documents or records that can be made by the FBI during a Predicated Investigation relevant to a threat to national security. The standard for issuing an NSL, except under 15 U.S.C. § 1681v, is relevance to an authorized investigation to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a United States person (USPER) is not predicated solely on activities protected by the First Amendment of the Constitution of the United States.



b7E

ACLU EC-243

Q-4

UNCLASSIFIED – FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

b7E

(U//FOUO) Operational Division or Operational Unit: “Operational” division or operational unit as used in the DIOG means the FBIHQ division or unit responsible for management and program oversight of the file classification for the substantive investigative matter (i.e., Assessment or Predicated Investigation). Previously referred to as the FBIHQ “substantive” division or substantive unit.

(U//FOUO) Pen Register Device: Records or decodes dialing, routing addressing or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided that such information must not include the contents of any communication.

(U//FOUO) Physical Surveillance (Not Requiring a Court Order): The deliberate observation by an FBI employee of persons, places, or events, on either a limited or continuous basis, in areas where there is no reasonable expectation of privacy. Note: DIOG Section 18.5.8 makes a distinction between “casual observation” and physical surveillance, and specifies factors to be considered when determining whether a particular plan of action constitutes casual observation or physical surveillance. (See DIOG Section 18.5.8)

(U) Preliminary Investigation: A Preliminary Investigation is a type of Predicated Investigation authorized under the AGG-Dom that may be opened (predicated) on the basis of any “allegation or information” indicative of possible criminal activity or threats to the national security. Preliminary Investigations may be opened to detect, obtain information about, or prevent or protect against federal crimes or threats to the national security.

b7E

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

(U) Provider of Electronic Communication Services: Any service that provides the user thereof the ability to send or receive wire or electronic communications.

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

(U) Records: Any records, databases, files, indices, information systems, or other retained information.

(U) Relevance: Information is relevant if it tends to make a fact of consequence more or less probable.

ACLU EC-244

Q-5

UNCLASSIFIED – FOR OFFICIAL USE ONLY

Version Dated:
October 15, 2011

UNCLASSIFIED – FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

(U//FOUO) Remote Computing Services:

b7E

(U//FOUO) Sensitive Investigative Matter: An investigative matter involving a domestic public official, domestic political candidate, religious or domestic political organization or individual prominent in such an organization, or news media, or an investigative matter having academic nexus, or any other matter which, in the judgment of the official authorizing an investigation, should be brought to the attention of FBIHQ and other DOJ officials.

(U) Sensitive Monitoring Circumstance: Investigation of a member of Congress, a federal judge, a member of the Executive Branch at Executive Level IV or above, or a person who has served in such capacity within the previous two years; (Note: Executive Levels I through IV are defined in 5 U.S.C. §§ 5312-5315.)

- A) (U) Investigation of the Governor, Lieutenant Governor, or Attorney General of any state or territory, or a judge or justice of the highest court of any state or territory, concerning an offense involving bribery, conflict of interest, or extortion related to the performance of official duties;
- B) (U) A party to the communication is in the custody of the Bureau of Prisons or the United States Marshals Service or is being or has been afforded protection in the Witness Security Program; or
- C) (U) The Attorney General, the Deputy Attorney General, or an Assistant Attorney General has requested that the FBI obtain prior approval for the use of consensual monitoring in a specific investigation.

(U) Special Agent in Charge: The Special Agent in Charge of an FBI field office (including an Acting Special Agent in Charge), except that the functions authorized for Special Agents in Charge by these Guidelines may also be exercised by the Assistant Director in Charge or by any Special Agent in Charge designated by the Assistant Director in Charge in an FBI field office headed by an Assistant Director, and by FBI Headquarters officials designated by the Director of the FBI.

(U) Special Events Management: Planning and conduct of public events or activities whose character may make them attractive targets for terrorist attack.

(U) State, Local, or Tribal: Any state or territory of the United States or political subdivision thereof, the District of Columbia, or Indian tribe.

(U//FOUO) Surveillance:


- A) (U//FOUO) **Electronic surveillance (ELSUR)** - under Title III and FISA is the non-consensual electronic collection of information (usually communications) under circumstances in which the parties have a reasonable expectation of privacy and court orders or warrants are required.

b7E


ACLU EC-245

UNCLASSIFIED – FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide



B) (U//FOUO) **Consensual monitoring of communications, including consensual computer monitoring, or electronic surveillance (ELSUR)** - where there is no reasonable expectation of privacy is permitted in Predicated Investigations. These methods usually do not require court orders or warrants unless they involve an intrusion into an area where there is a reasonable expectation of privacy or non-consensual monitoring of communications, but legal review is generally required to ensure compliance with legal requirements. 



(U//FOUO) **Physical surveillance** - is the deliberate observation by an FBI employee of persons, places, or events, on either a limited or continuous basis, in areas where there may or may not be a reasonable expectation of privacy. (See DIOG Section 18.5.8 for physical surveillance in situations not requiring a court order and a discussion of the distinction between physical surveillance and casual observation). Factors to consider in determining whether observations are casual observation or physical surveillance include:  b7E



(U) **Threat to the National Security:** International terrorism; espionage and other intelligence activities, sabotage, and assassination, conducted by, for, or on behalf of foreign powers, organizations, or persons; foreign computer intrusion; and other matters determined by the Attorney General, consistent with Executive Order 12333 or a successor order.

(U//FOUO) **Trap and Trace Device:** Captures the incoming electronic or other impulses that identify the originating number or other dialing, routing, addressing or signaling information reasonably likely to identify the source of a wire or electronic communication, provided that such information does not include the contents of any communication.

(U//FOUO) **Undercover Activity:** An “undercover activity” is any investigative activity involving the use of an assumed identity by an undercover employee for an official purpose, investigative activity, or function.

(U//FOUO) **Undercover Employee:** An employee of the FBI, another federal, state, or local law enforcement agency, another entity of the United States Intelligence Community (USIC), or another foreign intelligence agency working under the direction and control of the FBI whose relationship with the FBI is concealed from third parties by the maintenance of a cover or alias identity for an official purpose, investigative activity, or function.

(U//FOUO) **Undercover Operation:** An “undercover operation” is an operation that involves a series of related “undercover activities” over a period of time by an “undercover employee.” A

ACLU EC-246

Q-7

UNCLASSIFIED – FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

series of related undercover activities consists of more than five separate substantive contacts by an undercover employee with the individuals under investigation. [REDACTED]



b7E

(U) United States: When used in a geographic sense, means all areas under the territorial sovereignty of the United States.

(U) United States Person (USPER): Any of the following, but not including any association or corporation that is a foreign power, defined as an entity that is openly acknowledged by a foreign government or governments to be directed and controlled by such foreign government or governments:

- A) (U) An individual who is a United States citizen or an alien lawfully admitted for permanent residence;
- B) (U) An unincorporated association substantially composed of individuals who are United States persons (USPERs); or
- C) (U) A corporation incorporated in the United States.

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

(U) Use: When used with respect to human sources, means obtaining information from, tasking, or otherwise operating such sources.

APPENDIX S: (U) LISTS OF INVESTIGATIVE METHODS

S.1 INVESTIGATIVE METHODS LISTED BY NAME (ALPHABETIZED)

- (U) Administrative subpoenas. (Section [18.6.4](#))
- (U) CHS use and recruitment. (Section [18.5.5](#))
- (U) Closed-circuit television/video surveillance, direction finders, and other monitoring devices. (Section [18.6.3](#))
- (U) Consensual monitoring of communications, including electronic communications. (Section [18.6.1](#))
- (U) Electronic surveillance – FISA and FISA Title VII (acquisition of foreign intelligence information). (Section [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 – only for telephone or electronic mail subscriber information in Type 1 & 2 Assessments. (Section [18.5.9](#))
- (U) Information voluntarily provided by governmental or private entities. (Section [18.5.7](#))
- (U) Intercepting the communications of a computer trespasser. (Section [18.6.2](#))
- (U) Interview or request information from the public or private entities. (Section [18.5.6](#))
- (U) Mail covers. (Section [18.6.10](#))
- (U) National Security Letters. (Section [18.6.6](#))
- (U) On-line services and resources. (Section [18.5.4](#))
- (U) Pen registers and trap/trace devices. (Section [18.6.9](#))
- (U) Physical Surveillance (not requiring a court order). (Section [18.5.8](#))
- (U) Polygraph examinations. (Section [18.6.11](#))
- (U) Public information. (Section [18.5.1](#))
- (U) Records or information - FBI and DOJ. (Section [18.5.2](#))
- (U) Records or information - Other federal, state, local, tribal, or foreign government agency. (Section [18.5.3](#))
- (U) Searches – with a warrant or court order. (Section [18.7.1](#))

ACLU EC-248

UNCLASSIFIED – FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

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

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

(U) Undercover Operations (Section 18.6.13)

S.2 INVESTIGATIVE METHODS LISTED BY ORDER IN DIOG SECTION 18

18.5.1 (U) Public information

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

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

18.5.4 (U) On-line services and resources.

18.5.5 (U) CHS use and recruitment.

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

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

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

18.5.9 (U) Grand jury subpoenas – only for telephone or electronic mail subscriber information.

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) Trash Covers (Searches that do not require a warrant or court order).

18.6.13 (U) Undercover operations.

ACLU EC-249

UNCLASSIFIED – FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

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).