

# The Federal Bureau of Investigation's Compliance with the Attorney General's Investigative Guidelines



Office of the Inspector General  
September 2005

## TABLE OF CONTENTS

TABLE OF CONTENTS .....	i
TABLE OF APPENDICES .....	vii
INDEX OF CASE STUDIES, DIAGRAMS, AND TABLES .....	ix
EXECUTIVE SUMMARY.....	1
I. Overview .....	1
II. Background .....	5
III. The Scope and Methodology of the OIG Review .....	6
IV. OIG Findings.....	7
A. The Attorney General’s Guidelines Regarding the Use of Confidential Informants .....	7
B. The Attorney General’s Guidelines on Federal Bureau of Investigation Undercover Operations .....	9
C. The Attorney General’s Guidelines on General Crimes, Racketeering Enterprise and Terrorism Enterprise Investigations.....	10
D. Procedures for Lawful, Warrantless Monitoring of Verbal Communications (Consensual Monitoring Guidelines) .....	14
E. FBI Compliance Oversight Mechanisms.....	14
F. The FBI’s Implementation Process for the Revised Guidelines.....	15
V. Recommendations .....	16
CHAPTER ONE: INTRODUCTION.....	17
I. Background .....	17
II. Scope and Methodology of the OIG Review.....	21
A. Scope of the Review.....	21
B. Methodology of the Review .....	24
III. Organization of the Report.....	25
CHAPTER TWO: HISTORICAL BACKGROUND OF THE ATTORNEY GENERAL’S INVESTIGATIVE GUIDELINES .....	29
I. Introduction.....	29

II.	The Pre-Guidelines Period .....	29
III.	Establishment of the Attorney General Guidelines.....	36
A.	The Levi Guidelines – 1976 .....	36
B.	The Civiletti Guidelines – 1980-1981.....	39
C.	The Smith Guidelines – 1983 .....	46
D.	The Thornburgh Guidelines – 1989.....	50
E.	The Reno Guidelines – 2001.....	55
IV.	Conclusion .....	59
CHAPTER THREE: THE ATTORNEY GENERAL’S GUIDELINES REGARDING THE USE OF CONFIDENTIAL INFORMANTS .....		63
I.	Role of Confidential Informants .....	63
II.	The Benefits and Risks of Using Confidential Informants in FBI Investigations .....	64
III.	Significant Requirements of the Guidelines .....	75
A.	Suitability Reviews.....	75
B.	Instructions .....	79
C.	Authority to Engage in Otherwise Illegal Activity (OIA).....	80
D.	Unauthorized Illegal Activity (UIA) .....	82
E.	Deactivation of Confidential Informants .....	88
IV.	Major Revisions to the Guidelines .....	89
V.	The OIG Review of the FBI’s Compliance with the Confidential Informant Guidelines .....	90
VI.	Compliance Findings .....	93
A.	Initial and Continuing Suitability Reviews.....	96
B.	Instructions .....	98
C.	Authority to Engage in Otherwise Illegal Activity (OIA).....	103
D.	Unauthorized Illegal Activity (UIA) .....	108
E.	Deactivation of Confidential Informants .....	109
F.	Seeking Approval or Concurrence from, and Providing Notification to, the United States Attorney’s Office.....	109
VII.	OIG Analysis.....	112
VIII.	Recommendations .....	133

CHAPTER FOUR: THE ATTORNEY GENERAL'S GUIDELINES ON FBI UNDERCOVER OPERATIONS .....	137
I. Role of FBI Undercover Operations .....	137
A. The Need for Undercover Operations .....	137
B. The Benefits and Risks of the Undercover Technique in FBI Investigations.....	140
II. Significant Requirements of the Undercover Guidelines .....	144
A. Group I Undercover Operations.....	145
B. Group II Undercover Operations.....	148
III. Major Revisions to the Guidelines.....	148
IV. The OIG Review of the FBI's Compliance with the Undercover Guidelines.....	150
V. Compliance Findings.....	151
VI. OIG Analysis .....	156
VII. OIG Recommendations.....	164
CHAPTER FIVE: ATTORNEY GENERAL'S GUIDELINES ON GENERAL CRIMES, RACKETEERING ENTERPRISE AND TERRORISM ENTERPRISE INVESTIGATIONS.....	169
I. Levels of Investigative Activities .....	169
II. Preliminary Inquiries.....	170
A. Significant Requirements .....	170
B. Major Revisions to the Guidelines.....	171
C. The OIG Review of Preliminary Inquiries.....	172
D. Compliance Findings.....	172
E. OIG Analysis and Recommendations .....	173
III. General Crimes Investigations .....	174
A. Role of General Crimes Investigations.....	174
B. Significant Requirements .....	175
C. Major Revisions to the Guidelines.....	175
D. The OIG Review of General Crimes Investigations .....	176
E. Compliance Findings.....	176
F. OIG Analysis and Recommendations .....	178
IV. Criminal Intelligence Investigations .....	178
A. Role of Criminal Intelligence Investigations.....	178
B. Significant Requirements .....	179

C.	Major Revisions to the Guidelines .....	181
D.	The OIG Review of Criminal Intelligence Investigations.....	181
E.	Compliance Findings .....	182
F.	OIG Analysis and Recommendations.....	186
V.	Part VI of the General Crimes Guidelines: Counterterrorism Activities and Other Authorizations.....	188
A.	Rationale for the New Part VI Authorities .....	188
B.	New Authorities Added to the General Crimes Guidelines.....	190
C.	The OIG Review of the FBI's Use of Part VI Authorities .....	191
D.	Compliance Findings .....	192
1.	The FBI's Use of Part VI Authorities Since May 30, 2002, and the FBI's Implementing Guidance.....	192
2.	Internal Controls Regarding Predication for the Exercise of Part VI.A.2 Authorities .....	196
3.	Internal Controls for Record Retention Relating to the Exercise of Part VI.A.2 Authorities .....	200
E.	OIG Analysis and Recommendations.....	202
CHAPTER SIX: PROCEDURES FOR LAWFUL, WARRANTLESS MONITORING OF VERBAL COMMUNICATIONS (CONSENSUAL MONITORING) .....		207
I.	Role of Consensual Monitoring.....	207
II.	Significant Requirements .....	208
III.	Major Revisions to the Consensual Monitoring Guidelines.....	210
IV.	The OIG Review of the FBI's Compliance with the Consensual Monitoring Guidelines.....	211
V.	Compliance Findings .....	212
VI.	OIG Analysis and Recommendations.....	215
CHAPTER SEVEN: FBI AND DOJ COMPLIANCE OVERSIGHT AND ENFORCEMENT MECHANISMS.....		217
I.	FBI-DOJ Committees that Approve and Monitor Certain Undercover Operations and Confidential Informants .....	217
A.	Criminal Undercover Operations Review Committee (CUORC).....	217
1.	The CUORC Review Process.....	219
2.	The CUORC's Activities from October 2003 to March 2005.....	221
3.	FBI Undercover Coordinator Survey Responses.....	223

4.	OIG Analysis and Recommendations .....	224
B.	Confidential Informant Review Committee (CIRC) .....	225
1.	The CIRC Review Process .....	227
2.	The CIRC's Activities from August 2003 to April 2005 .....	228
3.	OIG Survey of Confidential Informant Coordinators Regarding the CIRC.....	232
C.	OIG Analysis and Recommendations .....	233
II.	Inspection Division.....	235
A.	Background on the Inspection Function .....	236
1.	Organization of the Inspection Division .....	236
2.	How Inspections Are Conducted.....	237
3.	What is Inspected .....	241
B.	Changes in the Inspections Process After the May 2002 Revisions of the Attorney General Guidelines.....	247
C.	Inspection Division Findings Regarding Attorney General Guidelines Compliance.....	247
1.	Criminal Informant Program .....	248
2.	Inspection Division Audits of Undercover Operations and Consensual Monitoring .....	257
3.	General Crimes, REIs, and TEIs .....	257
D.	OIG Analysis .....	258
1.	Scope of On-site Inspections .....	258
2.	Promoting Accountability .....	262
3.	The Timing of Inspections and Better Use of Technology.....	263
E.	Recommendations.....	265
III.	On-site Reviews by Program Offices .....	266
A.	Undercover & Sensitive Operations Unit On-site Reviews .....	266
B.	Asset/Informant Unit Reinspections.....	267
C.	OIG Analysis and Recommendations .....	270
IV.	FBI Disciplinary Process.....	271
A.	Investigative Guidelines Issues Addressed by the FBI Disciplinary Process .....	273
1.	Classification of Offenses .....	273
2.	Investigative Guidelines Violations Adjudicated by OPR from 1999 to 2004 .....	274
B.	OIG Analysis .....	274
1.	Standards for Referral to the FBI Disciplinary Process.....	275
2.	Additional Offense Codes .....	276
3.	Technology and Information Dissemination.....	277
C.	Recommendations.....	278

CHAPTER EIGHT: HOW THE FBI IMPLEMENTED THE MAY 30, 2002, REVISIONS TO THE ATTORNEY GENERAL'S INVESTIGATIVE GUIDELINES .....	279
I. The FBI's Implementation Process for the Revised Investigative Guidelines .....	279
A. Planning for Implementation.....	279
B. Communication and Guidance.....	280
C. Training.....	282
D. Administrative Support, Including Mechanisms to Promote Accountability.....	288
II. OIG Analysis and Recommendations .....	292
CHAPTER NINE: CONCLUSION .....	297

## **TABLE OF APPENDICES**

Appendix A	Organization Charts: <ul style="list-style-type: none"><li>• Department of Justice</li><li>• Federal Bureau of Investigation</li></ul>
Appendix B	The Attorney General's Investigative Guidelines issued May 30, 2002 <ul style="list-style-type: none"><li>• The Attorney General's Guidelines Regarding the Use of Confidential Informants</li><li>• The Attorney General's Guidelines on Federal Bureau of Investigation Undercover Operations</li><li>• The Attorney General's Guidelines on General Crimes, Racketeering Enterprise and Terrorism Enterprise Investigations</li><li>• Memorandum Regarding Procedures for Lawful, Warrantless Monitoring of Verbal Communications</li></ul>
Appendix C	Table of Revisions to the Attorney General's Investigative Guidelines of May 30, 2002
Appendix D	USAO Criminal Division Chiefs' Views on Adequacy of FBI Coordination on Confidential Informant Guidelines Issues
Appendix E	Department of Justice Office of the Inspector General's Recommendations
Appendix F	Discrepancies Between the Attorney General's Investigative Guidelines and FBI Policy Manuals
Appendix G	FBI Response to OIG Recommendations
Appendix H	OIG Analysis of the FBI Response to OIG Recommendations
Appendix I	List of Acronyms



[BLANK PAGE]

## **INDEX OF CASE STUDIES, DIAGRAMS, AND TABLES**

	Page
Case Study 1	71
FBI Informants James J. “Whitey” Bulger and Stephen J. “The Rifleman” Flemmi	
Case Study 2	85
FBI Informant Gregory Scarpa, Sr. and his FBI Handler, R. Lindley DeVecchio	
Case Study 4.1	139
Operation Greylord	
Case Study 4.2	143
Operation “Lighting Strike”	
Case Study 7.1	246
FBI Inspection Division Audit of a Field Division’s Criminal Informant Program	
Case Study 7.2	252
The San Francisco Criminal Informant Program	
Diagram 3.1	102
Confidential Informant Coordinators’ Views on Field Office Compliance with CI Guidelines Requirement to Give Instructions to Confidential Informants	
Diagram 3.2	104
Confidential Informant Coordinators’ Views on Field Office Compliance with CI Guidelines Requirements Relating to Authorization to Engage in “Otherwise Illegal Activities”	
Diagram 3.3	114
The Three Issues Most Frequently Raised by Special Agents Regarding the Confidential Informant Guidelines According to Confidential Informant Coordinators	
Diagram 3.4	125
Confidential Informant Coordinators’ Views on Need for Training	
Diagram 4.1	159
Undercover Coordinators’ Views on Their Duties	
Diagram 4.2	160
Division Counsel’s Views on Frequency of Field Agents’ Consultation on Select Issues Concerning Undercover Operations	
Diagram 5.1	202
Division Counsel’s Views on Consultation Regarding Part VI.A.2 Authorities of the General Crimes Guidelines and Clarity of Related FBI Guidance	
Diagram 7.1	224
Undercover Coordinators’ Views on the Effectiveness of CUORC Oversight of Undercover Operations	

Diagram 7.2	Confidential Informant Coordinators' Views on the Effectiveness of CIRC Oversight of Confidential Informants	232
Diagram 7.3	Organization of the Inspection Division	236
Diagram 7.4	Organization Chart: FBI Disciplinary Units	272
Diagram 8.1	Division Counsel Reporting of Special Agents who have Received Training on the Investigative Guidelines in Their Field Offices as of March 2004	284
Diagram 8.2	Division Counsel's Views on the Need for Investigative Guidelines Training	285
Diagram 8.3	Confidential Informant Coordinators' Views on the Need for Investigative Guidelines Training	286
Diagram 8.4	Effectiveness of Training of Confidential Informant Coordinators and Undercover Coordinators on the Investigative Guidelines	287
Diagram 8.5	Division Counsel's Views of the Effectiveness of Their Training on the Investigative Guidelines	288
Table 3.1	OIG Findings on Confidential Informant Guidelines Compliance Deficiencies in Select FBI Field Offices	94
Table 3.2	Compliance with Confidential Informant Guidelines Instruction Requirements in Select FBI Field Offices	100
Table 3.3	Timeliness of Instructions Given to Confidential Informants in Select FBI Field Offices	101
Table 3.4	Compliance Deficiencies Involving FBI Authorization of Otherwise Illegal Activity in Select FBI Field Offices	107
Table 3.5	Training and Other Measures Proposed by USAO Criminal Division Criminal Chiefs to Promote Adherence to the Confidential Informant Guidelines	111
Table 3.6	Views of 12 FBI Senior Field Managers on the Confidential Informant Guidelines	115
Table 3.7	Suitability Elements Missing from Initial Suitability Reports & Recommendations (ISR&Rs) in Select FBI Field Offices	118
Table 3.8	Division Counsel's Views on Need for Training on Confidential Informant Guidelines	126

Table 4.1	OIG Compliance Findings from 83 Group I and Group II Undercover Operations in Select Field Offices	155
Table 5.1	OIG Compliance Findings from 46 Preliminary Inquiries in Select FBI Field Offices	173
Table 5.2	Documentation of Racketeering Enterprise Investigation Predication and Field Office Notifications to DOJ, USAOs, and FBIHQ	184
Table 5.3	Division Counsel's Views on Consultation Regarding Part VI Authorities of the General Crimes Guidelines	194
Table 6.1	OIG Compliance Findings on Consensual Monitorings Conducted Without Written Authorization in Select FBI Field Offices	213
Table 7.1	Group I Undercover Operations Approved During FY 2003	219
Table 7.2	Audits Conducted During Inspection Division On-Site Inspections	242
Table 7.3	Percentage of Criminal Informant Program Files with Compliance Deficiencies Identified by the Inspection Division (May 2002 – October 2004)	249
Table 7.4	Inspection Division Deficiency Data for Criminal Informant Program in Select Field Offices	250
Table 7.5	Types of Confidential Informant Guidelines Violations Identified by the Inspection Division (May 2002 – October 2004)	256
Table 7.6	Comparison of Deficiency Measures for Select FBI Field Office Criminal Informant Programs	261
Table 7.7	Inspection and Reinspection Non-compliance Rates for Select Criminal Informant Programs	268

[BLANK PAGE]

## **EXECUTIVE SUMMARY\***

### **I. Overview**

After the September 11, 2001, terrorist attacks, the Department of Justice (DOJ or Department) initiated a comprehensive review of four sets of the Attorney General's Investigative Guidelines (Guidelines or Investigative Guidelines) that govern most aspects of the Federal Bureau of Investigation's (FBI) authority to investigate crimes committed by individual criminals, criminal enterprises and groups, as well as those who may be threatening to commit crimes. The purpose of the review was to identify changes to the Guidelines that would enhance the Department's ability to detect and prevent terrorist attacks. The four Guidelines are:

- The Attorney General's Guidelines Regarding the Use of Confidential Informants (Confidential Informant Guidelines);
- The Attorney General's Guidelines on Federal Bureau of Investigation Undercover Operations (Undercover Guidelines);
- The Attorney General's Guidelines on General Crimes, Racketeering Enterprise and Terrorism Enterprise Investigations (General Crimes Guidelines); and
- Procedures for Lawful, Warrantless Monitoring of Verbal Communications (Consensual Monitoring Guidelines).

On May 30, 2002, the Attorney General approved revisions to each of these Guidelines.

The Department of Justice Office of the Inspector General (OIG) conducted this review of the FBI's implementation of the revised Investigative Guidelines with two main objectives: 1) to assess the FBI's compliance with the revised Guidelines; and 2) to evaluate the procedures that the FBI employed to ensure that the revised Guidelines were properly implemented.

Our review was conducted in five phases. The first phase consisted of background interviews of key program managers at FBI Headquarters and an extensive document review. The second phase consisted of interviews of FBI Headquarters and DOJ personnel who oversee critical aspects of the substantive programs governed by the Guidelines. In the third phase, we surveyed three groups of Special Agents in the FBI's 56 field offices who

---

\* The full version of this report includes a limited amount of information that the Federal Bureau of Investigation (FBI) considered to be law enforcement sensitive and therefore could not be publicly released. To create this public version of the report, the OIG redacted (deleted) the portions of the full report that were considered sensitive by the FBI, and we indicated where those redactions were made.

played key roles in promoting adherence to the Guidelines: Confidential Informant Coordinators; Undercover Coordinators; and Division Counsel, who serve as chief legal advisers in the field offices. We also conducted another survey of the Criminal Division Chiefs of the 93 U.S. Attorneys' Offices. That survey focused on the Guidelines' provisions requiring approval, concurrence, or notification to U.S. Attorneys' Offices relating to significant Guidelines-related authorities.

The fourth phase of our review consisted of 12 FBI field office site visits during which we reviewed a judgmental sample of FBI investigative and administrative files reflecting use of the authorities or operational techniques authorized by the Guidelines. In that sample of files, we also reviewed the various forms and other administrative paperwork supporting the activities governed by the Guidelines.<sup>1</sup> Following our field office visits, we interviewed the senior manager of each of those field offices – either the Assistant Directors in Charge or Special Agents in Charge (SACs).<sup>2</sup>

During the fifth phase of the review, after analyzing the data from FBI Headquarters and the 12 field offices and the other documents produced by the FBI and the DOJ, including more than 40 triennial FBI Inspection Reports generated by the FBI's Inspection Division, we interviewed several senior FBI officials in Headquarters about organizational and other plans that could affect Headquarters and field supervision of the authorities governed by the Guidelines. We also interviewed the FBI Director in April 2005.

We now summarize some of the key findings regarding each set of the Guidelines which we explain in greater detail later in this Executive Summary.

We found that the FBI's compliance with each of the four Investigative Guidelines differed considerably by Guideline and field office. The most significant problems were failures to comply with the Confidential Informant Guidelines. For example, we identified one or more Guidelines violations in 87 percent of the confidential informant files we examined. By contrast, we found approximately 90 percent of the undercover operations and consensual monitoring files we reviewed contained no authorization-related Guidelines deficiencies.

---

<sup>1</sup> We included in our field office site visits six of the largest FBI field offices: New York, Washington, D.C., Los Angeles, Chicago, Miami, and Boston; four medium-sized field offices: Denver, Salt Lake City, Portland, and Buffalo; and two of the smaller field offices: Columbia, S.C., and Memphis.

<sup>2</sup> The senior field managers of the FBI's larger field offices are designated Assistant Directors in Charge. However, for convenience, throughout this report we refer collectively to the senior field managers as SACs.

**Confidential Informant Guidelines.** Our review found that FBI Headquarters has not adequately supported the FBI's Criminal Informant Program, which has hindered FBI agents in complying with the Confidential Informant Guidelines. Although we noted some improvements in this area during the course of our review, in many instances agents lacked access to basic administrative resources and guidance that would have promoted compliance with the Confidential Informant Guidelines. For example, the FBI did not have a field guide or standardized and up-to-date forms and compliance checklists. The FBI also did not plan for, or provide, adequate training of agents, supervisors, and Confidential Informant Coordinators on informant policies and practices.

**Undercover Operations Guidelines.** We found that the FBI generally was compliant with the Undercover Guidelines and that the Headquarters unit supporting undercover operations was well managed and effective. That unit generates an up-to-date field guide and standardized forms, and it uses technology, such as a centralized database which permits effective monitoring of undercover operations, to aid field office compliance with the Undercover Guidelines and Headquarters oversight of the Guidelines.

**General Crimes Guidelines.** We found that the FBI generally adhered to the provisions of the General Crimes Guidelines. For example, 71 of the 72 files we reviewed identified appropriate predication in the case opening memorandum and, when disseminating information regarding these investigations to other law enforcement agencies, the FBI consistently documented an adequate basis to do so, in conformity with the Guidelines. However, the FBI has not developed adequate controls to ensure that notifications to U.S. Attorneys, DOJ, and FBI Headquarters are made on a timely basis and documented in the case files, that authorizations for the extension and renewal of preliminary inquiries and for the conversion of preliminary inquiries to full investigations are documented, that SAC reviews of criminal intelligence investigations are documented, and that progress reports to DOJ on terrorism enterprise investigations lasting for more than 180 days are included in the files.

We also reviewed the FBI's new authorities in Part VI of the General Crimes Guidelines, which allow FBI agents to visit public places and attend public events to detect or prevent terrorist activities in the absence of any particularized evidence that a crime has occurred or is likely to occur. We found that the FBI encourages but does not require agents to obtain supervisory approval prior to visiting public places or attending public events. Moreover, neither FBI field offices nor Headquarters consistently maintains records regarding the use of and compliance with these authorities, including the provisions that address the FBI's authority to collect, maintain, and disseminate information obtained at such events, and provisions forbidding retention of certain information. Without access to data reflecting approval or documentation of such visits, we were unable to



draw conclusions about the FBI's utilization of these authorities or its record of compliance with Part VI authorities.

**Consensual Monitoring Guidelines.** The Attorney General Guidelines governing consensual monitoring cover non-telephonic consensual monitorings, which include the use of body recorders and transmitting devices. We found that the FBI was generally in compliance with the Consensual Monitoring Guidelines, although we identified deficiencies, particularly with regard to the Guidelines' requirements for supervisory authorization.

**FBI Oversight of Compliance with Attorney General Guidelines.** The FBI and DOJ have various mechanisms to promote compliance with each of the Investigative Guidelines, including first-line field supervisors; the expertise of field office Confidential Informant Coordinators, Undercover Coordinators, and Division Counsel; two joint FBI-DOJ committees (the Criminal Undercover Operations Review Committee (CUORC) and the Confidential Informant Review Committee (CIRC)) which approve certain undercover operations and confidential informants; the FBI's Inspection Division; the employee disciplinary process; and various policy manuals.

We found that the joint review committees were operating effectively and in accordance with assigned missions. However, we found that field supervisors frequently were not held accountable for compliance violations, particularly in the Criminal Informant Program, and that the FBI at times failed to ensure that FBI personnel with special expertise and responsibility for issues addressed in the Guidelines, such as Informant Coordinators, Undercover Coordinators, and Division Counsel, were properly consulted regarding investigative activities. Our review also found that the Inspection Division's triennial audits were useful in promoting compliance, but were not sufficiently comprehensive and did not adequately address the underlying causes of Guidelines violations.

**Implementation of the Guidelines.** The process adopted by the FBI to implement the revised Guidelines was not optimal. Although several FBI components performed these duties well – particularly the Office of the General Counsel and the Undercover and Sensitive Operations Unit (USOU) within the Criminal Investigative Division (CID) – we found inadequate inter-division planning, coordination and direction. This hindered provision of necessary training for FBI employees on the revised Guidelines and also resulted in the failure to timely update standardized forms, inspection checklists, and other technical support. In addition, the lack of adequate case management and other information technology tools hindered the FBI's ability to identify, track, and evaluate its compliance with the Guidelines.

In the next section of this Executive Summary, we summarize in greater detail the contents of the report, including the background of the revised Guidelines, the scope and methodology of our review, our findings

and conclusions regarding the FBI's compliance with each of the four Investigative Guidelines, the oversight mechanisms used to promote Guidelines compliance, the implementation process, and our recommendations to address the issues identified in the report.<sup>3</sup>

## **II. Background**

The four Investigative Guidelines govern the FBI's use of general crimes investigations to develop evidence about the commission of federal crimes and the FBI's use of criminal intelligence investigations to develop evidence about the nature, size, and composition of ongoing criminal enterprises where the objective may not necessarily be to prosecute but to determine whether a pattern of criminal activity exists. The Investigative Guidelines also constrain the FBI's use of three key techniques used to conduct general crimes and criminal intelligence investigations: the use of confidential informants, undercover operations, and non-telephonic consensual monitoring of verbal communications.

The first Attorney General Investigative Guidelines were issued in 1976 by Attorney General Edward Levi following congressional hearings and published reports criticizing the FBI's domestic surveillance activities in the 1950s and 1960s that targeted protest groups and others. Since then, the Guidelines have been revised by virtually every Attorney General, often after allegations of abuse by the FBI in the use of the authorities permitted by the Guidelines.

The Investigative Guidelines apply to the FBI and in some cases other Justice Law Enforcement Agencies (JLEAs) or components of the United States Government.<sup>4</sup> The Guidelines set forth detailed procedures and review mechanisms to ensure that law enforcement authorities are exercised appropriately and with adequate oversight, both in the field and, with respect to certain authorities or sensitive investigations, at FBI Headquarters and DOJ. For example, the Guidelines require that before

---

<sup>3</sup> Individual recommendations are provided at the end of Chapters Three through Eight of the report. A complete list of recommendations is provided in Appendix E.

<sup>4</sup> In addition to the FBI, the JLEAs bound by the Confidential Informant Guidelines are the Drug Enforcement Administration (DEA), United States Marshals Service, and the Department of Justice Office of the Inspector General. The Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) became a Department of Justice Law Enforcement Agency (JLEA) effective in January 2003 and therefore is subject to the Attorney General's Guidelines Regarding the Use of Confidential Informants. ATF told the OIG that it is adapting its orders concerning the use of confidential informants and the conduct of undercover operations orders to conform fully with the Attorney General's Guidelines and anticipates that it will soon be forwarding draft Orders on these subjects to the Criminal Division for review. The General Crimes and Undercover Guidelines apply only to the FBI. The Consensual Monitoring Guidelines apply to all Executive Branch departments and agencies.

FBI agents employ certain intrusive investigative techniques, sufficient evidentiary predication must be established. The Guidelines also require agents to ensure that confidential informants working for the FBI are suitable and understand the limits on their activities, including their authority to engage in actions that would be illegal if engaged in by someone without such authority; that undercover operations used to develop evidence to prosecute white collar crimes, public corruption, terrorism, and other crimes are approved only after a thorough review of the risks and benefits of the operation; and that before the FBI intercepts and monitors oral non-telephonic communications without the consent of all parties, there is careful review of the reasons for the monitoring, the duration of the monitoring, the location of the monitoring, and the nature of any danger to the party consenting to the monitoring.

### **III. The Scope and Methodology of the OIG Review**

The OIG review was conducted by a team of attorneys, inspectors, auditors, and paralegals. The OIG team conducted interviews of over 70 officials and employees at FBI Headquarters, typically Unit Chiefs, Section Chiefs, and Assistant Directors. We attended dozens of meetings of the CIRC and the CUORC. We also examined over 2,000 FBI documents from FBI Headquarters' operating and support divisions. Among the documents we analyzed were investigative case files, Headquarters guidance memoranda, correspondence, and reports by the FBI's Inspection Division, Undercover and Sensitive Operations Unit (USOU), and the FBI Office of Professional Responsibility (OPR).

In addition, the OIG surveyed four groups within the FBI and DOJ who work with the Guidelines on a daily basis. We surveyed the FBI's Confidential Informant Coordinators, its Undercover Coordinators, and its Division Counsel, all of whom work in the 56 FBI field offices around the country. In addition, because U.S. Attorneys' Offices have responsibility for approving or concurring in certain authorities in the Guidelines, or are required to be notified of certain activities or developments, we also surveyed the Chiefs of the Criminal Division of the 93 U.S. Attorneys' Offices.

After receiving the survey results, we visited FBI field offices from May through August 2004. OIG teams traveled to 12 FBI field offices to conduct interviews and examine a judgmental sample of nearly 400 administrative and investigative files pertaining to investigations governed by the revised Investigative Guidelines during the period May 30, 2002, to May 30, 2004. We examined this sample of individual investigative and administrative files to determine whether key provisions of the Investigative Guidelines were followed.

In addition to our review of case files, we assessed the steps the FBI took to implement the revised Guidelines. In this portion of our review, we assessed the FBI's planning, communication, guidance, and training for

implementation of the revised Guidelines. We also evaluated the FBI's mechanisms to ensure compliance, including the role of Supervisory Special Agents and senior managers in FBI field offices, the FBI's Inspection Division, on-site reviews conducted by units within FBI Headquarters' operating divisions, and the FBI disciplinary process.

Toward the end of our review, we conducted interviews of the SACs of the 12 field offices we visited. We also interviewed three FBI Executive Assistant Directors and the FBI Director.

#### **IV. OIG Findings**

##### **A. The Attorney General's Guidelines Regarding the Use of Confidential Informants**

The Attorney General's Guidelines on Confidential Informants are designed to ensure that proposed confidential informants undergo thorough scrutiny for suitability before they are approved and periodically thereafter; are warned about the limits on their authority by means of instructions that must be administered at least annually; and are authorized to engage in otherwise illegal activities that are justified in unusual circumstances only after such activities are carefully defined and their scope is approved by responsible DOJ and FBI personnel. The Guidelines also provide that when an informant engages in unauthorized illegal activity, it is promptly reported to FBI Headquarters and the appropriate prosecutor. They also require that if an informant is deactivated, whether for "cause" or other reasons, the deactivation is properly recorded, the confidential informant and appropriate FBI and DOJ personnel are notified, and any authority to engage in otherwise illegal activity is revoked.

We found significant problems in the FBI's compliance with Guidelines' provisions. Those violations occurred mainly in suitability reviews; the cautioning of informants about the limits of their activities; the authorization of otherwise illegal activity; documentation and notice of unauthorized illegal activity by informants; and the deactivation of informants. In total, we found one or more Guidelines compliance errors in 87 percent of the informant files we examined.<sup>5</sup>

---

<sup>5</sup> As explained later in this report, we selected a judgmental sample of 120 confidential informant files subject to the May 2002 Guidelines from 12 of the FBI's largest, medium-sized, and smaller field offices. We randomly chose between 9 and 11 of the pertinent files to examine in each field office, except in offices where there were only a small number of files within a certain category of informants, in which case we reviewed all files. We did not pre-select CI files that had been identified as non-compliant by internal FBI inspections or other internal compliance mechanisms, nor did we base our selection of field offices on the compliance record of those field offices or on any other criteria that would produce a bias or skewing of the judgmental sample.

(continued)

These compliance errors are troubling in light of the history of the Confidential Informant Guidelines. As a result of a 2-year review after high-profile problems in the FBI informant program came to light in the 1990s, Attorney General Reno issued revised Confidential Informant Guidelines in January 2001 that made the approval process for opening and operating informants more rigorous. Attorney General Ashcroft issued further revisions to the Guidelines in May 2002, but left the provisions regarding opening and operating informants essentially unchanged. Yet, when we examined informant files in May 2004 and surveyed FBI field personnel, we found that serious compliance deficiencies still existed with regard to the approval, monitoring, documentation, and notification provisions of the Guidelines.

Throughout our review, we were told by field office and FBI Headquarters personnel that the Confidential Informant Guidelines are cumbersome and the supporting paperwork requirements are onerous, and that these factors combine to discourage agents from developing informants or to use sources who are not formally registered in the informant program. A majority of the SACs in the 12 field offices we visited told us that they believe the Confidential Informant Guidelines are workable and well understood, but that the associated paperwork is too cumbersome.

We found serious shortcomings in the supervision and administration of the Criminal Informant Program. The FBI's Criminal Informant Program lacks adequate administrative and technological support from Headquarters and certain field offices. For example, the FBI has not provided standardized, automated forms to field agents to support their applications for informant-related authorities or a standard field guide describing the requirements to operate confidential informants. In addition, the FBI has provided insufficient training and administrative support to field supervisors and Confidential Informant Coordinators, and does not develop timely compliance data for field managers or FBI Headquarters.<sup>6</sup>

---

As is the case, however, with any judgmental sample, one cannot extrapolate with statistical certainty that the non-compliance rate of the entire population of FBI confidential informant files would be identical to the non-compliance rate we found in our sample.

<sup>6</sup> As noted in the FBI's response to the OIG's recommendations (provided in Appendix G), the FBI states that the Directorate of Intelligence (DI) has initiated a "re-engineering" of its Confidential Human Source Program. Because its internal human source policies, practices, and manuals must account for and comply with the Attorney General's Guidelines, the FBI enlisted DOJ to assist in the re-engineering effort. In December 2004, the FBI established a working group, including representatives from DOJ, to revise FBI policies regarding human sources (including confidential informants.) The working group's goals are to develop new guidelines, policies, and processes for the utilization of confidential human sources that are designed to reduce burdensome paperwork, standardize source administration procedures, clarify compliance requirements, and improve Guidelines compliance.

In November 2004, several months after the OIG's field office visits ended, the Criminal Investigative Division (CID) at FBI Headquarters generated a self-assessment in analyzing the field office-level compliance deficiencies regarding the Confidential Informant Guidelines identified in the course of our review. CID concluded that field agents still were not familiar with the Guidelines' requirements two years after their implementation, executive managers did not exercise effective oversight, FBI case agents and supervisors did not recognize the implications of some of the most serious Guidelines violations, the FBI had not generated basic administrative tools using existing technology and resources to support operation of the program, and the FBI's basic database tools were so archaic that they seriously limited the ability of field office and Headquarters personnel to support Guidelines compliance. The fact that CID's critique found some of the same problems we did underscores the need for decisive action to remedy the systemic problems we found in the Criminal Informant Program.

## **B. The Attorney General's Guidelines on Federal Bureau of Investigation Undercover Operations**

Our findings regarding the Criminal Informant Program are in contrast to our generally favorable findings regarding the FBI's compliance with the Attorney General's Guidelines on FBI Undercover Operations. FBI undercover operations, while more limited in scope than the Criminal Informant Program, entail similar Headquarters and field supervision challenges, operational risks, and administrative support needs. But with a few important exceptions, we found the FBI compliant with the Undercover Guidelines.

For example, we found that the CID's Operational Support Section and USOU were supporting and monitoring undercover operations in field offices and were using technological support and other guidance materials to achieve its objectives. Undercover Coordinators, Division Counsel, and other agents experienced with undercover techniques also assisted with ensuring compliance with the Undercover Guidelines.

In contrast to the 87 percent rate of Guidelines' violations in confidential informant files, our judgmental sample of undercover files in 12 field offices found Undercover Guidelines violations in 12 percent of the files that we examined. These violations concerned the failure to obtain proper authorization for particular undercover activities. Sixty percent of these violations reflected errors relating to field office-approved undercover operations that continued beyond their expiration date or operations in which the FBI participated in a task force that was using undercover techniques. In addition to these authorization violations, 20 percent of the files contained documentation-related errors related to the FBI's Undercover Guidelines compliance responsibilities. These omissions included the failure to document field management reviews of undercover employee

conduct, adequately describe “otherwise illegal activity,” and include a supporting letter from the U.S. Attorney’s Office which made the five required findings. We believe that the majority of these compliance deficiencies likely would have been avoided if the FBI had procedures in place that ensured greater consultation between agents and Undercover Coordinators and Division Counsel. Yet, while not insignificant, we do not believe that these violations reflect the fundamental deficiencies that we encountered in the Criminal Informant Program.

### **C. The Attorney General’s Guidelines on General Crimes, Racketeering Enterprise and Terrorism Enterprise Investigations**

During our field work, we examined a judgmental sample of 92 general crimes and criminal intelligence investigations files to assess compliance with Guidelines’ requirements relating to the initiation of investigations, notification to FBI Headquarters and the appropriate U.S. Attorneys’ Offices of specified developments, and the approval by the SAC to use certain authorities.

#### **General Crimes Investigations**

The General Crimes Guidelines provide direction for initiating and pursuing full investigations where the “facts or circumstances reasonably indicate that a federal crime has been, is being, or will be committed.” The Guidelines also require that sensitive criminal matters must be brought to the attention of the U.S. Attorney or other appropriate DOJ officials, as well as to FBI Headquarters. Our review found general compliance with these Guidelines. Specifically, we found:

- all but 1 of the 72 files we reviewed contained the required predication in the opening documentation;
- with respect to investigations of sensitive criminal matters, the FBI provided the required notifications to FBI Headquarters and either DOJ or the U.S. Attorney on a consistent basis, although a copy of the written notification was not regularly included in the case files; and
- the FBI consistently documented notification of case closings.

#### **Criminal Intelligence Investigations**

Criminal intelligence investigations do not focus on the prosecution of completed criminal acts, but instead seek intelligence on criminal enterprises. Criminal intelligence investigations focus on such factors as the size and composition of ongoing criminal enterprises, their geographic dimensions, past activities, intended criminal goals, and capacity to inflict harm. There are two types of criminal intelligence investigations:

rackeering enterprise investigations (REIs), which focus on organized crime, and terrorism enterprise investigations (TEIs), which focus on enterprises that seek to further political or social goals through activities that involve force or violence, or that otherwise aim to engage in terrorism or terrorism-related crimes.

With respect to criminal intelligence investigations, we examined whether the investigative files contained evidence of the required predication and whether the requisite notifications were made to FBI Headquarters, DOJ, and the pertinent U.S. Attorney's Office. The files we examined reflected appropriate predication for the initiation of the REIs and TEIs. However, opening notifications to DOJ and U.S. Attorneys' Offices were not evident in many of the files for REIs (71 percent and 86 percent, respectively). With respect to TEIs, 60 percent of the files did not contain evidence of required notification to the DOJ's Counterterrorism Section, and 80 percent of the files did not contain evidence of the required notification to DOJ's Office of Intelligence Policy and Review (OIPR) and to the pertinent U.S. Attorney's Office. Although only a few files (14 percent) lacked documentation of opening notifications to FBI Headquarters, we found a general lack of consistency in the FBI's documentation practices and supervisory reviews.

### **Counterterrorism Activities and Other Authorizations**

The General Crimes Guidelines contain a new Part VI, labeled "Counterterrorism Activities and Other Authorizations." This portion of the Guidelines explicitly authorizes the FBI to visit public places and attend public events on the same terms and conditions as members of the public for the purpose of detecting or preventing terrorist activities. Previously, the FBI's authority to engage in these activities generally was interpreted to be limited to the investigation of crimes or the collection of criminal intelligence only when agents had a sufficient evidentiary basis to check leads, conduct a preliminary inquiry, or conduct a full investigation.

We evaluated the timeliness and adequacy of the FBI's guidance to the field regarding these new Part VI authorities and attempted to determine how frequently these authorities were utilized. We also examined the approval process and documentation practices used by field offices.

In our interview of FBI personnel at Headquarters and the field offices, we found widespread recognition of the constitutional and privacy implications of these authorities. We also found that the FBI's Office of the General Counsel (OGC) and the Counterterrorism Division (CTD) issued periodic guidance to address several issues pertaining to recordkeeping and dissemination of information derived from these activities.

However, we found gaps in the FBI's implementation of the Part VI authorities. Under present FBI policy, FBI agents are encouraged, but not required, to obtain supervisory approval to visit a public place or attend a



public event under Part VI. They also are not permitted to document what they learn unless they obtain information that pertains to potential terrorist or criminal activity. If agents believe it is appropriate to retain information from these visits, but the information is insufficient to justify the opening of an investigation, the information is normally retained in a file called a “zero file.” Zero files are maintained in field offices and contain miscellaneous information, stacked cumulatively in hard copy, without the capability to readily retrieve all information pertaining to a particular issue or threat.

Our survey of Division Counsel, the legal officers in FBI field offices, revealed that while 86 percent of Division Counsel said they have been consulted between May 2002 and February 2004 about the propriety of retaining information derived from visiting public places or attending public events, 63 percent said they believed that the FBI’s guidance on this issue was not clear when the revised Guidelines were issued, and 55 percent said they believed it was still not clear 21 months later. The FBI also did not establish a Headquarters point of contact to respond to field inquiries regarding constitutional and privacy issues, including questions concerning the Part VI authorities, until March 2003, ten months after the Guidelines became effective. Further, the FBI’s guidance on collecting, indexing, and disseminating information derived from the monitoring or surveillance of protest events was not issued until September 2004.

Due to the absence of routine documentation of the FBI’s use of these authorities and the FBI’s practice of retaining information from these activities in “zero files,” we were unable to determine how frequently the authorities are used. In May 2003, in response to a congressional inquiry, the FBI stated that its informal survey of 45 field offices indicated that agents had visited a mosque only once pursuant to Part VI. At the field offices we visited, we were told that with few exceptions agents did not have time to visit public places or attend public events other than in connection with ongoing investigations.

However, the way the information is retained makes it difficult for field managers or Headquarters to determine when these authorities are used, and whether information derived from their use is appropriately retained, indexed, and disseminated. And, unlike the practices associated with the FBI’s authority to visit public places and attend public events in ongoing investigations (whether in connection with a preliminary inquiry or full investigation under the counterterrorism classification, a full investigation under the General Crimes Guidelines, or under the Undercover Guidelines), neither program managers nor the Inspection Division is able to assess the exercise of these new authorities. While we understand that the FBI does not want to unduly burden case agents with paperwork and approvals, we believe that the FBI should reconsider the approval and documentation process related to Part VI authorities.

In the course of this review, news articles were published stating that the FBI had questioned political demonstrators across the United States in connection with threatened violent and disruptive protests at the Republican National Convention and Democratic National Convention held in the summer of 2004.<sup>7</sup> The initial article stated that dozens of people had been interviewed in at least six states, including anti-war demonstrators and political demonstrators and their friends and family members. Newspaper articles reported that the Department of Justice responded that the interviews were largely limited to efforts at disrupting a plot to bomb a news van at the July 2004 Democratic National Convention in Boston.<sup>8</sup>

Following publication of the news articles, several Members of Congress asked the OIG to initiate an investigation into “possible violations of First Amendment free speech and assembly rights by the Justice Department in connection with their investigations of possible protests at the Democratic and Republican political conventions in Boston and New York and other venues.”<sup>9</sup> Because the request coincided with the investigative work then underway in connection with this review, the OIG commenced an examination of the FBI’s use of investigative authorities in advance of the national political conventions in 2004.

In examining this issue, the OIG has conducted interviews of FBI Headquarters and field personnel and reviewed FBI documents concerning the basis for the interviews referenced in these news stories. We determined that the FBI’s pre-convention interviews were conducted pursuant to several different investigative authorities, only one of which falls within the scope of this review – the General Crimes Guidelines, including the authority to check leads or to conduct preliminary inquiries or full investigations. We therefore decided that in order to address fully the questions that have been raised regarding the scope of the FBI’s activities in relation to the 2004 conventions, we would need to examine the FBI’s use of other authorities that are outside the scope of this review, such as the authorities granted pursuant to Presidential Decision Directive (PDD) 39 and the Antiterrorism and Effective Death Penalty Act of 1996, 18 U.S.C. § 2332b(f). This aspect

---

<sup>7</sup> *Interrogating the Protestors*, The New York Times, Aug. 17, 2004; Eric Lichtblau, *Inquiry into FBI Questioning is Sought*, The New York Times, Aug. 18, 2004. A FOIA request has led to the release of some FBI documents relating to the pre-Convention interviews. See Dan Eggen, *Protestors Subject to ‘Pretext Interviews’*, Washington Post, May 18, 2005; Eric Lichtblau, *Large Volume of F.B.I. Files Alarms U.S. Activist Groups*, The New York Times, July 18, 2005.

<sup>8</sup> Eric Lichtblau, *Protestors at Heart of Debate on Security vs. Civil Rights*, The New York Times, August 28, 2004.

<sup>9</sup> Letter to Glenn Fine from Congressmen John Conyers, Jr., Robert C. Scott, and Jerrold Nadler, dated August 17, 2004.

of our review is still ongoing. We intend to continue this review of the FBI's compliance with the pertinent authorities that applied to its actions in connection with these events, and we will produce a separate report describing our findings.

#### **D. Procedures for Lawful, Warrantless Monitoring of Verbal Communications (Consensual Monitoring Guidelines)**

Non-telephonic consensual monitoring, including the use of body recorders and transmitting devices, is governed by the Consensual Monitoring Guidelines. We examined 103 non-telephonic consensual monitoring files that included recorded conversations to assess compliance with the Guidelines' requirements. We determined whether the files contained evidence of advice from the U.S. Attorney's Office regarding the legality and appropriateness of the monitoring, DOJ approval when monitoring "sensitive" individuals, SAC or ASAC approval prior to recording monitored conversations, and timely authorizations for extensions.

We found that 90 percent of the files were compliant with these Guidelines. The FBI requires that all consensual monitorings be requested on a standard form which addresses the requirements in the Consensual Monitoring Guidelines. We found that the consensual monitoring files consistently included evidence that the U.S. Attorney's Office had provided advice that the consensual monitorings were legal and appropriate.

However, although the standard form includes space for approvals from the SAC and DOJ, the field offices we visited were not consistent in documenting these approvals. Significantly, we found that nine percent of the consensual monitoring files we examined indicated that "overhears" were recorded prior to receiving SAC or ASAC approval and that the recording of conversations occurred from 1 to 59 days prior to receiving this authorization. We were told in some offices that the SAC approval had been obtained orally prior to recording, but had not been annotated. One percent of the monitoring requests involving "sensitive" individuals did not contain evidence of written DOJ approval. In addition, we found that an ambiguity exists in the Consensual Monitoring Guidelines regarding the permissible duration of non-sensitive consensual monitorings.

#### **E. FBI Compliance Oversight Mechanisms**

Our review found that the FBI did not consistently ensure that FBI personnel with special expertise and responsibility for issues addressed in the Guidelines (such as Informant Coordinators, Undercover Coordinators, and Division Counsel) were properly consulted regarding routine investigative activities. For example, we believe the most serious violations of the Undercover Guidelines we identified during this review likely would not have occurred if the Undercover Coordinator or Division Counsel had been consulted by the case agents, even at a minimal level.

Our review concluded that Department of Justice personnel make important contributions to the oversight of the FBI's Criminal Informant Program and the FBI's use of undercover operations, including the promotion of compliance with the applicable Guidelines. This occurs through formal and informal consultations between FBI field personnel and local U.S. Attorneys' Offices, and through DOJ's membership on two key joint FBI-DOJ committees that approve and oversee certain undercover operations and confidential informants: the Criminal Undercover Operations Review Committee (CUORC) and the Confidential Informant Review Committee (CIRC). We agree with the members of these two committees, who stated that the committees are operating smoothly and that DOJ appropriately exercises oversight of sensitive criminal undercover operations and certain high-risk or sensitive confidential informants. With limited exceptions, we found good communication between the FBI and U.S. Attorneys' Offices regarding approval, concurrence, and notice issues under each of the four Investigative Guidelines.

#### **F. The FBI's Implementation Process for the Revised Guidelines**

We assessed the FBI's implementation of the revised Guidelines, including: 1) initial planning for implementation of the revisions; 2) guidance regarding the revisions; 3) training on the revisions; and 4) administrative support for ensuring compliance with the revisions. We believe it is important to evaluate how the FBI implemented the revised Guidelines because lessons learned from this process can be useful when future revisions to Guidelines are made.

We concluded that the FBI's implementation of the revised Guidelines was problematic. Although certain FBI components undertook significant steps to implement the revised Guidelines, such as issuing guidance and providing training, insufficient planning and inter-division coordination affected important aspects of the Guidelines' implementation. Our interviews with FBI personnel revealed, for example, that no entity in the FBI made decisions regarding the priority that should be accorded to Guidelines training throughout the FBI and the form it should take. As a consequence, our surveys of FBI employees approximately two years after revision of the Guidelines revealed that although 100 percent of agents in some offices had received training on individual Guidelines, agents in other offices had received no training. According to the surveys, most Informant Coordinators and Division Counsel believed that they, along with agents in their offices, still required additional training or guidance on the revised Guidelines.

We also found that certain of the FBI's administrative tools used to support compliance with the Guidelines were outdated or otherwise deficient. For example, with regard to the FBI's primary investigative resource manual – the Manual of Investigative Operations and Guidelines

(MIOG) – it took many months, and in some cases closer to two years, for the FBI to update sections to account for the May 2002 Guideline changes. We believe that the FBI's lack of adequate attention to the implementation process contributed to many of the deficiencies we found.

## **V. Recommendations**

It is important to recognize that the May 30, 2002, revisions to the Attorney General Guidelines were developed and issued within months of the September 11 terrorist attacks. During that period, the demands on the FBI and DOJ were extraordinary, and many of those demands continue today.

In making recommendations about the implementation of the Guidelines, we also recognize that there are inevitable tensions between promoting aggressive, proactive, and fully effective investigative tools, on the one hand, and the need to have clearly articulated Guidelines, measures to assure that the Guidelines are followed, reliable data to measure compliance, and accountability for Guidelines' violations, on the other.

We have therefore made 47 recommendations to help improve the FBI's compliance with the Attorney General's Guidelines. In general terms, our recommendations seek to ensure that:

- agents are provided the training, administrative, and technological support they need to comply with the Attorney General Guidelines and related MIOG requirements;
- procedures are in place to ensure that personnel at the FBI and DOJ with responsibility for implementing the Guidelines (including Confidential Informant Coordinators, Undercover Coordinators, Division Counsel, and members of the CUORC and CIRC) participate in important decisions that are made under each of the Guidelines;
- the FBI use technology to better identify, track, and monitor its Guidelines' compliance performance;
- the highly variable and often poor compliance performance of the Criminal Informant Program be remedied;
- the FBI increase inspection coverage of Guidelines-related issues, promote greater accountability for Guidelines deficiencies, and conduct more inspections of priority programs and programs experiencing significant compliance problems; and
- the FBI more effectively implement future revisions of the Guidelines through advance planning, timely guidance, better administrative support, and training of key FBI personnel.

# CHAPTER ONE

## INTRODUCTION

### I. Background

This report describes the results of the OIG's review of the FBI's implementation of the Attorney General's Investigative Guidelines issued on May 30, 2002. Four sets of Attorney General Guidelines were revised at that time:

- 1) The Attorney General's Guidelines Regarding the Use of Confidential Informants (CI or Confidential Informant Guidelines);
- 2) The Attorney General's Guidelines on FBI Undercover Operations (Undercover or UC Guidelines);
- 3) The Attorney General's Guidelines on General Crimes, Racketeering Enterprise and Terrorism Enterprise Investigations (General Crimes or GCI Guidelines); and
- 4) Procedures for Lawful, Warrantless Monitoring of Verbal Communications (Consensual Monitoring or CM Guidelines).<sup>10</sup>

The provisions of these four sets of Attorney General Guidelines are mandatory.<sup>11</sup>

The objectives of our review were to 1) assess the FBI's compliance with these critical controls, and 2) evaluate the methods and procedures used by the FBI to ensure that the revised Guidelines were properly put into practice.

To place this review in context, it is important to recognize that the FBI operates under legal constraints in addition to the Guidelines, such as:

- the Bill of Rights of the United States Constitution;

---

<sup>10</sup> Throughout this report, we refer to these four sets of Guidelines collectively as the "Guidelines," "Attorney General Guidelines," or "Investigative Guidelines." The May 30, 2002, Guidelines are attached at Appendix B and are available electronically on the web site of the Office of Legal Policy of the Department of Justice at: <http://www.usdoj.gov/olp>.

Although the Attorney General's May 30, 2002, memorandum entitled, *Procedures for Lawful, Warrantless Monitoring of Verbal Communications* is not referred to as an Attorney General "Guideline," we included the FBI's compliance with this memorandum in our review. For convenience, we refer to the memorandum as one of the Attorney General's Investigative Guidelines.

<sup>11</sup> See, e.g., § I.A.3 of the CI Guidelines ("These Guidelines are mandatory . . ."); Preamble to GCI Guidelines ("These Guidelines provide guidance for general crimes and criminal intelligence investigations by the FBI. The standards and requirements set forth herein govern the circumstances under which such investigations may be begun, and the permissible scope, duration, subject matters, and objectives of these investigations.").

- numerous federal statutes and regulations, including laws authorizing the use of wiretaps and other investigative techniques, privacy protection laws limiting government access to bank records, medical records, and credit information; specialized laws limiting access to video rental information, telephone call logs, and educational institution records; and federal case law interpreting these protections;
- Executive Orders and Presidential Decision Directives that establish various law enforcement and intelligence priorities and objectives, such as anti-terrorism initiatives issued before and after the attacks of September 11, 2001; and
- policy, administrative, and operational pronouncements issued by the Attorney General, the FBI Director, and the Department of Justice (DOJ) and the FBI, including Attorney General Directives, the FBI's Manual of Investigative Operations and Guidelines (MIOG), and the FBI's Manual of Administrative Operations and Procedures (MAOP).

We focused this review on compliance with the Attorney General Guidelines, rather than on these other legal constraints, for several reasons.

First, the Investigative Guidelines govern most aspects of an FBI agent's day-to-day authority to investigate federal crimes and to conduct criminal intelligence investigations.<sup>12</sup>

Second, these were the first Attorney General Guidelines issued after the September 11, 2001, terrorist attacks. When they were issued, the Attorney General and the FBI Director underscored that the revisions were necessary to remove bureaucratic obstacles to the ability of field agents and their supervisors to address terrorist threats, while at the same time guide the day-to-day activities of key federal law enforcement agencies within constitutional and other legal constraints.

Third, the revised Guidelines give the FBI broader authorities in connection with its efforts to detect and prevent terrorism and to investigate other criminal activity. For example, the May 2002 Investigative Guidelines authorize the FBI to:

- initiate certain types of investigations with lower evidentiary thresholds and without FBI Headquarters approval;

---

<sup>12</sup> One FBI Headquarters official referred to the Investigative Guidelines as the "blueprint" or "template" for the FBI's investigative activities, and others referred to the Guidelines as "the Bible."

- conduct preliminary inquiries and full investigations for longer periods prior to obtaining authority to renew them, and use mail covers during preliminary inquiries;<sup>13</sup>
- use undercover techniques during criminal intelligence investigations (racketeering enterprise and terrorism enterprise investigations), not only in general crimes investigations;
- visit public places and attend public events on the same terms as members of the public for the purpose of detecting or preventing terrorist activities, without the predication required to investigate leads or conduct a preliminary inquiry or full investigation;
- perform general topical research in support of its investigative activities; and
- conduct online searches and access online sites and forums on the same terms as members of the public for the purpose of detecting or preventing terrorism or other criminal activities.

In addition, the Guidelines were revised to state that “the FBI shall not hesitate to use any lawful techniques consistent with these Guidelines, even if intrusive, where the intrusiveness is warranted in light of the seriousness of a crime or the strength of the information indicating its commission or potential future commission,” particularly in conducting counterterrorism investigations.<sup>14</sup>

With respect to the FBI’s use of confidential informants, the most significant recent revisions of the Confidential Informant Guidelines occurred in January 2001, when the version immediately preceding the May 2002 revisions was issued. We believe it is important to evaluate how the FBI’s authorities regarding confidential informants are being utilized.

Fourth, the passage of three years since issuance of the May 2002 Guidelines has given the FBI a reasonable period within which to implement the revisions and a meaningful period by which to measure compliance and assess the implementation process.

Fifth, the May 2002 revised Guidelines were adopted without customary congressional consultation.

Sixth, this is the first comprehensive review of the FBI’s implementation of the May 2002 Investigative Guidelines.<sup>15</sup> While the FBI

---

<sup>13</sup> A mail cover is the recording of any data appearing on the outside cover of any class of mail. MIOG II § 10-6.2.

<sup>14</sup> General Crimes Guidelines, § I at B-68.

<sup>15</sup> In June 2003, David M. Walker, Comptroller General of the United States, testified before a congressional committee that the United States General Accounting Office (GAO) (continued)



Director, the Attorney General, and other officials of the DOJ have responded to several congressional inquiries about the implementation of certain provisions of the May 2002 Guidelines and the FBI's use of some of its new authorities, this OIG review is the first detailed review of the steps the FBI has taken to implement the Guidelines.

We also recognized that our review was conducted during a period of fundamental organizational change within the FBI, the DOJ, other federal law enforcement agencies, and the United States intelligence community in response to the attacks of September 11, 2001.<sup>16</sup> Since late 2001, the FBI has been implementing major changes in its focus and organization, beginning with the December 2001 announcement of the reorganization of its executive management, followed by the May 2002 realignment of FBI resources from traditional criminal investigations to counterterrorism and counterintelligence, the development of greater analytical capabilities, and the institution of a targeted hiring program to fill acknowledged gaps. In June 2004, the FBI Director initiated the process for establishing an intelligence directorate within the FBI. These reforms have been accompanied by significant legal and operational changes in the relationships and information-sharing authorities between the law enforcement and intelligence communities, most notably through the passage of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, known as the USA PATRIOT Act.<sup>17</sup>

---

investigators had conducted a preliminary review of the FBI's implementation of the Guidelines and had determined that internal controls were in place to monitor compliance with the Guidelines. Walker stated that neither the FBI nor any of the oversight bodies or private groups had alerted the GAO to any abuses under the Guidelines. See U.S. General Accounting Office, *FBI Reorganization: Progress Made in Efforts to Reform, but Major Challenges Continue*, GAO-03-759T, 26-32 & App. VI (June 18, 2003).

Both the House and Senate Judiciary Committees have held oversight hearings on different aspects of the revised Investigative Guidelines. With respect to the FBI's use of confidential informants, the House Committee on Government Reform issued a report, *Everything Secret Degenerates: The FBI's Use of Murderers as Informants*, H.R. Rep. No. 108-414 (2004). The House Committee on Government Reform advised the Attorney General in a letter dated May 6, 2004, that it was undertaking an investigation of the FBI's "handling of confidential informants, including its guidelines, policies and practices."

<sup>16</sup> Organization charts for the DOJ and the FBI are attached at Appendix A.

<sup>17</sup> In addition, on June 29, 2005, the President announced a further restructuring of the intelligence community, the Department of Justice, and the FBI. A new National Security Division will be created in the Department of Justice, under the supervision of an Assistant Attorney General, which will consolidate the Department's intelligence resources within one division. At the FBI, a new senior position directly under the FBI Deputy Director will be created to oversee the FBI's intelligence, counterterrorism, and (continued)

The FBI's work in implementing the Investigative Guidelines has also occurred at the same time as other operational and administrative changes affecting the Headquarters and senior field managers who share responsibility with the FBI's 12,000 agents to comply with the Guidelines. During our review, for example, FBI Headquarters' oversight of the Criminal Informant Program moved from the Criminal Investigative Division (CID) to the new Directorate of Intelligence, where all human sources are now supervised in accordance with a Presidential Decision Directive.

During the course of this review, the FBI has addressed some of the concerns identified in this report and is in the process of addressing others. In addition, further revisions of the Investigative Guidelines are under consideration by DOJ and the FBI, including a major overhaul of the various Guidelines used to operate human sources. We believe that the lessons learned from this review of the implementation process employed following the May 2002 revisions of the Investigative Guidelines will be useful whenever the next round of revisions is considered, drafted, issued, and implemented.

## **II. Scope and Methodology of the OIG Review**

### **A. Scope of the Review**

Our review examined the FBI's compliance with the four Attorney General Investigative Guidelines that were revised on May 30, 2002, and the procedures that the FBI relied upon to ensure their proper implementation. Because the Investigative Guidelines govern a broad array of investigative activity, we limited the scope of our compliance review to a number of key provisions in each of the Guidelines.<sup>18</sup>

The revised Guidelines address the FBI's utilization of general crimes investigations to investigate various federal crimes and criminal enterprises, as well as the FBI's use of three key methods or techniques used to conduct general crimes or criminal intelligence investigations:

- (i) the use of *Confidential Informants* – individuals who are used by the FBI to obtain information or to perform certain activities in furtherance of FBI criminal or intelligence investigations, with or without compensation, under the supervision of FBI case agents and their supervisors;

---

counterintelligence components, which will be combined to form a National Security Service within the FBI.

<sup>18</sup> However, we collected a significant amount of information on the FBI's implementation practices beyond those key measures. For example, with regard to FBI undercover operations that were reviewed at FBI Headquarters, we evaluated more than 50 separate variables for each undercover operation we examined.

- (ii) the use of *Undercover Operations* – defined as “investigative activities involving the use of an assumed name or cover identity by an FBI employee or other law enforcement agency working with the FBI which involves an element of deception, the purpose of which is to detect, prevent, and prosecute certain federal offenses;”<sup>19</sup> and
- (iii) the use of *Non-telephonic Consensual Monitoring* – the consensual monitoring of non-telephonic communications.

In addition to the FBI’s compliance performance under each of the four Investigative Guidelines, we examined the steps the FBI has taken since May 2002 to implement the Guidelines, including its planning for implementation, distribution and communication of the Guidelines and related guidance, formal and informal training on the Guidelines, and administrative support provided by FBI Headquarters and the field divisions.

We also examined the operation of the two joint FBI-DOJ committees that review and approve certain types of confidential informants and undercover operations. Those committees are the Confidential Informant Review Committee (CIRC) and the Criminal Undercover Operations Review Committee (CUORC). In addition, we examined the role of FBI components that monitor compliance with some of the Guidelines, including the Undercover and Sensitive Operations Unit (USOU), the Asset/Informant Unit (A/IU),<sup>20</sup> the Office of the General Counsel (OGC), the Inspection Division, and the FBI’s Office of Professional Responsibility (OPR).

Our review also examined, to a limited extent, internal FBI operational changes in the fall of 2003 that shifted Headquarters’ oversight of certain counterterrorism investigations from CID to the Counterterrorism Division (CTD), and the corresponding internal guidance that shifted the applicable Attorney General Guidelines governing those investigations from the General Crimes Guidelines to the Attorney General Guidelines on FBI National Security Investigations and Foreign Intelligence Collection (NSI Guidelines), which were revised on October 31, 2003.

We did not include within our review the FBI’s implementation of the NSI Guidelines. However, as discussed in various recommendations offered throughout this report, because similar operational and administrative challenges are attendant to implementation of the NSI Guidelines, we

---

<sup>19</sup> Field Guide for Undercover & Sensitive Operations (FGUSO) (rev. July 25, 2003), at 1.

<sup>20</sup> During the period of this review, the FBI’s Asset/Informant Unit was in the Criminal Intelligence Section of the CID. Effective November 15, 2004, that unit moved to the Directorate of Intelligence and was renamed the Human Intelligence Unit.

believe the principles we outline for promoting more effective compliance with the Investigative Guidelines may also apply to implementation of the NSI Guidelines.

Following the September 11, 2001, attacks, the Attorney General ordered a top-to-bottom review of the Guidelines “to ensure that they provide front-line field agents with the legal authority they need to protect the American people from future terrorist attacks.”<sup>21</sup> When the revised Guidelines were announced in May 2002, the Attorney General stated that the driving force behind the changes was the belief that “the [investigative] guidelines bar FBI field agents from taking the initiative to detect and prevent future terrorist acts unless the FBI learns of possible criminal activity from external sources.”<sup>22</sup>

Because the Attorney General identified the primary focus of the May 2002 revisions as the prevention and detection of terrorism, our review also sought to determine how the FBI has used the new or expanded authorities and the internal control mechanisms that exist to monitor the exercise of these authorities. For example, we assessed the FBI’s implementation of the new (or newly clarified) authorities to visit public places and attend public events, which are set forth in Part VI of the General Crimes Guidelines.

It is also important to identify several significant internal controls that we did not examine. The FBI and other DOJ law enforcement agencies operate under other Attorney General Guidelines that are beyond the scope of this review. These include the NSI Guidelines mentioned above; Online Investigative Principles for Federal Law Enforcement Agents (for Undercover Operations) (1999); the Attorney General Guidelines for Extraterritorial FBI Operations and Criminal Investigations; the Attorney General Guidelines on the Development and Operation of FBI Criminal Informants and Cooperative Witnesses in Extraterritorial Jurisdictions; the Attorney General Guidelines for Victim and Witness Assistance (2000); and the Attorney General’s Directives Regarding Information Sharing Under the USA PATRIOT Act (2002). With limited exceptions, this review also did not examine the FBI’s compliance with its internal operational mandates that supplement the requirements of the Investigative Guidelines, principally the FBI’s MIOG and the MAOP.<sup>23</sup>

---

<sup>21</sup> Id.

<sup>22</sup> Remarks of Attorney General Ashcroft, Attorney General Guidelines, May 30, 2002, available at: <http://www.usdoj.gov/ag/speeches/2002/53002agpreparedremarks.htm>.

<sup>23</sup> One exception was the MIOG requirement that field supervisors review each case agent’s investigative files every 90 days. See MIOG § 137-4(3). We considered this to be a critical requirement to promote adherence to the Guidelines, and we included it in our data collection at 12 FBI field offices.

In addition, this review did not examine the FBI's compliance with its expanded authorities under the USA PATRIOT Act, including its investigation of international terrorism matters that are now principally governed by the NSI Guidelines. We did, however, seek to determine if there is any operational overlap between the Investigative Guidelines and the NSI Guidelines and, if so, whether there are any gaps or confusion in the field as to which Guidelines apply, what the Guidelines mean, and which FBI Headquarters Division is responsible for supervising the exercise of these authorities. Finally, our review did not examine whether the FBI has been successful in utilizing its new and expanded authorities in accordance with any internal performance measures, standards, or goals that align with the FBI's stated priorities.

## **B. Methodology of the Review**

Our review proceeded in five general phases, some of which overlapped. The first phase consisted of background interviews of key program managers at FBI Headquarters, along with a review of the guidance memoranda and other initial communications by FBI Headquarters to field personnel about the revised Guidelines.

The second phase consisted of over 40 interviews of FBI Headquarters and DOJ personnel who oversee key aspects of the substantive programs governed by the Guidelines; members of the FBI's Office of the General Counsel, which provides periodic guidance and legal advice to the field and conducts training on the Guidelines; senior FBI and DOJ personnel who serve on the joint committees that administer certain aspects of the Guidelines relating to confidential informants and undercover operations; and FBI officials who head the Inspection Division and FBI OPR – each of which plays an important role in promoting adherence to, and monitoring compliance with, the Investigative Guidelines. During this phase of our review, we examined over 1,000 documents generated by the FBI and the DOJ in the course of implementing and monitoring compliance with the revised Guidelines.

During the third phase, we conducted web-based surveys of three groups of FBI agents in the FBI's 56 field offices who play a key role in promoting adherence to the Investigative Guidelines: Criminal Informant Coordinators, Undercover Coordinators, and Chief Division Counsel/Assistant Division Counsel (collectively referred to as Division Counsel) who serve as chief legal advisors in the field. We also administered a fourth survey to Criminal Division Chiefs of the 93 U.S. Attorneys' Offices that focused on the Guidelines' provisions requiring routine approval or concurrence by, or notification of, U.S. Attorneys' Offices.

The fourth phase consisted of 12 field office site visits during which we reviewed a judgmental sample of FBI investigative and administrative files reflecting use of the Guidelines' authorities during the period May 2002

to May 2004.<sup>24</sup> These files reflected investigations of domestic terrorism, international terrorism (prior to September 2003, when the FBI made an internal operational change shifting the Guidelines applicable to these cases to the Attorney General’s Guidelines for National Security Investigations and Foreign Counterintelligence Collection), organized crime, public corruption, narcotics trafficking, and health care fraud. We reviewed cases falling into the category of general crimes investigations as well as criminal intelligence investigations, which includes racketeering enterprise and terrorism enterprise investigations. We examined cases that were in the preliminary inquiry phase as well as full investigations. We also examined field office practices with respect to utilization of the new authorities set forth in Part VI of the General Crimes Guidelines (“Counterterrorism Activities and Other Authorizations”), pursuant to which the FBI is now explicitly authorized to visit public places and attend public events for the purpose of detecting or preventing terrorist activities. In each instance, we examined whether the available documentation showed that key provisions of the four sets of Guidelines were followed. Following our field office site visits, we conducted interviews of the senior managers of each of those field offices – the Special Agents in Charge (SACs).

During the fifth and final phase of the review, after collecting and assimilating the data we collected from FBI Headquarters and the 12 field offices and the other documents produced by the FBI and DOJ, we interviewed several newly appointed senior FBI Headquarters officials and in some cases re-interviewed other senior officials about organizational and other plans that would impact Headquarters and field supervision of the programs governed by the Guidelines. We also interviewed the FBI Director in April 2005.

### **III. Organization of the Report**

This report is organized into nine chapters, beginning with this Introduction. Chapter Two recounts the historical background of the Attorney General Guidelines. It discusses the initial versions of the Guidelines and events that prompted revisions of the different sets of Guidelines.

Chapter Three focuses on the Confidential Informant Guidelines. It addresses the background of the May 2002 revisions, the role of confidential informants in FBI investigations, and the benefits and risks of using confidential informants. We then summarize the major revisions to the

---

<sup>24</sup> We included in our field office site visits six of the largest FBI field offices: New York, Washington D.C., Los Angeles, Chicago, Miami, and Boston; four medium-sized field offices: Denver, Salt Lake City, Portland, and Buffalo; and two smaller field offices: Columbia, S.C., and Memphis.

Guidelines and report the findings of our field office site visits and the significant data collected from our surveys of Confidential Informant Coordinators, FBI Division Counsel, and the Criminal Division Chiefs of the U.S. Attorneys' Offices. We provide our compliance findings – including our observations on how the different aspects of the FBI's implementation process affected compliance outcomes – and provide our recommendations.

Chapter Four examines the revised Undercover Guidelines. It addresses the use of the undercover technique in FBI investigations, the benefits and risks of undercover operations, and the major revisions made to the May 2002 Guidelines. We then report the findings of our field office site visits and the significant data collected from our surveys of FBI Undercover Coordinators, FBI Division Counsel, and the Criminal Division Chiefs of the U.S. Attorneys' Offices. We also present our compliance findings and recommendations.

Chapter Five addresses the revised General Crimes Guidelines and the FBI's use of general crimes and criminal intelligence investigations. After summarizing the major revisions to the Guidelines, we report the findings of our field office site visits and the data collected from our surveys of FBI Division Counsel and the Criminal Division Chiefs of the U.S. Attorneys' Offices. We also analyze the FBI's utilization of its new authority to visit public places and attend public events for the purpose of detecting and preventing terrorist activities contained in Part VI of the General Crimes Guidelines under the heading, "Counterterrorism Activities and Other Authorization." We then provide our analysis of our compliance findings, followed by our recommendations.

Chapter Six focuses on the revised Consensual Monitoring Guidelines. It summarizes the revisions to the Guidelines and reports the findings of our field office site visits, together with data collected from our surveys of FBI Division Counsel and the Criminal Division Chiefs of the U.S. Attorneys' Offices. We also present our compliance findings and recommendations.

Chapter Seven discusses the mechanisms employed by FBI Headquarters to ensure compliance with the Guidelines. These include the operation of the two joint FBI-DOJ oversight committees that review, approve, and monitor certain types of undercover operations and confidential informants: the Criminal Undercover Operations Review Committee (CUORC) and the Confidential Informant Review Committee (CIRC). It also includes inspections conducted of FBI field offices by the Inspection Division every three years; on-site reviews of undercover operations conducted by USOU; and the reinspections of the Criminal Informant Program conducted by CID's Asset/Informant Unit (A/IU) (a function transferred in November 2004 to the Human Intelligence Unit within the Field Intelligence Management Section of the Intelligence Directorate), and the FBI's disciplinary process. The chapter provides our analysis of the effectiveness of each of these functions.

Chapter Eight describes the implementation process employed by the FBI with respect to the May 2002 revisions, including its planning for implementation, its distribution and communication of the Guidelines and related guidance, formal and informal training on the Guidelines, and administrative support provided by FBI Headquarters and the field divisions, including measures used to promote accountability and compliance with the Guidelines. We provide analysis of how the FBI's decisions on each of these aspects of the implementation process impacted Guideline compliance and conclude with our recommendations.

Chapter Nine contains our conclusions. The appendices to the report provide organization charts of the FBI and the DOJ; the text of the four Investigative Guidelines; a table illustrating the May 2002 revisions to the Investigative Guidelines; a table showing the views of USAO Criminal Division Chiefs on the adequacy of FBI coordination on Confidential Informant Guidelines issues; a list of the recommendations that appear at the end of Chapters Three through Eight; a table showing discrepancies between the Investigative Guidelines and FBI policy manuals; the FBI's response to the report; and the OIG's analysis and summary of actions needed to close the report.



[BLANK PAGE]

## **CHAPTER TWO**

### **HISTORICAL BACKGROUND OF THE ATTORNEY GENERAL'S INVESTIGATIVE GUIDELINES**

The May 30, 2002, Investigative Guidelines that are the subject of this review are the latest version of the Attorney General's Investigative Guidelines, the first version of which was issued by Attorney General Edward Levi in 1976. Before addressing the FBI's implementation of the Investigative Guidelines in the succeeding chapters of this report, we believe it is important to describe the historical events that prompted issuance of the first set of Guidelines in 1976 and the context in which the various revisions to them were made thereafter.

#### **I. Introduction**

Since their inception nearly 30 years ago, one of the principal legal constraints under which the FBI has operated has been the Attorney General Guidelines. The FBI does not operate under a general statutory charter but, rather, under Attorney General Guidelines that have been revised from time to time pursuant to the authorities set forth in 28 U.S.C. §§ 509, 510, and 533.

Historically, the Investigative Guidelines have been divided into subject areas, addressing both the types of investigations the FBI may conduct (e.g., checking leads, making preliminary inquiries, or conducting full investigations in connection with general crimes or criminal intelligence investigations), and the specialized techniques the FBI may use in the course of such investigations (e.g., using confidential informants, undercover operations, or non-telephonic consensual monitoring).

In this chapter, we summarize the major revisions of the Attorney General's Investigative Guidelines, noting significant changes to investigative authorities and techniques and the events associated with each revision.

#### **II. The Pre-Guidelines Period**

From its inception, the FBI has had as part of its mission the collection of domestic intelligence and the investigation of domestic security matters. Attorney General Charles J. Bonaparte established the Bureau of Investigation within DOJ in 1908. During the post-World War I period, the Bureau of Investigation was charged with the investigation of suspected anarchists, Bolsheviks, socialists, and other radicals in contemplation of prosecution under the Espionage Act and the Immigration Act.

In 1919 and 1920, a series of bombs exploded in eight American cities that targeted federal and local officials, judges, police departments, and financial institutions on Wall Street. In response, Attorney General A. Mitchell Palmer established a position within DOJ to focus on anti-radical activities and obtained funding from Congress to fight subversion.

On November 7, 1919, with the assistance of Justice Department attorney J. Edgar Hoover, who headed the DOJ's General Intelligence Division, and the Immigration Service within the Labor Department, Attorney General Palmer ordered the first of a year-long sequence of coordinated raids in 12 cities to round up and deport hundreds of members of the Federation of the Union of Russian Workers and other suspected "radicals." In early January 1920, a second wave of coordinated raids led to the arrest of between 5,000 to 10,000 suspected radicals.

During the 1930s, President Franklin D. Roosevelt expressed concern over the growing indications of subversive activities within the United States, especially those of communist and fascist supporters. At the direction of President Roosevelt, the FBI began gathering intelligence on the activities of such individuals and groups.<sup>25</sup> After the end of World War II, as Cold War tensions grew, the FBI refocused its attention on counterespionage activities, including the investigation of Ethel and Julius Rosenberg, who were convicted of espionage against the United States on behalf of the Soviet Union, and executed.

From World War II through the 1970s, the FBI conducted what it called "internal security investigations," the objective of which was to collect intelligence about the political influence of organizations and individuals who espoused what the FBI regarded as revolutionary or extremist viewpoints. The FBI carried out these investigations during periods of intense congressional interest in the nation's internal security, leading to the introduction of legislation in the 1940s and 1950s, principally, the Smith Act<sup>26</sup>, the Voorhis Act<sup>27</sup>, and the Internal Security Act of 1950.<sup>28</sup>

---

<sup>25</sup> The FBI's activities from 1936 to 1945 are described in the final report of the Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities, *Book II: Intelligence Activities and the Rights of Americans*, S. Rep. No. 94-755, at 23-37 (1976) (hereafter "Church Committee, *Book II: Intelligence Activities and the Rights of Americans*").

<sup>26</sup> 18 U.S.C. § 2385 (1952).

<sup>27</sup> 18 U.S.C. § 2386 (1952).

<sup>28</sup> Pub. L. No. 81-831, 64 Stat. 987 (1950) (codified as amended in 50 U.S.C. §§ 831-32; 834-35). The Supreme Court issued a series of decisions in the 1950s and 1960s examining the scope or constitutionality of some of the key federal statutes criminalizing subversive activities. Among the most significant cases were *Dennis v. United States*, 341 U.S. 494 (1951) (upholding constitutionality of the Smith Act); *Service v. Dulles*, 354 U.S. 363 (1957) (reversing Secretary of State's discharge of foreign service officer under the "McCarran Rider" to the Department of State Appropriation Act of 1947); *Yates v. United States*, 354 U.S. 298 (1957) (overturning convictions of Communist leaders, requiring that the government must show advocacy "of action and not merely abstract doctrine" under the Smith Act); *Communist Party of the United States v. Subversive Activities Control Bd.*, 367 U.S. 1 (1961) (upholding constitutionality of Subversive (continued)

In the 1950s, the FBI also developed a series of covert programs designed to collect intelligence about the Communist influence in the United States (COMINFIL).<sup>29</sup> The FBI established other counterintelligence programs, collectively referred to as COINTELPRO, to investigate “racial matters,” “hate organizations,” and “revolutionary-type subversives” whose activities were monitored in accordance with internal FBI policy even if they did not satisfy the “advocacy of violence” standard articulated in the Supreme Court’s controlling decisions.

During the 1960s, the FBI’s internal security investigations extended to the investigation of the activities and supporters of the anti-war and civil rights movements.<sup>30</sup> The FBI used informants throughout this period, including Gary Thomas Rowe, who infiltrated the highest levels of the Birmingham, Alabama chapter of the Ku Klux Klan from 1959 to 1965.<sup>31</sup> Rowe’s activities as an informant came to light during the murder trial of three Klan members who were convicted of killing a white civil rights worker, Viola Gregg Liuzzo, on March 25, 1965, the night after the Selma-Montgomery voting rights march.<sup>32</sup> Rowe was one of the four Klansmen in the killer’s car and witnessed the murder.<sup>33</sup> He reported the crime to the

---

Activities Control Act); and *Brandenburg v. Ohio*, 395 U.S. 444 (1969) (striking down state syndicalism law).

<sup>29</sup> Annual Report of the Attorney General for Fiscal Year 1958, at 338. COMINFIL authorized the investigation of legitimate noncommunist organizations that the FBI suspected were being infiltrated by Communist influences.

<sup>30</sup> The FBI investigated the activities of the NAACP and its members for 25 years and specifically targeted Dr. Martin Luther King, Jr. in attempts to neutralize his public appeal. The surveillance activity of Dr. King and the Southern Christian Leadership Conference (SCLC) spanned nearly five years from December 1963 until his death in April 1968. It included wiretaps of Dr. King’s home telephone and the homes and offices of some of his advisers, wiretaps of the SCLC’s telephone, hidden microphones in Dr. King’s hotel rooms, and the use of FBI informants. Conducted under the FBI’s investigative classification COMINFIL, the efforts to discredit Dr. King included efforts to cut off SCLC’s funding sources, disrupt his marriage, undermine his efforts with foreign heads of state, and discredit him with the clerical and academic communities as well as the media. Church Committee, Book III, *Supplemental Detailed Staff Reports on Intelligence Activities and the Rights of Americans*, S. Rep. No. 94-75, at 79-184 (1976) (hereafter “Church Committee, Book III: Supplementary Detailed Staff Reports on Intelligence Activities and the Rights of Americans”). The Church Committee concluded that the investigation was “unjustified and improper.” *Id.* at 85.

<sup>31</sup> Church Committee, *Book III: Supplementary Detailed Staff Reports on Intelligence Activities and the Rights of Americans*, at 239.

<sup>32</sup> *Liuzzo v. United States*, 565 F. Supp. 640 (E.D. Mich. 1983).

<sup>33</sup> *Id.* at 642.

FBI within hours, and it is undisputed that Rowe's information led to the conviction of the three perpetrators.<sup>34</sup>

In 1975, the Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities, known as the "Church Committee," under the chairmanship of Senator Frank Church, and the House Select Committee on Intelligence under the chairmanship of Otis Pike ("Pike Committee") conducted parallel hearings. The Church Committee examined what the FBI knew of Rowe's knowledge of and involvement in the Klan's activities and what instructions he was given.<sup>35</sup> The Committee heard evidence that the FBI instructed Rowe to join a Klan "Action Group," which "conducted violent acts against blacks and civil rights workers."<sup>36</sup> Rowe testified that he and other Klansmen "had beaten people severely, had boarded buses and kicked people off; and went in restaurants and beaten them with blackjacks, chains, pistols."<sup>37</sup> On one occasion, Rowe said that despite giving the FBI advance warning that Klan members were planning violence against blacks, his FBI contact agent or "handler" instructed him to "go and see what happened."<sup>38</sup> Rowe admitted he participated in the resulting violence to protect his cover.<sup>39</sup> According to the Church Committee, the FBI appeared to walk a fine line in utilizing Rowe, who had provided important information on a variety of murders and other violent crimes.<sup>40</sup> FBI Headquarters instructed the field office to ensure that Rowe understood that he was not to "direct, lead, or instigate any acts of violence."<sup>41</sup> On the other hand, he was present on many occasions when

---

<sup>34</sup> Church Committee, *Book III: Supplementary Detailed Staff Reports on Intelligence Activities and the Rights of Americans*, at 241. Liuzzo's heirs brought an unsuccessful civil suit against the Government under the Federal Tort Claims Act, 28 U.S.C. § 1291, et seq. The court rejected their claim, holding in *Liuzzo v. United States*, 565 F. Supp. 640, 646 (E.D. Mich. 1983), that the Government was not liable because the FBI agents who handled Rowe as an FBI informant acted reasonably and prudently. After an Alabama jury found the three Klansmen not guilty of murder, the Klansmen were convicted of violating Liuzzo's civil rights. See *Liuzzo v. United States*, 485 F. Supp. 1274, 1275-77 (E.D. Mich. 1980).

<sup>35</sup> Church Committee, *Book III: Supplementary Detailed Staff Reports on Intelligence Activities and the Rights of Americans*, at 243-44.

<sup>36</sup> Id. at 243 (footnote omitted).

<sup>37</sup> Id.

<sup>38</sup> Id.

<sup>39</sup> Id.

<sup>40</sup> Id. at 239. The Church Committee's final report included a case study on Rowe, noting Attorney General Nicholas Katzenbach's strong defense of the FBI's use of informants (calling them "critical to the solution of the three murdered civil rights workers") while at the same time acknowledging that an "effective informant program" may produce what Attorney General Katzenbach termed "disruptive results." Id. at 240.

<sup>41</sup> Id. at 244.

violence occurred, and he participated in acts of violence. Rowe's FBI handler testified: "If he happened to be with some Klansman and they decided to do something, he couldn't be an angel and be a good informant."<sup>42</sup>

When the Church Committee presented its findings in 1976, Senator Church described the Committee's work evaluating the FBI's involvement in domestic intelligence in the following terms:

[The Committee investigation's] purpose is . . . to evaluate domestic intelligence according to the standards of the Constitution and the statutes of our land. If fault is to be found, it does not rest in the Bureau alone. It is to be found also in the long line of Attorneys General, Presidents, and Congresses who have given power and responsibility to the FBI, but have failed to give it adequate guidance, direction, and control.<sup>43</sup>

During its 15-month investigation, the Committee determined that FBI Headquarters alone had developed over 500,000 domestic intelligence files on Americans and domestic groups.<sup>44</sup> The targets of the intelligence activities included organizations and individuals espousing revolutionary,

---

<sup>42</sup> Id. at 244 (footnote omitted). Rowe also testified before the Church Committee. See *Intelligence Activities: Hearings on S. Res. 21 Before the Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities of the United States*, 94th Cong., Vol. 6: *Federal Bureau of Investigation*, at 107-32 (1976) (hereafter "Church Committee, Vol. 6: *Federal Bureau of Investigation*") (statement of Gary Thomas Rowe).

Rowe was also present when Walter Bergman, one of the "Freedom Riders," was attacked and severely beaten by a mob in Birmingham, Alabama in 1961. Bergman brought a civil suit seeking damages under the Federal Tort Claims Act, successfully maintaining that the FBI violated its common law and statutory duties by ignoring credible threats of violence and failing to report them to the Department of Justice until four days after the events. A federal district court upheld two of three theories of liability advanced by Bergman in resolving the "question of the government's responsibility to give effect and meaning to our system of laws, and protect those who sought to exercise their rights of free action." *Bergman v. United States*, 565 F. Supp. 1353, 1415 (W.D. Mich. 1983). See also *Bergman v. United States*, 551 F. Supp. 407 (W.D. Mich. 1982); *Bergman v. United States*, 579 F. Supp. 911 (W.D. Mich. 1984); and *Bergman v. United States*, 648 F. Supp. 351 (W.D. Mich. 1986), *aff'd*, 844 F.2d 353 (6th Cir. 1988). Rowe's December 1975 testimony before the Church Committee that he was an FBI informant at the time of the beatings and had told the FBI of the expected attack three weeks before it took place, was referenced in the court's opinion in *Bergman v. United States*, 565 F. Supp. at 1382-85, 1392. Rowe wrote an account of the Freedom Riders incident in his autobiography, *My Undercover Years with the Ku Klux Klan* (Bantam Books 1976).

<sup>43</sup> Church Committee, Vol. 6: *Federal Bureau of Investigation*, at 1-2 (statement of Chairman Frank Church).

<sup>44</sup> Church Committee, *Book II: Intelligence Activities and the Rights of Americans*, at 6.

racist, or otherwise “extremist” ideological viewpoints, but during the 1960s also included investigations of the civil rights, anti-war, and women’s movements. In total, the FBI conducted more than 2,000 COINTELPRO operations before the program was discontinued in April 1971.<sup>45</sup>

Significantly, the Church Committee found that the FBI went beyond investigation and employed COINTELPRO operations to disrupt groups and discredit or harass individuals. While the Committee’s final report did not question the need for lawful domestic intelligence, it concluded that the Government’s domestic intelligence policies and practices required fundamental reform.<sup>46</sup>

The FBI’s use of informants also was the subject of a staff report issued by the Church Committee entitled, “The Use of Informants in FBI Domestic Intelligence Investigations.” Noting that the FBI was using more than 1,500 informants in 1975 in connection with domestic security investigations, the report focused on the absence of clear guidance for FBI agents as to how they should operate informants and what constraints applied to handling agents’ and informants’ activities:

The [FBI’s] Manual contains no standard limiting an informant’s reporting to information relating to the commission of criminal offenses or even to violent or potentially violent activity. In fact, intelligence informants report on virtually every aspect of a group’s activity serving, in the words of both FBI officials and an informant, as a “vacuum cleaner” of information.

\* \* \*

The Manual does not set independent standards which must be supported by facts before an organization can be the subject of informant coverage. Once the criteria for opening a regular intelligence investigation are met, and the case is opened, informants can be used without any restrictions. There is no specific determination made as to whether the substantial intrusion represented by informant coverage is justified by the government’s interest in obtaining information. There is nothing that requires that a determination be made of whether less

---

<sup>45</sup> Church Committee, *Book III: Supplementary Detailed Staff Reports on Intelligence Activities and the Rights of Americans*, at 3 (citation omitted).

<sup>46</sup> The Church Committee held hearings on the FBI’s role in COINTELPRO in November and December 1975. The body of its publicly released work included 1) an interim report with findings on the United States’ involvement in assassination plots against foreign leaders; 2) seven volumes of public hearings; and 3) seven additional “Books” on various topics, including *Book II, Intelligence Activities and the Rights of Americans* (April 26, 1976), and *Book III, Supplementary Detailed Staff Reports on Intelligence Activities and the Rights of Americans* (April 23, 1976).

intrusive means will adequately serve the government's interest. There is also no requirement that the decisions of FBI officials to use informants be reviewed by anyone outside the Bureau. In short, intelligence informant coverage has not been subject to the standards which govern the use of other intrusive techniques such as wiretapping or other forms of electronic surveillance.<sup>47</sup>

In response to these ongoing concerns about ineffective internal controls and oversight, the Congress periodically considered subjecting the FBI to a statutory charter. In 1976 the Church Committee in its Final Report proposed a "comprehensive legislative charter defining and controlling the domestic security activities of the Federal Government."<sup>48</sup> Initially, the legislative charter proposal was supported by FBI Director Clarence Kelly and his successor, William Webster.<sup>49</sup>

Two years later, in 1980, the House Judiciary Committee held oversight hearings on a proposal for a legislative charter. Attorney General Civiletti and FBI Director William Webster supported the House bill.<sup>50</sup> Attorney General Civiletti testified that the charter "is intended to be the foundational statement of the basic duties and responsibilities of the FBI and also its general investigative powers and the principal minimum

---

<sup>47</sup> Church Committee, *Book III: Supplementary Detailed Staff Reports on Intelligence Activities and the Rights of Americans*, at 229-30 (footnotes omitted).

<sup>48</sup> Church Committee, *Book II: Intelligence Activities and the Rights of Americans* at 293-94.

<sup>49</sup> *Legislative Charter for the FBI: Hearings on H.R. 5030 Before the Subcommittee on Civil and Constitutional Rights of the House Committee on the Judiciary, 96th Cong. 1 (1980) (hereafter "1979-1980 House FBI Charter Bill Hearings"); Law Enforcement Undercover Activities: Hearings Before the Senate Select Committee to Study Law Enforcement Undercover Activities of Components of the Department of Justice, 97th Cong. 1041 (1982) (hereafter "1982 Senate Select Committee Hearing on Law Enforcement Undercover Activities") (statement of William H. Webster, Director, FBI).*

A major reform that emerged from the Church Committee was passage of the Foreign Intelligence Surveillance Act of 1978 (FISA), Pub. L. No. 95-511, 92 Stat. 1783 (codified at 50 U.S.C. § 1801-11 (1994 & Supp. IV 1998), amended by Act of Dec. 3, 1999, Public L. No. 160-120, 113 Stat. 1606)), which was signed into law by President Carter on October 24, 1978.

<sup>50</sup> *1979-1980 House FBI Charter Bill Hearings* 3-15 (Testimony of Benjamin R. Civiletti, Attorney General, and William Webster, FBI Director). The Senate's bill was S. 1612, The Federal Bureau of Investigation Charter Act of 1979, 96th Cong. (1979), reprinted in *FBI Charter Act of 1979, S. 1612: Hearings on S. 1612 Before the Senate Committee on the Judiciary, 96th Cong. pt. 2, 427 (1980)*. Section 537 of the bill authorized the FBI Director to impose fines up to \$5,000 on agents who willfully abused "sensitive investigative techniques," which included misuse of informants or intrusive surveillance authorities. *Id.* at 469.



limitation on those powers.”<sup>51</sup> He also stated that “the charter depends for enforcement on the internal disciplinary system of the FBI.”<sup>52</sup>

As we discuss below, Congress did not adopt a general legislative charter defining the FBI’s investigative authorities because of the adoption of the first Attorney General Guidelines in 1976.

### **III. Establishment of the Attorney General Guidelines**

#### **A. The Levi Guidelines – 1976**

Attorney General Edward Levi issued the first Attorney General Guidelines, entitled “Domestic Security Investigation Guidelines.” These guidelines, which were known as the first of the “Levi Guidelines,” became effective on April 6, 1976.<sup>53</sup>

In congressional testimony prior to release of the first Guidelines, Attorney General Levi stated that the Guidelines “proceed from the proposition that Government monitoring of individuals or groups because they hold unpopular or controversial political views is intolerable in our society.”<sup>54</sup> The Guidelines represented a significant shift in DOJ’s approach to domestic terrorism. For the first time, investigations of domestic terrorism were treated as matters for criminal law enforcement, rather than as avenues for intelligence collection.

The Guidelines placed specific limits on techniques the FBI could use and distinguished three types of domestic security investigations:

---

<sup>51</sup> 1979-1980 *House FBI Charter Bill Hearings*, at 3 (Statement of Benjamin R. Civiletti, Attorney General).

<sup>52</sup> *Id.* at 7.

<sup>53</sup> The Levi Guidelines can be found at *FBI Statutory Charter: Hearings Before the Senate Committee on the Judiciary*, 95th Cong. pt. 1, 20-26 (1978) (hereafter “1978 *Senate Hearings on FBI Statutory Charter Part 1*”) and in *FBI Oversight: Hearings Before the Subcommittee on Civil and Constitutional Rights of the House Judiciary Committee on the Judiciary*, 95th Cong. 181-87 (1978).

Today, the FBI includes a reference to the Levi Guidelines on its history timeline as one of only 12 key events in the 1970s. See [www.fbi.gov/fbihistory.htm](http://www.fbi.gov/fbihistory.htm).

<sup>54</sup> *FBI Oversight: Hearings Before the Subcommittee on Civil and Constitutional Rights of the House Committee on the Judiciary*, 94th Cong. 257 (1976) (hereafter “1976 *House FBI Oversight Hearing*”) (testimony of Edward H. Levi, Attorney General, Department of Justice). A second set of Guidelines issued by Attorney General Levi governed the FBI’s authority to investigate groups it suspected of links to foreign powers. The Attorney General’s Guidelines for Foreign Counterintelligence Investigations (FCI) are classified. Today, these authorities are set forth in the Attorney General’s Guidelines for FBI National Security Investigations and Foreign Intelligence Collection (NSI Guidelines). The unclassified portions are available at: <http://www.usdoj.gov/olp>.

1) preliminary investigations, 2) limited investigations, and 3) full investigations.<sup>55</sup> The Guidelines provided that the FBI could commence a full domestic security investigation only on the basis of “specific and articulable facts giving reason to believe that an individual or group is or may be engaged in activities which involve the use of force or violence.”<sup>56</sup>

In a memorandum dated December 15, 1976, Attorney General Levi issued the second set of Attorney General Guidelines entitled, “Use of Informants in Domestic Security, Organized Crime, and Other Criminal Investigations” (“Levi Informant Guidelines”).<sup>57</sup> Noting that the Government’s use of informants may involve deception and intrusion into the privacy of individuals and may require Government cooperation with persons whose reliability and motivation may be open to question, the Guidelines outlined the factors to be evaluated in using informants, the instructions informants were to be given, and the steps to be taken in the event the FBI learned that an informant used in investigating criminal activity had violated the instructions or learned of the commission of a crime.<sup>58</sup>

The Informant Guidelines were part of a broader effort to reform the FBI’s investigative and intelligence operations in light of the findings of the Church Committee.<sup>59</sup> Attorney General Levi emphasized that it was imperative that “special care be taken not only to minimize [use of

---

<sup>55</sup> 1978 Senate Hearings on FBI Statutory Charter Part 1 at 20 (Levi Guidelines § II.A). Although titled the “Domestic Security Investigation Guidelines,” the Levi Guidelines governed not only investigations of domestic security threats, but the FBI’s general criminal investigative authorities.

<sup>56</sup> Id. at 22 (Levi Guidelines § II.I).

<sup>57</sup> The Levi Informant Guidelines can be found at Final Report of the Select Committee to Study Undercover Activities of Components of the Department of Justice, S. Rep. No. 97-682, at 531-35 (1983) (hereafter “*1982 Final Report of the Senate Select Committee to Study Undercover Activities*”).

<sup>58</sup> Id. The Guidelines “were intended, in part, to diminish the perceived need for legislation to regulate and restrict the FBI’s use of informants.” See generally *United States v. Salemme*, 91 F. Supp. 2d 141, 190-91 (D. Mass. 1999).

<sup>59</sup> According to the Church Committee, on December 23, 1974, FBI Headquarters sent employee conduct standards to all FBI field offices. The communication stated: “You are reminded that these instructions relate to informants in the internal security [domestic, intelligence] field and no informant should be operated in a manner which would be in contradiction of such instructions.” Church Committee, *Book III: Supplementary Detailed Staff Reports on Intelligence Activities and the Rights of Americans*, at 267. According to the Church Committee report, this instruction was the only written provision applying FBI employee conduct standards to informants. Prior to the issuance of this instruction in 1974, there were no formal or specific provisions relating to informant conduct in FBI directives. Id.

informants] but also to ensure that individual rights [were] not infringed and that the government itself did not become a violator of the law.”<sup>60</sup> The Guidelines stated that while informants were not employees of the FBI, “the relationship of an FBI informant to the FBI impos[ed] a special responsibility upon the FBI when the informant engage[d] in activity where he received, or reasonably [thought] he received, encouragement or direction for that activity from the FBI.”<sup>61</sup> Attorney General Levi also stressed that while the FBI would have primary responsibility for these investigations, DOJ would have “much greater involvement.”<sup>62</sup>

The Levi Informant Guidelines left significant decision-making authority within the discretion of the agents handling the informant. For example, neither the DOJ nor the U.S. Attorneys had any approval or oversight function in connection with an informant’s participation in otherwise illegal activity.<sup>63</sup> However, if an informant committed an unauthorized criminal act in connection with an FBI assignment, the Guidelines required notification of the appropriate law enforcement or prosecutive authorities.<sup>64</sup>

The impact of the new Guidelines was readily apparent in FBI case statistics. William Webster, who served as FBI Director from 1978 to 1987, provided information in connection with a March 16, 1978, hearing indicating that the FBI’s domestic security investigations had declined from 21,414 in July 1973 to 4,868 in March 1976, and stated publicly on May 3, 1978, that the Bureau was “practically out of the domestic security field.”<sup>65</sup>

---

<sup>60</sup> 1982 *Final Report of the Senate Select Committee to Study Undercover Activities*, at 531 (Levi Informant Guidelines, Introduction).

<sup>61</sup> *Id.*

<sup>62</sup> 1976 *House FBI Oversight Hearing*, at 258.

<sup>63</sup> Under the Levi Informant Guidelines, the FBI was merely required to notify DOJ if a confidential informant violated the law in furtherance or unconnected to an FBI assignment when notification to local authorities was inadvisable due to “exceptional circumstances.”

As we discuss in Chapters Three and Seven, since the Confidential Informant Guidelines were revised in January 2001, the decision to approve a high level, long-term, or a privileged or media-affiliated confidential informant is made by the joint FBI-DOJ Confidential Informant Review Committee (CIRC).

<sup>64</sup> 1982 *Final Report of the Senate Select Committee to Study Undercover Activities*, at 533 (Levi Informant Guidelines § C.2). When an informant violated the law, and notification to local authorities was inadvisable due to “exceptional circumstances”, the DOJ determined when law enforcement or prosecutive authorities should be notified; what use, if any, should be made of the information gathered; and whether the FBI should continue using the informant. *Id.* at 533-34 (Levi Informant Guidelines § C).

<sup>65</sup> Report of the Subcommittee on Security and Terrorism, 98th Cong., *Impact of Attorney General’s Guidelines for Domestic Security Investigation (The Levi Guidelines)* 5 (continued)

Before a number of high-profile investigations occurred in the 1980s, the Attorney General Guidelines were generally considered to be working well. As Attorney General Civiletti stated when he testified in 1980 in support of the FBI charter legislation:

I believe the experience of the last three years with the Levi Guidelines has been highly encouraging. It has demonstrated that guidelines can be drawn which are well understood by Bureau personnel and by the public and which can be filed and reviewed by the appropriate congressional committees. It has also shown that guidelines can be successfully applied to particular kinds of investigative activity and even to certain specific decisions made on a case-by-case basis. The reasonable conclusion which can be drawn from the success of these guidelines is that the charter need not detail every limitation or safeguard by express statutory terms. Such details are better covered in guidelines, with the charter setting forth the obligatory principles and objectives which the guidelines must meet and achieve.<sup>66</sup>

Within the FBI, however, there was concern that the Levi Guidelines would unduly limit authorized techniques and would not permit the FBI to be proactive, to collect intelligence before disaster struck, and to develop an adequate intelligence base.<sup>67</sup>

## **B. The Civiletti Guidelines – 1980-1981**

Revelations regarding the conduct of some informants, FBI agents' knowledge of these activities, and interpretations of FBI statements or actions promising immunity for the informants prompted Attorney General Civiletti to issue revised confidential informant guidelines on December 4, 1980.<sup>68</sup> The revised Guidelines explicitly provided that, if necessary and appropriate, informants may be authorized to participate in two different

---

(Comm. Print 1984) (hereafter "*Impact of the Levi Guidelines*"). The most significant drop occurred prior to the issuance of the Levi Guidelines, a development which the Subcommittee indicated was due in part to the fact that "the FBI was reducing its domestic security work for some time before the Guidelines were imposed." *Id.* From March 31, 1976, to February 24, 1978, the number of domestic security investigations dropped from 4,868 to 102. *Id.*

<sup>66</sup> 1979-1980 House FBI Charter Bill Hearings, at 4 (Statement of Benjamin R. Civiletti, Attorney General, Department of Justice).

<sup>67</sup> *Impact of the Levi Guidelines*, supra n.65, at 9.

<sup>68</sup> Attorney General's Guidelines on FBI Use of Informants and Confidential Sources (hereafter "*Civiletti Informant Guidelines*") can be found at 1982 *Final Report of the Senate Select Committee to Study Undercover Activities*, at 517-30.

types of “otherwise criminal activity” at the behest of the FBI, “ordinary” and “extraordinary.” “Ordinary” criminal activity could be authorized by an FBI field office supervisor or higher FBI official. “Extraordinary” criminal activity was defined as any activity involving a significant risk of violence, corrupt actions by high public officials, or severe financial loss to a victim.”<sup>69</sup> Only SACs could authorize extraordinary criminal activity, and only with the approval of the pertinent U.S. Attorney.<sup>70</sup>

In addition, both FBI Headquarters and the Assistant Attorney General in charge of the Criminal Division were to be “immediately” informed of any authorization of extraordinary criminal activity.<sup>71</sup> In the event an informant engaged in unauthorized criminal activity which was deemed “serious”, the approval of either the FBI Director or a senior Headquarters official in consultation with the Assistant Attorney General in charge of the Criminal Division was required to continue to use the informant.<sup>72</sup> The Civiletti Informant Guidelines also made modifications to the factors to be considered in determining the advisability of notifying appropriate law enforcement authorities of criminal activity by FBI informants.<sup>73</sup>

In addition, for the first time, the Guidelines assigned federal prosecutors a coordinating role in relation to informant activities:

In any matter presented to a United States Attorney or other federal prosecutor for legal action . . . where the matter has involved the use of an informant or a confidential source in any way or degree, the FBI shall take the initiative to provide full disclosure to the federal prosecutor concerning the nature and scope of the informant’s or confidential source’s participation in the matter.<sup>74</sup>

---

<sup>69</sup> 1982 *Final Report of the Senate Select Committee to Study Undercover Activities*, at 523 (Civiletti Informant Guidelines § F.2).

<sup>70</sup> *Id.* at 523 (Civiletti Informant Guidelines § F.3).

<sup>71</sup> *Id.*

<sup>72</sup> *Id.* at 524-25 (Civiletti Informant Guidelines § G).

<sup>73</sup> *Id.* at 526.

<sup>74</sup> *Id.* at 529 (Civiletti Informant Guidelines § L). In a memorandum explaining the Civiletti Guidelines, Director Webster stated that this provision was added merely to assist the prosecutor “in protecting the identity of our informants” and “should not be construed as the development of a partnership between the FBI and USDOJ in operating our informants.” See Staff Study: *Overview of Government’s Handling of Jackie Presser Investigation*, Permanent Subcommittee on Investigations of the Committee on Governmental Affairs (May 9, 1986) (hereafter “*Senate Staff Study on Jackie Presser Investigation*”), reprinted in *Department of Justice’s Handling of the Jackie Presser* (continued)

The Civiletti Informant Guidelines also revised the terms of the instructions required to be given to informants. The Civiletti Guidelines required FBI agents operating informants to advise informants that their relationship with the FBI would not protect them from arrest or prosecution for any violation of federal, state, or local law, except insofar as a field supervisor or SAC determined pursuant to appropriate Attorney General Guidelines that the informant's criminal activity was justified. If the required warnings were given to informants, they would reasonably understand that the FBI, without the involvement of any prosecutor, lacked the authority to decide if the informants would be protected from arrest and prosecution.<sup>75</sup>

In the 1980s, the Guidelines were again revised following press accounts and congressional hearings concerning the FBI's domestic intelligence and counterespionage activities, and its undercover operations. The most dramatic revelations involved several high profile undercover operations, one of which targeted members of the United States Congress in the ABSCAM investigation.

ABSCAM was an FBI "sting" operation run out of the FBI's Hauppauge, Long Island office which initially targeted trafficking in stolen property and thereafter was converted to a public corruption investigation. The investigation ultimately led to the conviction of a United States Senator, six members of the House of Representatives, the Mayor of Camden, New Jersey, members of the Philadelphia City Council, and an inspector for the Immigration and Naturalization Service.

During the ABSCAM investigation, the FBI relied on an informant, Melvin Weinberg, who presented himself as a business agent for "Abdul Enterprises," a fictitious organization ostensibly supported by two wealthy Arab sheiks looking for investment opportunities in America.<sup>76</sup> As part of the scheme, the sheiks approached designated public officials and offered them money or other consideration in exchange for favors assisting their cause. The undercover operation called for Weinberg to contact a variety of individuals and tell them that his principals were seeking to invest large sums of money. When the investigation became public in early 1980, controversy centered on the use of the "sting" technique and Weinberg's

---

*Ghostworkers Case*: Hearing Before the Permanent Subcommittee on Investigations of the Senate Committee on Governmental Affairs, 99th Cong. 105-106 (1986) (hereafter "*Senate Subcommittee Hearing on the Jackie Presser Ghostworkers Case*").

<sup>75</sup> 1982 *Final Report of the Senate Select Committee to Study Undercover Activities*, at 521 (Civiletti Informant Guidelines § E).

<sup>76</sup> For a discussion of the techniques used in ABSCAM, see *United States v. Kelly*, 707 F.2d 1460 (D.C. Cir.) (per curiam), cert. denied, 464 U.S. 908 (1983).

involvement in selecting targets. Although Weinberg was found to have previously engaged in numerous felonious activities, he avoided a three-year prison sentence and was paid \$150,000 in connection with the operation. Ultimately, all of the ABSCAM convictions were upheld on appeal,<sup>77</sup> although some judges criticized the tactics used by the FBI and lapses in FBI and DOJ supervision.<sup>78</sup>

In the wake of ABSCAM, Attorney General Civiletti issued “The Attorney General Guidelines for FBI Undercover Operations” (“Civiletti Undercover Guidelines”) on January 5, 1981.<sup>79</sup> These were the first Attorney General Guidelines for undercover operations, and they formalized procedures necessary to conduct undercover operations.

Following the initial press accounts about the ABSCAM investigation, Congress held a series of hearings to examine FBI undercover operations and the new Civiletti Undercover Guidelines. The House Subcommittee on Civil and Constitutional Rights began hearings on FBI undercover operations in March 1980 and concluded with a report in April 1984.<sup>80</sup>

---

<sup>77</sup> *United States v. Kelly*, 707 F.2d 1460 (D.C. Cir. 1983) (per curiam), rev’g 539 F. Supp. 363 (D.D.C. 1982), cert. denied, 464 U.S. 908 (1983); *United States v. Williams*, 705 F.2d 603 (2d Cir.), cert. denied, 464 U.S. 1007 (1983); *United States v. Myers*, 692 F.2d 823 (2d Cir. 1982), cert. denied sub. nom. Lederer v. United States, 461 U.S. 961 (1983); *United States v. Alexandro*, 675 F.2d 34 (2d Cir.), cert. denied, 459 U.S. 835 (1982); *United States v. Jannotti*, 673 F.2d 578 (3d Cir. 1982) (en banc), rev’g, 501 F. Supp. 1182 (E.D. Pa. 1980), cert. denied, 457 U.S. 1106 (1982).

<sup>78</sup> See, e.g., *United States v. Jannotti*, 673 F.2d at 612, 613-14 (Aldisert, J., dissenting); *United States v. Kelly*, 539 F. Supp. at 373-74 & n.45.

<sup>79</sup> The Civiletti Undercover Guidelines can be found at *1982 Final Report of the Senate Select Committee to Study Undercover Activities*, at 536-55. Attorney General Civiletti retained the Levi Domestic Security Guidelines but issued a revision on December 2, 1980, called, “The Attorney General’s Guidelines on Criminal Investigations of Individuals and Organizations.” The revisions distinguished between general crimes investigations and “racketeering enterprise investigations,” whose “immediate purpose” is to “obtain information concerning the nature and structure of the enterprise . . . with a view to the longer range objective of detection, prevention, and prosecution of the criminal activities of the enterprise.” *1982 Final Report of the Senate Select Committee to Study Undercover Activities* at 515 (Civiletti General Crimes Guidelines § II.C).

<sup>80</sup> *FBI Undercover Operations*, Report of the Subcommittee on Civil and Constitutional Rights of the House Committee on the Judiciary, 98th Cong. (1983) (hereafter “*1983 House Subcommittee Report on FBI Undercover Operations*”). The hearings are reported at *FBI Oversight: Hearings Before the Subcommittee on Civil and Constitutional Rights of the House Committee on the Judiciary*, 96th Cong. (1980); *FBI Undercover Guidelines: Oversight Hearings Before the Subcommittee on Civil and Constitutional Rights of the House Committee on the Judiciary*, 97th Cong. (1981) (hereafter “*1981 House Oversight Hearings*”); *FBI Undercover Operations: Hearings Before the Subcommittee on Civil and Constitutional Rights of the House Committee on the Judiciary*, 97th Cong. (1983) (hereafter “*1982 House Subcommittee Hearings*”); *FBI Undercover Activities, Authorization*, (continued)

Among the concerns expressed during the hearings were the undercover agents' involvement in illegal activity, the possibility of entrapping individuals, the prospect of damaging the reputations of innocent civilians, and the opportunity to undermine legitimate rights to privacy.<sup>81</sup> Several witnesses testified that the Civiletti Undercover Guidelines did not sufficiently address entrapment and called for the revision of the provisions prohibiting inducing subjects not suspected of criminal activity.<sup>82</sup> Congress also heard testimony from numerous individuals who claimed they were unjustly victimized by an FBI-sponsored undercover operation.<sup>83</sup> On April 29, 1982, FBI Director Webster reported that there were 10 undercover operations that resulted in the filing of 30 civil suits implicating the FBI and/or its employees.<sup>84</sup>

In March 1982, after the Senate debated a resolution to expel Senator Harrison A. Williams for his conduct in ABSCAM, the Senate established the Select Committee to Study Undercover Activities.<sup>85</sup> In December 1982, the Committee issued its final report, which was generally supportive of the undercover technique but observed that its use “creates serious risks to citizens’ property, privacy, and civil liberties, and may compromise law enforcement itself.”<sup>86</sup>

The Committee’s final report called for clarification of vague terminology in the Guidelines and strict approval procedures. The Committee stated that there were several weaknesses in the Civiletti Undercover Guidelines.

- The terms “extension,” “operation,” and “public official” were internally defined by the FBI “in a manner that makes each of

---

*and H.R. 3232: Oversight Hearings Before the Subcommittee on Civil and Constitutional Rights of the House Committee on the Judiciary, 98th Cong. (1983).*

<sup>81</sup> *1981 House Oversight Hearings*, at 2-7; 33-48 (statements of Professor Geoffrey R. Stone, Univ. Of Chicago Law School, and Gary T. Marx, Professor of Sociology, MIT).

<sup>82</sup> *1981 House Oversight Hearings*.

<sup>83</sup> *1982 House Subcommittee Hearings* at 1-35.

<sup>84</sup> *Id.* at 402.

<sup>85</sup> *1982 Final Report of the Senate Select Committee to Study Undercover Activities*, at 4-5.

<sup>86</sup> *Id.* at 11. The Committee observed that undercover operations “have substantially contributed to the detection, investigation, and prosecution of criminal activity, especially organized crime and consensual crimes such as narcotics trafficking, fencing of stolen property, and political corruption.” *Id.*



those terms redundant, exceedingly narrow, or inconsistent with usage in other guidelines and documents.”<sup>87</sup>

- The Guidelines failed to indicate what circumstances justified “the use of violence, the commission of a crime, or interference with a privileged relationship.”<sup>88</sup>
- The Guidelines failed to make clear what circumstances required the FBI to perform all the steps required to initiate an undercover operation or to modify an existing undercover operation.<sup>89</sup>

In addition, the report asked that Congress be consulted at least 30 days before the promulgation of every guideline governing undercover or criminal investigations, and every amendment to, or deletion or formal interpretation of, any such guideline.<sup>90</sup>

Both the House Subcommittee on Civil and Constitutional Rights and the Senate Select Committee concluded that the existing Attorney General Guidelines and the FBI’s internal controls were insufficient to constrain undercover investigations, and both proposed legislative solutions.<sup>91</sup> The Senate Select Committee recommended federal legislation to govern law enforcement undercover operations and the inclusion of congressional oversight mechanisms. Although the Senate Select Committee supported legislation, it rejected the House’s recommendation of a judicial warrant requirement. Instead, the Senate Select Committee proposed a “probable cause” standard for undercover operations seeking to infiltrate governmental, religious, or news media organizations, and a finding of “reasonable suspicion” for all other operations seeking to detect past, ongoing, or planned criminal activity.<sup>92</sup>

Three years after the Civiletti Guidelines were issued and a year following the 1982 House hearings at which DOJ officials provided repeated assurances that the Undercover Guidelines would “ensure that critical judgments are made at appropriate levels of authority,” a House Judiciary Subcommittee examined their application in a Cleveland-based undercover operation, code-named “Operation Corkscrew.”<sup>93</sup> The investigation was

---

<sup>87</sup> Id. at 54.

<sup>88</sup> Id. at 55.

<sup>89</sup> Id. at 53.

<sup>90</sup> Id. at 25.

<sup>91</sup> Id. at 23-29; *1984 House Subcommittee Report on FBI Undercover Operations*, at 9-11.

<sup>92</sup> *1982 Final Report of the Senate Select Committee to Study Undercover Activities*, at 377-78.

<sup>93</sup> *1984 House Subcommittee Report on FBI Undercover Operations*, at 7.

designed to probe case-fixing in the Cleveland Municipal Court. Conducted in 1977 to 1982, the operation did not produce evidence deemed worthy of prosecution by the U.S. Attorney's Office. While the paperwork submitted by the case agents asserted that the primary targets were judges, the only evidence developed was that the Court's "antiquated recordkeeping system . . . could be easily tampered with or circumvented by any employee with access to these documents."<sup>94</sup>

In blunt criticism directed at the FBI's failure to adhere to the Attorney General Guidelines, the House Subcommittee concluded that in Operation Corkscrew "virtually every one of the principal safeguards was either directly violated, ignored, or administratively construed in a manner inconsistent with their stated purposes with profoundly disturbing results to the FBI, the suspects, and the public."<sup>95</sup> The Subcommittee asserted there were major Guidelines violations:

- the operation was initiated without the requisite evidentiary threshold of "reasonable suspicion" of judicial case-fixing;<sup>96</sup>
- the Guidelines' provision requiring that the proposed criminal activity be "clear and unambiguous" was "not only ignored but was apparently deliberately violated in order to produce 'evidence' of wrongdoing;"<sup>97</sup>
- evidence casting doubt on the principal FBI informant's credibility was not investigated by the case agents or brought to the attention of field supervisors or FBI Headquarters;
- the fact that the subject matter of the investigation qualified as a "sensitive circumstance" under the Guidelines did not result in special scrutiny either at FBI Headquarters or DOJ;
- the Undercover Operations Review Committee (composed of both FBI and DOJ personnel) was provided "incomplete and misleading information" and failed to "challenge or test the sufficiency and accuracy of information" provided by field agents;<sup>98</sup> and
- the U.S. Attorney's Office did not appear to assess independently the evidence developed in the investigation.<sup>99</sup>

---

<sup>94</sup> Id. at 55.

<sup>95</sup> Id. at 7.

<sup>96</sup> Id.

<sup>97</sup> Id. at 8.

<sup>98</sup> Id.

<sup>99</sup> Id. at 74.

Finally, the Subcommittee asserted that the problems in the ABSCAM and Corkscrew investigations “are not aberrations, but in fact reflect a pattern of recurrent problems which are inherent in the process.”<sup>100</sup>

### **C. The Smith Guidelines – 1983**

In the 1980s, Congress also scrutinized the FBI’s domestic security investigations. In 1982 and 1983, the Senate Subcommittee on Security and Terrorism held a series of five hearings on the Levi Domestic Security Guidelines.<sup>101</sup> Some members of the Congress believed that the Levi Guidelines “unduly restricted” the FBI’s authority to monitor and prevent potential terror or violence against persons and property in the United States, pointing to the provisions that required a criminal predicate to initiate an investigation.<sup>102</sup>

The Subcommittee completed its assessment of the Levi Guidelines with the issuance of a report entitled, “Impact of Attorney General Guidelines for Domestic Security Investigations (The Levi Guidelines).” The Subcommittee concluded that the Attorney General Guidelines are “necessary and desirable” but recommended that the Guidelines be revised to delete the criminal standard for initiating domestic security investigations; extend time limits for investigations, particularly those for preliminary and limited investigations; lower the evidentiary threshold for initiating limited investigations; relax restrictions on the recruitment and use of new informants; and authorize investigations of systematic advocacy of violence, alleged anarchists, or other activities calculated to weaken or undermine federal or state governments.<sup>103</sup> The Subcommittee recommended that the revised Guidelines be tested and evaluated and that DOJ should thereafter “present legislative recommendations to Congress to justify the enactment into law of adequate and effective guidelines for domestic security investigations.”<sup>104</sup>

After an 8-month review involving numerous DOJ components and consultation with members of the Congress, Attorney General Smith issued a revised set of Attorney General Guidelines, entitled “The Attorney General’s Guidelines on Domestic Security Investigations” (the “Smith

---

<sup>100</sup> Id. at 8-9.

<sup>101</sup> *Attorney General’s Guidelines for Domestic Security Investigations (Smith Guidelines)*: Hearings Before the Subcommittee on Security and Terrorism of the Senate Committee on the Judiciary, 98th Cong. 1 (1983) (hereafter “1983 Senate Subcommittee Hearings on Smith Guidelines”).

<sup>102</sup> Id. at 5 (statement of Senator John P. East, Member, Committee on the Judiciary).

<sup>103</sup> *Impact of the Levi Guidelines*, supra n.65, at 29, 34-35.

<sup>104</sup> Id. at 35.

Guidelines”), on March 7, 1983.<sup>105</sup> In announcing the revisions, Attorney General William French Smith stated that the Guidelines were needed “to ensure protection of the public from the greater sophistication and changing nature of domestic groups that are prone to violence” but would “retain adequate protections for lawful and peaceful political dissent.”<sup>106</sup> Attorney General Smith stated that FBI agents had “demonstrated their professional competence, integrity, and ability to adhere to requirements.”<sup>107</sup> Moreover, he said that the integration of all FBI law enforcement investigation guidelines into one document was meant to enhance the effectiveness of terrorism investigations by applying to these investigations the concepts and standards that effectively governed the FBI’s racketeering enterprise investigations.<sup>108</sup>

The Smith Guidelines introduced a new type of investigation called the “criminal intelligence investigation,” which had a broader organizational focus than a general crimes investigation and authorized the FBI to investigate certain enterprises which sought “either to obtain monetary or commercial gains or profits through racketeering activities or to further political or social goals through activities that involve criminal violence.”<sup>109</sup> In addition to retaining the racketeering enterprise investigation carried forward from the Civiletti Guidelines, the Smith Guidelines provided for a “domestic security/terrorism investigation,” whose purpose is “to obtain information concerning the nature and structure of the enterprise . . . with a view to the longer range objective of detection, prevention, and prosecution of the criminal activities of the enterprise.”<sup>110</sup> A domestic security/terrorism investigation could lawfully collect information regarding “(i) the members of the enterprise and other persons likely to be knowingly acting in

---

<sup>105</sup> Press Release, Department of Justice (March 7, 1983), reprinted in *1983 Senate Subcommittee Hearing on Smith Guidelines* at 47. The Smith Guidelines can be found at *FBI Domestic Security Guidelines: Oversight Hearings Before the Subcommittee on Civil and Constitutional Rights of the House Committee on the Judiciary, 98th Cong.* 67-85 (1983) (hereafter “*1983 House Oversight Hearings on Domestic Security Guidelines*”).

<sup>106</sup> Press Release, Department of Justice (March 7, 1983), reprinted in *1983 Senate Subcommittee Hearing on Smith Guidelines*, at 47.

<sup>107</sup> *Id.* at 48.

<sup>108</sup> *Id.*

<sup>109</sup> *1983 House Oversight Hearings on Domestic Security Guidelines*, at 75 (Smith Guidelines § III). There were two types of criminal intelligence investigations depending on the objective of the enterprise: a racketeering enterprise investigation and a domestic security/terrorism enterprise investigation.

<sup>110</sup> *Id.* at 80 (Smith Guidelines § III.B.2). The Smith Guidelines brought the Civiletti Guidelines’ category of “racketeering enterprise investigations” under the rubric of “criminal intelligence investigations.” *Id.* at 76 (Smith Guidelines § III.A).

furtherance of its criminal objectives, provided that the information concerns such persons' activities on behalf of or in furtherance of the enterprise; (ii) the finances of the enterprise; (iii) the geographic dimensions of the enterprise; and (iv) past and future activities and goals of the enterprise.”<sup>111</sup>

FBI Director Webster characterized the changes to the Guidelines as “evolutionary,” “not revolutionary,” stating that the Guidelines needed to adjust as the FBI learned more about organized crime and criminal enterprises. According to Webster, the revisions allowed agents to address the needs of the time, particularly those posed by terrorist organizations that were becoming more fluid with inconsistent structure and varied personnel composition.<sup>112</sup>

The Smith Guidelines also lowered the evidentiary thresholds for initiating full domestic security/terrorism investigations, requiring the FBI to identify “facts or circumstances reasonably indicat[ing] that two or more persons are engaged in an enterprise for the purpose of furthering political or social goals wholly or in part through activities that involve force or violence and a violation of the criminal laws of the United States.”<sup>113</sup> This replaced the “specific and articulable facts” standard in the Levi Guidelines. The Smith Guidelines provided that the “reasonable indication” standard required an objective, factual basis for initiating the investigation, but did not require specific facts or circumstances indicating a past, current, or impending violation.<sup>114</sup> The Smith Guidelines also filled a gap in the Levi Guidelines by permitting “low-level” monitoring of dormant groups even though they did not appear to be an immediate threat.<sup>115</sup>

The Smith Guidelines restricted the scope of the “preliminary inquiry” tool in domestic security investigations. While the Levi Guidelines permitted preliminary inquiries in domestic security investigations to determine if there was a factual predicate for opening a full investigation, the Smith Guidelines eliminated the use of preliminary inquiries in domestic security

---

<sup>111</sup> Id. at 81 (Smith Guidelines § III.B.3).

<sup>112</sup> 1983 Senate Subcommittee Hearing on Smith Guidelines, at 13.

<sup>113</sup> 1983 House Oversight Hearings on Domestic Security Guidelines, at 79 (Smith Guidelines § III.B.1).

<sup>114</sup> Id. Don Edwards, Chairman of the House Subcommittee on Civil and Constitutional Rights, and others continued to urge the passage of restrictive charter legislation for the FBI after the Smith Guidelines were issued. See Letter to The Honorable William H. Webster, April 12, 1983, reprinted in 1983 House Oversight Hearings on Domestic Security Guidelines, at 141-44.

<sup>115</sup> 1983 House Oversight Hearings on Domestic Security Guidelines, at 82 (Smith Guidelines § III.B.4.d).

investigations, leaving the technique available only for general crimes investigations.<sup>116</sup> Under both the Levi and Smith Guidelines, neither informants nor mail covers could be used during preliminary inquiries. The Smith Guidelines extended the duration of preliminary inquiries from 60 to 90 days, permitting extensions by FBI Headquarters upon “a written request and statement of reasons why further investigative steps are warranted when there is no ‘reasonable indication’ of criminal activity.”<sup>117</sup>

The Smith Guidelines cautioned that investigations could not be initiated solely on the basis of an individual’s exercise of First Amendment rights, a restriction that has remained in place for over 20 years and is in effect today. See General Crimes Guidelines § I (General Principles). In addition, the Smith Guidelines instructed agents to consider, in evaluating the use of various law enforcement techniques, the use of “less intrusive means.”<sup>118</sup> With respect to use of the undercover technique, the Smith Guidelines required FBI Headquarters’ approval with notification to the DOJ if the FBI initiated “undisclosed participation in the activities of an organization by an undercover employee or cooperating private individual in a manner that may influence the exercise of rights protected by the First Amendment.”<sup>119</sup>

One key member of Congress observed that the Guidelines were “instrumental in curtailing intelligence abuse by the FBI” and should not be changed “without careful Congressional and public scrutiny to assure that [the Smith Guidelines are] not a retreat.”<sup>120</sup>

The following year, coinciding with the House Subcommittee’s final year of hearings on FBI undercover operations discussed above, the FBI instituted an internal review of undercover operations. On February 8, 1984, the FBI’s Office of Program Evaluation and Audits (OPEA) in the Inspection Division released a study of FBI undercover operations which concluded that the FBI was doing an effective job in undercover

---

<sup>116</sup> Id. at 71 (Smith Guidelines § II.B and III.B). According to a 1976 GAO report, preliminary inquiries were used to open investigations of all black student leaders and in other political intelligence investigations in the 1960s. See General Accounting Office, FBI Domestic Intelligence Operations: Their Purpose and Scope: Issues That Need to be Resolved, GGD-76-50 (Feb. 24, 1976).

<sup>117</sup> 1983 House Oversight Hearings on Domestic Security Guidelines, at 71 (Smith Guidelines § II.B.3).

<sup>118</sup> Id. at 82 (Smith Guidelines § IV.A).

<sup>119</sup> Id. at 83 (Smith Guidelines § IV.B.3).

<sup>120</sup> Leslie Maitland, *Eased F.B.I. Curbs Touch Off Dispute*, The New York Times, May 14, 1983, § 1 (remarks by Rep. Don Edwards, Chairman, Subcommittee on Civil and Constitutional Rights, House Committee on the Judiciary).

investigations in the criminal field. In terms of management controls, the report concluded that the Criminal Undercover Operations Review Committee (CUORC), the Undercover and Special Operations Unit (USOU), and the Undercover Guidelines improved centralized control of undercover activities.<sup>121</sup>

Also during 1983 and 1984, Congress debated a bill which would subject undercover operations to congressional control. The Undercover Operations Act would require that before the FBI could initiate an undercover operation, federal law enforcement agencies would have to establish a factual predicate of “probable cause” or “reasonable suspicion.”<sup>122</sup> Director William Webster did not support the entire bill, arguing that it would not allow agents to effectively perform investigations. Director Webster cited the effectiveness of the Attorney General Guidelines, which set thresholds and guidance for undercover operations.<sup>123</sup> Director Webster also stated that the flexibility in the Guidelines allowed “responses in specific situations which arise in the context of the investigative field,” while adhering to regulatory requirements.<sup>124</sup>

#### **D. The Thornburgh Guidelines – 1989**

In September 1981, the FBI opened a criminal investigation of the Committee in Solidarity with the People of El Salvador, or “CISPES,” a United States-based group that opposed the Reagan Administration’s policies in Central America.<sup>125</sup> According to the FBI, the investigation was opened to determine if CISPES had violated the Foreign Agents

---

<sup>121</sup> The OPEA report, *FBI Undercover Operations in Criminal Matters*, made recommendations to refine the FBI’s undercover training program, improve agent selection, initiate a debriefing program for lengthy undercover operations, improve national coordination of operations, and increase the fiscal flexibility for undercover operations.

<sup>122</sup> See *Undercover Operations Act*. Hearing Before the Senate Subcommittee on Criminal Law of the Senate Committee on the Judiciary, 98th Cong. 9 (1984). The bill was never brought to a vote.

<sup>123</sup> See *id.* at 173-77.

<sup>124</sup> *Id.* at 175-76. With the exception of a number of modifications to the Undercover Guidelines that were made in 1992 by Attorney General William Barr, the Guidelines were not changed again until the May 2002 revisions described *infra* in Chapter Four. The 1992 revisions included changes to the definition of certain “sensitive circumstances,” limited the applicability of the Guidelines to only those cases where an undercover agent was involved, authorized SACs to delegate approval authority to designated ASACs, and allowed SACs to authorize nonsensitive UCOs for up to one year.

<sup>125</sup> Senate Select Committee on Intelligence, 101st Cong., *The FBI and CISPES* 11 (Comm. Print 1989) (hereafter “*The FBI and CISPES*”). At the time of the CISPES investigation, the FBI’s authorities were governed by the Attorney General’s Foreign Counterintelligence Guidelines. *Id.*

Registration Act, 22 U.S.C. § 611-621. The FBI closed the investigation in February 1982, but continued to collect information about CISPES from an informant who claimed that the group was involved in international terrorism. Under the auspices of its Counterterrorism Program, the FBI thereafter opened an international terrorism investigation in March 1983 pursuant to the Foreign Counterintelligence Investigations (FCI) Guidelines, during which it conducted surveillance of CISPES and allied groups. Finding no evidence to support the informant's claims, the FBI closed the investigation in June 1985.

In January 1988, the CISPES investigation was brought to public attention when the Center for Constitutional Rights released material it had obtained under the Freedom of Information Act (FOIA).<sup>126</sup> CISPES later alleged that the FBI investigated the group, its members, and affiliated groups solely because of its political views, and that the investigation violated the First Amendment and the constitutional rights of various individuals and organizations.<sup>127</sup>

After consultations with the Congress in early 1988, FBI Director William S. Sessions ordered an independent inquiry into the FBI's handling of the CISPES investigation to determine if the FBI had broken any laws, violated any Attorney General Guidelines or rules, regulations or policy, or used poor judgment in the course of the investigation. The inquiry also examined whether the requisite evidentiary threshold had been established to initiate the investigation, whether the investigation remained opened for the appropriate period of time, whether DOJ oversight was sufficient, whether the initial informant was reliable, and whether the FBI's practice of "indexing" information obtained from the investigation was proper.<sup>128</sup>

The FBI's May 27, 1988, report concluded that the FBI had conducted an appropriate investigation for the initial period, but that its objectives became overly broad when FBI Headquarters directed all offices to treat each of the estimated 180 chapters of CISPES as subjects of the investigation. The report also concluded that FBI Headquarters and the Dallas Field Office had inadequately supervised the investigation, principally by their failure to conduct a background check of the informant who prompted the investigation, failing to continually ensure that the informant

---

<sup>126</sup> Id. at 15.

<sup>127</sup> Committee in Solidarity With The People of El Salvador (CISPES) v. Sessions, 929 F.2d 742, 743-44 (D.C. Cir. 1991).

<sup>128</sup> General Accounting Office, *International Terrorism: FBI Investigates Domestic Activities to Identify Terrorists*, (hereafter "GAO Report, *International Terrorism: FBI Investigates Domestic Activities to Identify Terrorists*") GAO/GGD-90-112, at 28 (Sept. 7, 1990), available at: <http://161.203.16.4/d22t8/142382.pdf>.



was reliable and accurate, and failing to adequately supervise and direct the informant.<sup>129</sup>

With respect to the Attorney General's FCI Guidelines, the report found 31 separate violations, including:

- conducting inquiries beyond what was permitted without opening an investigation;
- receiving information about individuals' mail without obtaining proper authority; and
- initiating investigations without an adequate evidentiary predicate.<sup>130</sup>

The Senate's Select Committee on Intelligence also investigated the CISPES matter. On September 14, 1988, FBI Director Sessions told the Committee that "the investigation should never have been initiated," but denied that the FBI had acted illegally in conducting the inquiry.<sup>131</sup> Director Sessions notified the Committee that several agents had been disciplined and that internal procedures had been revised to ensure that such errors would not recur.<sup>132</sup>

Although the Senate Committee concluded that the FBI's CISPES investigation did not reflect "significant FBI political or ideological bias," it concluded that its activities "resulted in the investigation of domestic political activities protected by the First Amendment that should not have come under governmental scrutiny."<sup>133</sup> The Committee also stressed the key role FBI policy and, particularly, the Attorney General Guidelines play in constraining the FBI's investigative authorities:

Federal laws do not regulate most of the FBI's standard investigative methods, including photographic and visual surveillance, trash checks, the use of informants and undercover agents, attendance at meetings and infiltration of

---

<sup>129</sup> *The FBI and CISPES* at 58.

<sup>130</sup> *Id.* at 6, 89-91, 101, 120.

<sup>131</sup> *Id.* at 103.

<sup>132</sup> *Id.*

<sup>133</sup> *The FBI and CISPES* at 3, 103. The Committee report that concluded:

"[T]he FBI's international terrorism investigation of CISPES was initiated primarily on the basis of allegations that should not have been considered credible; it was broadened beyond the scope justified even by those allegations; and it continued after the available information had clearly fallen below the standards required by the applicable guidelines."

*Id.* at 1.

groups, interviews of individuals and their employers and associates, and checks of various law enforcement, license, utility, and credit records. Investigations such as the CISPES case using these methods are governed by internal FBI policies and by guidelines issued by the Attorney General. Violations are normally punishable only by internal disciplinary action. The CISPES investigation demonstrated the vital importance of adherence to policies and guidelines that keep the FBI from making unjustified inquiries into political activities and associations.<sup>134</sup>

The controversy surrounding the CISPES investigation ultimately led to the establishment of a DOJ working group which proposed changes to the Attorney General's FCI Guidelines. Those revisions, which became effective in September 1989, provided more guidance to FBI field offices about reporting on international terrorism investigations.<sup>135</sup>

In the wake of the CISPES disclosures, the House Judiciary Committee asked the General Accounting Office (GAO) to review the FBI's international terrorism program. The GAO sampled closed cases and used a questionnaire to develop a profile of international terrorism cases. In its September 1990 report, "International Terrorism: FBI Investigates Domestic Activities to Identify Terrorists," the GAO found that:

- the FBI closed approximately 67 percent of its investigations because it did not develop evidence indicating that the subjects were engaging in international terrorist activities;
- United States citizens and permanent resident aliens were the subject of 38 percent of the 18,144 cases opened during January 1982 – June 1988;
- mosques were among the religious institutions targeted in the 1980s investigations; and
- the FBI monitored First Amendment-related activities in about 11.5 percent of those cases; indexed information about individuals

---

<sup>134</sup> *The FBI and CISPES* at 12.

<sup>135</sup> The Guidelines revisions issued in March 1989 were relatively minor. They clarified that the use in preliminary inquiries of investigative techniques that require approval by a Supervisory Special Agent (SSA) must comply with the Guidelines' provisions that govern investigative techniques generally, authorized criminal intelligence investigations against enterprises engaged in narcotics trafficking, and specified that the use of trap and trace devices and access to stored wire and electronic communications and transactional records must be in accordance with Title 18 of the U.S. Code. The revisions were entitled, "The Attorney General's Guidelines on General Crimes, Racketeering Enterprise and Domestic Security/Terrorism Investigations."

who were not subjects of FBI investigations in about 47.8 percent of the cases; and indexed information about groups which were not subjects of the investigations in about 11.6 percent of the cases.<sup>136</sup>

However, the GAO stated that because it was not afforded access to full case files, it could not determine if the FBI violated First Amendment rights of the individuals and groups which were monitored or if the FBI had the requisite basis to monitor the activities of these individuals and groups. According to the GAO Report, while the FBI declined the opportunity to provide written comments on its report, “GAO discussed the report with FBI officials who generally agreed with the facts.”<sup>137</sup>

In addition to the CISPES inquiry, another informant controversy arose in the late 1980s. After a 3-year investigation by the Department of Labor’s Office of the Inspector General and DOJ into charges of labor fraud by Teamsters President Jackie Presser, the Department of Justice ended the investigation in the summer of 1985. At the time, Presser’s uncle, Allen Friedman, and a Cleveland organized crime leader, John Nardi, Jr., had already been convicted of receiving unauthorized payments while serving as “ghostworkers” for the Teamsters. It later came to light that Presser’s FBI contact agent or “handler,” Robert S. Friedrich, admitted during an internal FBI investigation that Presser had been authorized by the FBI to employ the “no-show” employees.<sup>138</sup>

The decision to drop the Presser investigation prompted a congressional inquiry by the Senate Permanent Subcommittee on Investigations.<sup>139</sup> Following hearings, the Committee staff published a report that focused on whether DOJ was motivated by improper reasons not to prosecute Presser and what problems prompted the declination decision.<sup>140</sup> The Committee staff concluded that DOJ’s decision not to

---

<sup>136</sup> GAO Report, *International Terrorism: FBI Investigates Domestic Activities to Identify Terrorists*, supra n.128, at 3.

We discuss in Chapter Five our concerns about the FBI’s current inability to track the utilization of its broad authorities under Part VI of the General Crimes Guidelines, including its authority to visit public places and attend public events for the purpose of detecting or preventing terrorist activities.

<sup>137</sup> Id. at 5.

<sup>138</sup> *United States v. Friedrich*, 842 F.2d 382, 385 (D.C. Cir. 1988) (affirming suppression of statements made to DOJ attorneys in prosecution for false statements in previous interviews). Friedrich subsequently recanted his admission that the FBI had authorized the “no show” employees. The FBI’s OPR later concluded that Friedrich had concocted the authorization defense after the fact to protect Presser as a valued informant. Id. at 388.

<sup>139</sup> *Senate Subcommittee Hearing on the Jackie Presser Ghostworkers Case*.

<sup>140</sup> *Senate Staff Study on Jackie Presser Investigation*, supra n.74.

prosecute “was based on its evaluation of the impact of the agents’ authorization claims,” but the report did not reach a conclusion as to the evidence that the agents’ authorization statements were untrue.<sup>141</sup> The report noted that the Levi Guidelines made only passing reference to authorized criminal acts by informants or others. Those Guidelines provided that an informant may not participate in criminal activities “except insofar as the FBI determines that such participation is necessary to obtain information needed for purposes of federal prosecution.”<sup>142</sup> The report noted that the Civiletti Guidelines, by contrast, addressed the issue in some detail, requiring a written determination by an FBI supervisor that:

- (a) the conduct is necessary to obtain information or evidence for paramount prosecutive purposes, to establish and maintain credibility or cover with persons associated with criminal activity under investigation, or to prevent or avoid the danger of death or serious bodily injury; and
- (b) this need outweighs the seriousness of the conduct involved.<sup>143</sup>

Moreover, the Civiletti Guidelines required SAC approval for participation in “extraordinary” illegal activities, defined as those actions presenting a significant risk of “severe financial loss to a victim.” DOJ stated that the basic agreement with Presser predated the Levi Guidelines and because there was no retroactive requirement to report either pre- or post-Guidelines authorization of illegal informant activity, there was no violation of DOJ or FBI policy embodied in the Guidelines.

The Committee staff also examined the role DOJ attorneys played in questioning Presser’s handlers and their supervisors about Presser’s informant relationship. Although DOJ was not at the time required either to approve or monitor the types of activities Presser was involved in, the Senate staff report expressed concern that the DOJ was not exercising adequate oversight of the FBI in informant matters.

### **E. The Reno Guidelines – 2001**

On February 26, 1993, terrorists drove a truck loaded with explosives into a garage at the World Trade Center Tower in Manhattan, resulting in the death of 6 and injuring more than 1,000 people. On April 19, 1995, a massive fertilizer bomb destroyed the Alfred P. Murrah federal building in Oklahoma City, killing 168 people, including 19 children, and wounding

---

<sup>141</sup> Id. at 87.

<sup>142</sup> Id. at 101 (internal quotes omitted).

<sup>143</sup> Id. (citing the Civiletti Informant Guidelines).

674 others. The terrorist attacks prompted renewed congressional concerns about the adequacy of the FBI's tools to prevent and detect terrorism. In 1995, a Subcommittee of the House Judiciary Committee held a hearing on terrorist threats.<sup>144</sup> In response to a suggestion by several lawmakers to rewrite the Attorney General Guidelines addressing domestic security investigations and terrorism, FBI Director Louis Freeh testified that the current Guidelines afforded the authorities and flexibilities needed to investigate terrorist groups.<sup>145</sup> FBI Director Freeh also testified that prior to the Oklahoma City bombing, he and Attorney General Reno discussed the "necessity of reviewing with an objective of changing the interpretation of the guideline to give [the FBI] not broader authority, but more confidence to use the authority already articulated in the guidelines."<sup>146</sup>

On November 1, 1995, the FBI circulated to each of its field offices the reinterpretation of the domestic security/terrorism investigations and preliminary inquiry provisions of the Attorney General's Guidelines on General Crimes, Racketeering Enterprise and Domestic Security/Terrorism Investigations issued in March 1989, restating that the "reasonable indication" standard for opening a full investigation is "substantially lower than probable cause" and that a preliminary investigation could be opened on a lesser showing.<sup>147</sup> With respect to the initiation of domestic security investigations, the 1989 version of the Guidelines provided:

A domestic security/terrorism investigation may be initiated when the facts or circumstances reasonably indicate that two or more persons are engaged in an enterprise for the purpose of furthering political or social goals . . . through activities that involve force or violence and a violation of the criminal laws of the United States.

The FBI's practice had been to construe the "reasonable indication" standard as requiring evidence of an imminent violation of federal law. After the Oklahoma City bombing, the Guidelines were reinterpreted to justify the investigation of domestic groups that advocate violence provided that they have the ability to carry out violent acts that may violate federal law.<sup>148</sup>

---

<sup>144</sup> *Combating Domestic Terrorism*: Hearing before Subcommittee on Crime of the House Judiciary Committee, 104th Cong. (1996) (hereafter "*1995 House Subcommittee Hearing*").

<sup>145</sup> *1995 House Subcommittee Hearing*, at 13.

<sup>146</sup> *Id.* at 27.

<sup>147</sup> *Advice to Field Offices Regarding Domestic Security/Terrorism Investigations and Preliminary Inquiries Under the Attorney General's Guidelines on General Crimes, Racketeering and Domestic Security/Terrorism Investigations*, November 1, 1995.

<sup>148</sup> *Id.*

The most extensive revisions to the Confidential Informant Guidelines occurred in January 2001, just before the end of Attorney General Reno's tenure. The Confidential Informant Guidelines had not been modified since Attorney General Civiletti issued the second set of Informant Guidelines in December 1980.

The Reno review of the Guidelines was spurred in large part by the FBI Boston Field Office's mishandling of informants James "Whitey" Bulger and Stephen "The Rifleman" Flemmi. In 1995, the Government indicted Bulger and Flemmi on multiple charges of racketeering, including acts of extortion, murder, bribery, loan sharking, and obstruction of justice.<sup>149</sup> Bulger was tipped off to his pending arrest and remains a fugitive on the FBI's Ten Most Wanted List. Flemmi allegedly was tipped off but was arrested, later pled guilty, and is in prison serving a life sentence. The FBI's relationship with both Bulger and Flemmi was not acknowledged by the Government until court proceedings following their initial indictment.<sup>150</sup>

We provide in Chapter Three a detailed description of the FBI's association with Bulger and Flemmi. Evidence presented during pretrial hearings in the Government's case against Flemmi revealed misconduct and criminal activity by the FBI agents who handled the two mobsters. For example, agents accepted money and exchanged presents with them, hosted them for dinners, and provided intelligence on planned law enforcement activity targeted at their criminal operations, including identifying the location of electronic surveillance and the identities of informants. In one case, agents told Bulger and Flemmi that another FBI informant had implicated them in a murder. The informant was killed as he exited a restaurant in South Boston approximately one week after his request to be placed in the Government's Witness Protection Program was denied. In another matter, agents intervened with prosecutors and succeeded in having Bulger and Flemmi omitted from upcoming indictments. Although other law enforcement agencies, such as the Massachusetts State Police and the federal Drug Enforcement Administration, had succeeded in charging other Winter Hill Gang members, Bulger and Flemmi's ability to evade prosecution for so many years raised suspicions that they were being protected by the FBI.

Following lengthy internal investigations by DOJ and FBI, charges were brought against two FBI agents who handled informants in the Winter Hill Gang. One FBI Special Agent, John Connolly, the principal handler of Bulger and Flemmi, was convicted in April 2002 of multiple counts of

---

<sup>149</sup> United States v. Salemme, 91 F. Supp. 2d 141 (D. Mass. 1999).

<sup>150</sup> Id. at 303.

obstruction of justice and sentenced to 10 years in prison.<sup>151</sup> The other Special Agent, H. Paul Rico, died in jail prior to his trial on murder conspiracy charges.<sup>152</sup> In addition, approximately 20 civil suits have been brought against the FBI and several of its former agents based on the FBI's handling of Bulger and Flemmi. Many of these suits include claims for wrongful death brought by the families of victims who were murdered by Bulger and Flemmi.

As a result of the Bulger-Flemmi episode and other problem cases involving the FBI's operation of informants, DOJ formed a working group in 1999 to recommend revisions to the Confidential Informant Guidelines. The working group was initially chaired by Mary Jo White, then U.S. Attorney for the Southern District of New York, and later by Jonathan D. Schwartz, Principal Associate Deputy Attorney General, and included representatives of DOJ investigative agencies and federal prosecutors, including FBI Director Mueller, who was then serving as U.S. Attorney for the Northern District of California. The group met regularly for two years and submitted its recommended changes to Attorney General Reno.

In January 2001, DOJ issued revised Informant Guidelines superseding the 1980 Civiletti Guidelines. The changes included the following provisions:

- prohibiting federal prosecuting offices in specified circumstances from withholding informant information from the Department of Justice;
- prohibiting JLEAs from making promises of immunity to informants;
- establishing the Confidential Informant Review Committee to approve and monitor informants who are high level or long-term, or who are under the obligation of privilege or confidentiality or affiliated with the media;
- adding greater detail to informant instructions and requiring that several of them read verbatim to informants; and
- imposing notification and information-sharing requirements on JLEAs, such as the requirement to notify federal prosecutors in circumstances when an informant is the target of a federal investigation.<sup>153</sup>

---

<sup>151</sup> United States v. Connolly, 341 F.3d 16, 21 (1<sup>st</sup> Cir. 2003).

<sup>152</sup> J.M. Lawrence, *At 78, Rico Dies Under Guard: Former G-Man Was To Be Tried for Murder*, Boston Herald, Jan. 18, 2004.

<sup>153</sup> See Department of Justice Guidelines Regarding the Use of Confidential Informants (January 8, 2001), available at: <http://www.usdoj.gov/ag/readingroom/ciguidelines.htm>. (continued)

Both the Informant Guidelines and Domestic Security Guidelines remained in place without further revision until the events of September 11, 2001, prompted the reexamination of the existing Guidelines which led to issuance of the revised Guidelines on May 30, 2002.

#### **IV. Conclusion**

Several themes echo throughout the history of the evolution of the Attorney General's Investigative Guidelines that we found to be instructive in conducting this review.

First, Attorneys General and FBI leadership have uniformly agreed that the Attorney General Guidelines are necessary and desirable, and they have referred to the FBI's adherence to the Attorney General Guidelines as the reason why the FBI should not be subjected to a general legislative charter or to statutory control over the exercise of some of its most intrusive authorities.

Second, problems in the FBI's handling of informants or conducting undercover operations have occurred when field supervisors or FBI Headquarters, or both, failed to exercise appropriate oversight of field activities in accordance with the Guidelines.

Third, historically, the partnership between the FBI and DOJ in making key operational and oversight decisions has promoted adherence to the Attorney General Guidelines and allowed the Department to exercise critical judgments regarding sensitive FBI investigative activities, particularly with respect to its use of confidential informants and undercover operations.

Fourth, oversight by Congress has identified Guidelines violations and gaps in the coverage of the Guidelines.

Below we provide a timeline identifying the Attorney General Guidelines issued between 1976 and 2002, and the significant historical events associated with the revisions.

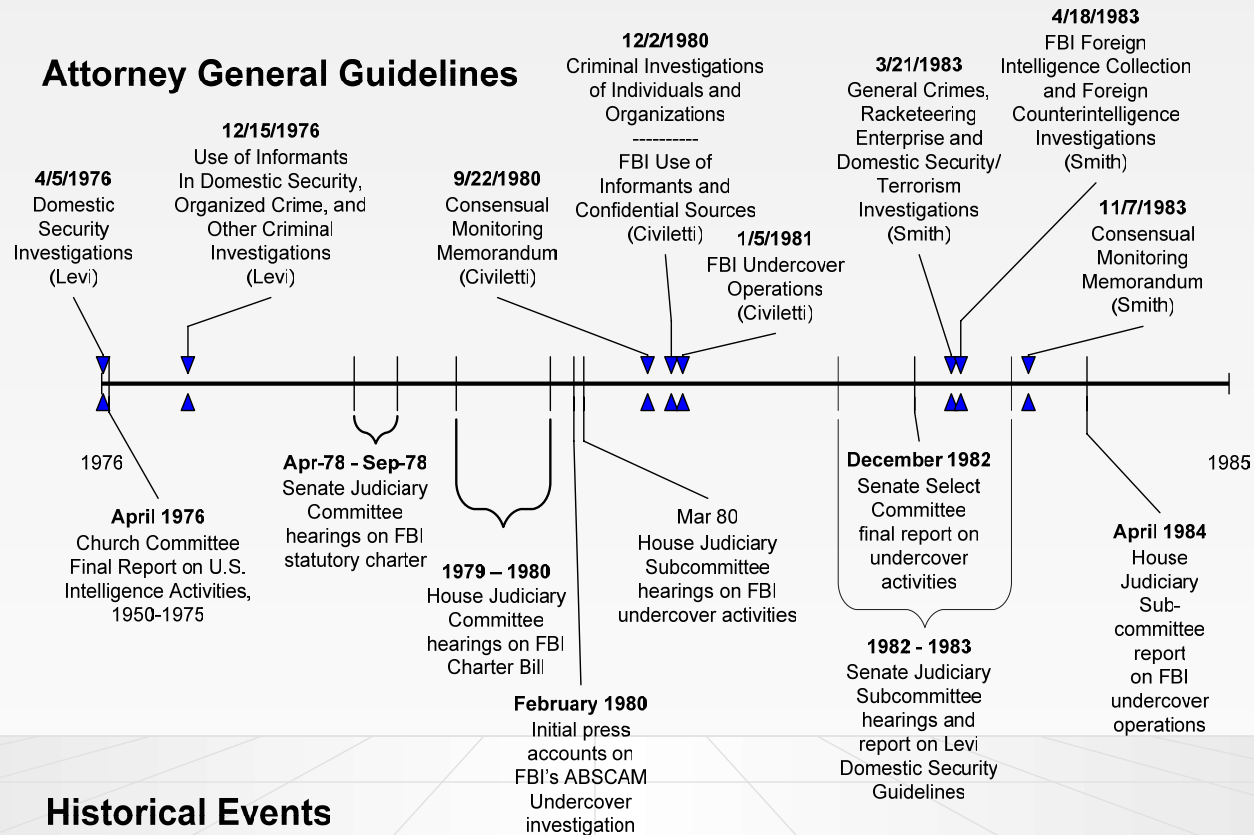
In the balance of our report, we present our findings with respect to the FBI's compliance with the May 2002 revisions to the Guidelines, mindful of their historical context and the lessons learned over the last 30 years.

---

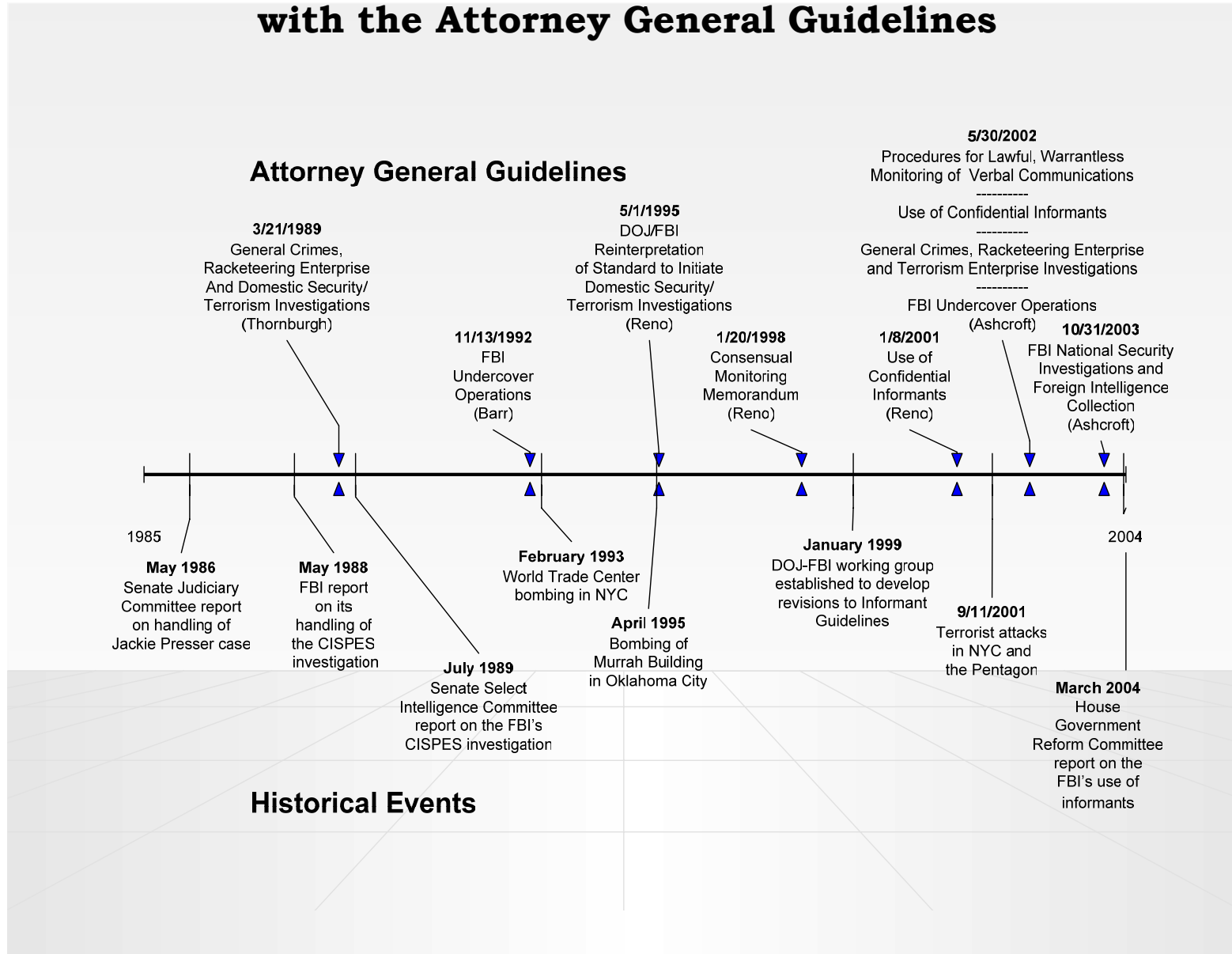
The House Committee on Government Reform held hearings in 2001 and 2002 on the FBI's use of informants in New England, leading to issuance of a report in 2004 entitled, *Everything Secret Degenerates: The FBI's Use of Murderers as Informants*, H. Rep. No. 108-414, 108th Cong. (2004), available at: <http://www.gpo.gov/hreports/108-414.html>. We address the Boston informant matters in the next chapter.



# Timeline of Events Associated with the Attorney General Guidelines



# Timeline of Events Associated with the Attorney General Guidelines



[BLANK PAGE]

## **CHAPTER THREE**

### **THE ATTORNEY GENERAL'S GUIDELINES REGARDING THE USE OF CONFIDENTIAL INFORMANTS**

In this chapter we discuss the role of confidential informants in FBI investigations and the rewards and risks associated with their operation. We also describe the requirements of the Confidential Informant Guidelines and the May 2002 revisions to the Guidelines. We then describe the results of our compliance review of informant files in 12 FBI field offices. Finally, we provide our analysis and recommendations based on those findings, our surveys and interviews, and the results of more than 40 FBI Inspection Division audits of field office Criminal Informant Programs.

#### **I. Role of Confidential Informants**

According to the Confidential Informant Guidelines, a confidential informant or "CI" is "any individual who provides useful and credible information to a Justice Law Enforcement Agency (JLEA) regarding felonious criminal activities and from whom the JLEA expects or intends to obtain additional useful and credible information regarding such activities in the future."<sup>154</sup> The Guidelines do not apply to the use of confidential informants in foreign intelligence or foreign counterintelligence investigations or to informants operating outside the United States in connection with extraterritorial criminal investigations (unless the informant is likely to be called to testify in a domestic case).<sup>155</sup>

A confidential informant differs from two other categories of sources. "Cooperating witnesses," or "CWs," differ from CIs in that CWs agree to testify in legal proceedings and typically have written agreements with the Department of Justice (DOJ) (usually with an Assistant U.S. Attorney) that spell out their obligations and their expectations of future judicial or prosecutive consideration. The FBI must obtain the concurrence of the U.S. Attorney's Office with regard to all material aspects of their use by the

---

<sup>154</sup> CI Guidelines § I.B.6 at B-8. The full text of the Attorney General's Guidelines Regarding the Use of Confidential Informants is attached at Appendix B.

<sup>155</sup> CI Guidelines § I.A.6 at B-7. Sources used in foreign intelligence or foreign counterintelligence investigations are operated pursuant to the partially classified Attorney General's Guidelines for National Security Investigations and Foreign Intelligence Collection (NSI Guidelines). The unclassified version is available at: <http://www.usdoj.gov/olp/nsiguideines.pdf>. Informants operated outside the United States in connection with extraterritorial criminal investigations are operated pursuant to a separate set of Attorney General Guidelines, which are classified.

JLEA.<sup>156</sup> “Assets” are sources who assist the FBI in international terrorism, foreign intelligence, or foreign counterintelligence investigations.

Persons who provide information to the FBI but do not fall into one of these specific classifications are referred to generally as “sources of information.” A source provides information to a law enforcement agency only as a result of legitimate routine access to information or records. Unlike what is often the case with regard to CIs and CWs, a source does not collect information by means of criminal association with the subjects of an investigation. Under the Guidelines, a source must provide information in a manner consistent with applicable law.<sup>157</sup>

Confidential informants are often uniquely situated to assist the FBI in its most sensitive investigations. They may be involved in criminal activities or enterprises themselves, may be recruited by the FBI because of their access and status, and, since they will not testify in court, usually can preserve their anonymity.

According to the FBI’s Manual of Investigative Operations and Guidelines (MIOG), CIs are classified in each of the following categories: Organized Crime, General Criminal, Domestic Terrorism, White Collar Crime, Confidential Source, Drugs, International Terrorism, Civil Rights, National Infrastructure Protection/Computer Intrusion Program, Cyber Crime, and Major Theft and Violent Gangs.<sup>158</sup>

## **II. The Benefits and Risks of Using Confidential Informants in FBI Investigations**

Since the inception of the FBI in 1908, informants have played major roles in the investigation and prosecution of a wide variety of federal crimes.<sup>159</sup> The FBI’s Top Echelon Criminal Informant Program was established in 1961 when FBI Director J. Edgar Hoover instructed all Special Agents in Charge (SACs) to “develop particularly qualified, live sources within the upper echelon of the organized hoodlum element who will be capable of furnishing the quality information” needed to attack

---

<sup>156</sup> CI Guidelines § I.B.7 at B-8.

<sup>157</sup> CI Guidelines § I.B.8 at B-9.

<sup>158</sup> MIOG § 137–3.

<sup>159</sup> For a history of the FBI’s informant programs in New England from the 1960s through the mid-1990s, see 21st Century Guide to FBI Informants, Congressional Investigation and Report on the Use of Murderers as Informants, Witness Protection, Federal Bureau of Investigation Memos and Exhibits, Top Echelon Informants, James “Whitey” Bulger, J. Edgar Hoover (CD-ROM) (GPO 2004).

organized crime.<sup>160</sup> In 1978, the FBI replaced that program with the Criminal Informant Program. Its mission is to develop a cadre of informants who can assist the FBI's investigation of federal crimes and criminal enterprises. Informants have become integral to the success of many FBI investigations of organized crime, public corruption, the drug trade, counterterrorism, and other initiatives.

Directors of the FBI frequently make reference to the value of informants while acknowledging that they present difficult challenges. In a June 1978 article, Director William Webster stated:

Not many people know very much about informants: and to many people, it's a queasy area. People are not comfortable with informants. There is a tradition against snitching in this country.

However, the informant is THE with a capital "T" THE most effective tool in law enforcement today – state, local, or federal. We must accept that and deal with it.

\* \* \*

We provide close supervision in the field at the special agent level. We have field and headquarters evaluation of what is going on in respect to our informants. We have inspectors . . . who check each field office to be sure there is compliance with our regulations with respect to the use of informants. *And we have the attorney general's guidelines on when, and under what circumstances, we may use informants, and they are scrupulously observed.*<sup>161</sup> [emphasis added]

When we asked Director Mueller about the value of confidential informants today, he stated:

Human sources are vitally important to our success against terrorists and criminals. They often give us critical intelligence and information we could not obtain in other ways, opening a window into our adversaries' plans and capabilities. Human sources can mean the difference between the FBI preventing an act of terrorism or crime, or reacting to an incident after the fact.

---

<sup>160</sup> House Committee on Government Reform, *Everything Secret Degenerates: The FBI's Use of Murderers as Informants*, 3<sup>rd</sup> Report, H.R. Rep. No. 108-414 at 454 (2004), also available at: <http://www.gov/hreports/108-414.html>.

<sup>161</sup> Webster, *The Director: Why the FBI Needs Undercover Snoops*, Los Angeles Herald Examiner, June 2, 1978, at A-21.

Since the May 2002 revisions to the Investigative Guidelines were issued, the FBI has operated up to [SENSITIVE INFORMATION REDACTED] confidential informants at any one time. Larger field offices may simultaneously operate as many as [SENSITIVE INFORMATION REDACTED] informants, while smaller offices [SENSITIVE INFORMATION REDACTED]. According to the FBI's Human Intelligence Unit (HIU), as of April 30, 2005, the FBI was operating among its informants:

- no more than [SENSITIVE INFORMATION REDACTED] “high level” confidential informants, defined as those “who are part of the senior leadership of an enterprise that has a national or international sphere of activities” or “high significance to the [FBI's] objectives, even if the enterprise's sphere of activities is local or regional;”<sup>162</sup>
- approximately [SENSITIVE INFORMATION REDACTED] “long-term” confidential informants, defined as those who have been registered for more than 6 consecutive years;<sup>163</sup> and
- [SENSITIVE INFORMATION REDACTED] “privileged” informants (e.g., attorneys, clergy, or physicians) or media-affiliated informants.

The FBI tracks the productivity of its CIs by aggregating their “statistical accomplishments,” i.e., the number of indictments, convictions, search warrants, Title III applications, and other contributions to investigative objectives for which the CI is credited.<sup>164</sup>

Many, if not most, of the successes of the Criminal Informant Program are not widely known, because unlike the case with a cooperating witness who typically testifies at trial, an informant's identity rarely becomes public. In the course of this review, the FBI provided the following illustrations of cases in which FBI informants played a pivotal role in recent prosecutions.

- A 3-year grand jury investigation into organized crime, drug trafficking, and illegal gambling resulted in the dismantlement of a criminal enterprise and the conviction of a career criminal and five of his criminal associates on racketeering, drug trafficking, money laundering, and illegal gambling charges. Seventeen RICO predicate crimes were charged in the indictment, including

---

<sup>162</sup> CI Guidelines § I.B.9 at B-9. Officials in the FBI's Human Intelligence Unit explained that when “high echelon” informants were eliminated in the revised Guidelines issued by the Attorney General in January 2001 and “high level” informants were introduced as a new category, few FBI informants qualified under the new definition.

<sup>163</sup> CI Guidelines § II.A.3.a at B-16.

<sup>164</sup> Statistical accomplishments are entered on standard FBI Form FD-209. See MIOG § 137-16(5).

extortion, witness tampering, obstruction of justice, and mail fraud. The prosecution also led to the forfeiture of \$500,000. The success of the grand jury investigation and the resulting prosecution was attributed in significant part to leads and information provided by FBI confidential informants.

- FBI confidential informants provided information to investigators which permitted them to identify appropriate targets for the investigation of three violent gangs in a northeastern city. The investigation resulted in 35 cases involving charges against a total of 54 gang members over a 5-year period. According to the FBI, the succession of prosecutions was instrumental in bringing about a dramatic reduction in acts of violence in that city.
- An FBI confidential informant played a crucial role in a 2-year undercover investigation by participating in over 1,000 consensually monitored conversations. The consensual monitorings lead to the indictment of four Houston City Council members, a Houston Port Authority Commissioner, and a lobbyist. The confidential informant, later a cooperating witness, testified in three lengthy trials that resulted in the conviction of a city council member and the Port Authority Commissioner.
- 2 Yemeni citizens, Mohammed Al Hasan Al-Moayad and Mohammed Mohsen Yahya Zayed, were arrested in January 2003 in Frankfurt, Germany based on criminal complaints issued in Brooklyn, New York. They were charged with conspiring to provide material support to the Al Qaeda and Hamas terrorist groups. According to the complaint, an FBI confidential informant met with Al-Moayad in January 2002 and was told by Al-Moayad in subsequent conversations that he regularly provided money to support Mujahideen fighters in Afghanistan, Chechnya, and Kashmir. According to the confidential informant, Al-Moayad also stated during this and other conversations that he had supplied Al Qaeda with arms and communication equipment in the past, delivering more than \$20 million to Al Qaeda prior to September 11, 2001. Al-Moayad also boasted of several meetings with Usama bin Laden and said he personally delivered the \$20 million to bin Laden with much of the money coming from contributors in the United States, including Brooklyn.<sup>165</sup>

---

<sup>165</sup> Department of Justice Press Release, March 4, 2003, available at: [http://www.usdoj.gov/opa/pr/2003/March/03\\_ag\\_134.htm](http://www.usdoj.gov/opa/pr/2003/March/03_ag_134.htm). Confidential informants are used by the FBI in a variety of domestic and international terrorism investigations where (continued)



Offsetting the many benefits that result from the use of confidential informants are the significant risks their use introduces for the United States Government. As Phillip B. Heymann, the former Deputy Attorney General and Assistant Attorney General in charge of the Criminal Division, observed:

[S]ome informants are responsible citizens who report suspected criminal activities without any hope of return. In the middle, other informants live in the midst of the criminal underworld and inform largely for cash. Still others, at the other pole, are charged with serious crimes and cooperate with law enforcement officials in return for the hope or promise of leniency.<sup>166</sup>

In some past cases, the FBI's use of informants violated the Informant Guidelines, the MIOG, or federal or state law, with serious adverse consequences to prosecutions, third parties, agents' careers, and the FBI's reputation. We describe below cases in which agents engaged in criminal or administrative misconduct in handling informants, informants committed unauthorized crimes and asserted claims and defenses against the government based on their informant status, and third parties initiated litigation against the government claiming injuries arising from the conduct of informants.

**FBI Misconduct Relating to Informants.** Serious FBI misconduct relating to the handling of informants can result in criminal prosecution. For example, in June 2002 John J. Connolly, Jr., who served as a Special Agent in the FBI's Boston office and handled complex organized crime investigations, was convicted following a jury trial of racketeering, obstruction of justice, and making false statements arising from his mishandling of FBI informants Whitey Bulger and Stephen Flemmi.<sup>167</sup> We describe the Bulger-Flemmi matter in CI Case Study 1, below.

---

the investigative objective is a criminal prosecution. In March 2005, both defendants were convicted of conspiring to provide material support to the Al Qaeda and Hamas terrorist groups.

<sup>166</sup> *FBI Statutory Charter*: Hearings Before the Subcommittee on Administrative Practice & Procedure of the Senate Committee on the Judiciary 95<sup>th</sup> Cong. 40 (1978) (Testimony of Philip B. Heymann, Assistant Attorney General, Criminal Division, Department of Justice). The complex relationship between the FBI and its informants is also described in *United States v. Doe*, No. 96 Cr. 749 (JG), 1999 WL 243627 (E.D.N.Y. Apr. 1, 1999).

<sup>167</sup> *United States v. Connolly*, 341 F.3d 16 (1<sup>st</sup> Cir. 2002).

Misconduct related to an informant can also result in administrative sanctions for the agent. In one recent case, an FBI Special Agent resigned while under investigation by the FBI's Office of Professional Responsibility (OPR) for having an inappropriate relationship with an informant and failing to be truthful during the ensuing OPR inquiry. OPR determined that among the factors aggravating the misconduct were the agent's failure to document his contacts with the informant, misuse of the agent's official position by assisting the informant's relative with legal and business matters, and the agent's effort to make the relative an "informal informant." In a 1999 case, an FBI agent was suspended for having an inappropriate relationship with a prospective informant, failing to properly document the individual as a CI, and failing to arrange for the arrest of the CI source after discovering there was an outstanding warrant for the source's arrest.<sup>168</sup>

**Criminal Prosecution of Informants.** Federal criminal prosecution of FBI informants can result from the informant's unauthorized criminal conduct or from situations in which the informant exceeds the scope of his authority to engage in "otherwise illegal activity" under the Informant Guidelines. In such cases, the informants often claim in defense that the government authorized or immunized their crimes. For example, in *United States v. Hilton*, 257 F.3d 50 (1<sup>st</sup> Cir. 2001), an informant who was prosecuted for possession of child pornography claimed "entrapment by estoppel," asserting that he reasonably believed he was lawfully permitted to download the pornography as long as he sent it on to law enforcement. The court rejected the defense, ruling that while the FBI contact agent had initially approved the defendant's possession of child pornography, the agent later clarified that "the FBI no longer required his assistance and that possession of child pornography was illegal." *Id.* at 56.

One of the more notorious of such cases is the Bulger-Flemmi matter described below in Confidential Informant Case Study 1. Stephen "the Rifleman" Flemmi and James "Whitey" Bulger, were "Top Echelon" confidential informants for the FBI's Boston office. Along with four co-defendants, they were indicted for racketeering, conspiracy, extortion, and bookmaking charges in 1995. Bulger was tipped off by FBI Special Agent

---

<sup>168</sup> *Id.* An internal report by the FBI's Behavioral Sciences & Law Enforcement Ethics Unit in June 2000 catalogued instances in which FBI agents were fired between 1986 and 1999 due to misconduct of various sorts, including cases involving informant-related misconduct. Among the types of misconduct chronicled in the report were sexual relationships between informants and agents and improper disclosure of information to informants. See Deshazor, *Behavioral and Ethical Trends Analysis (BETA): A Summary of Dismissals of FBI Agents and Egregious Behavior*. See also Chapter Seven, which catalogues instances in which mishandling of informants may become a misconduct issue to be addressed by FBI OPR.

John Connolly to his pending arrest. Bulger evaded law enforcement and remains a fugitive. As the following case study describes, when the government prosecuted Flemmi, he claimed that the FBI had authorized the crimes for which he was indicted.

Similarly, an “authorization” defense arose in the prosecution of Jackie Presser, a Teamsters official who was charged with embezzling over \$700,000 in union funds. Presser asserted as an affirmative defense that he had been an FBI informant for 10 years and was authorized by the FBI to hire “phantom” or “no-show” employees. When Presser’s FBI handlers testified under oath, they confirmed the assertions supporting Presser’s defense. The government thereafter declined to prosecute Presser and consented to vacating earlier convictions of two phantom employees. A report by the staff of the Senate’s Permanent Subcommittee on Investigations, one of three committees that investigated the matter, concluded that DOJ had failed to adequately monitor the FBI’s informant system and should have required the FBI to disclose information about its informants.<sup>169</sup>

---

<sup>169</sup> See Staff Study in *Overview of Government’s Handling of Jackie Presser Investigation*: Hearing Before the Permanent Subcommittee on Investigations of the Senate Government Affairs Committee, 99th Cong. 75 (1986) (hereafter “*Senate Staff Study*”).

The DOJ Office of Professional Responsibility (DOJ OPR) concluded that Presser had no FBI authorization to commit illegal activity. DOJ OPR concluded that the authorization story was invented after the fact to protect a highly valued informant, even though Presser was deactivated when he became Teamster president in 1983. DOJ attorneys also concluded that neither the Levi nor the Civiletti Guidelines were in place when Presser’s informant relationship began, and, once the Guidelines were issued, there was no retroactive application to informants already serving. *Senate Staff Study* at 107-08.

One of Presser’s FBI handlers, Robert Friedrich, was later indicted for making false statements to internal investigators about his role in Presser’s purported authorization by the FBI to engage in the scheme. The district court granted Friedrich’s motion to suppress all statements made in the interviews on the grounds that they were inadmissible under the Fifth Amendment. The court of appeals affirmed the district court’s ruling. *United States v. Friedrich*, 842 F.2d 382 (D.C. Cir. 1988). No additional charges were brought.

**Confidential Informant Case Study 1**  
**FBI Informants James J. “Whitey” Bulger and**  
**Stephen J. “The Rifleman” Flemmi**

FBI agent John Connolly, Jr. was sentenced in September 2002 to 10 years in prison for racketeering, obstruction of justice, and making false statements to investigators – all stemming from his handling of two FBI informants, James J. “Whitey” Bulger and Stephen J. “The Rifleman” Flemmi, leaders of South Boston’s Winter Hill Gang.

Bulger, Flemmi, and other defendants were indicted in January 1995 and charged with multiple counts of racketeering, extortion, and other crimes. Four days after Flemmi’s arrest and the day before his indictment, the Special Agent in Charge (SAC) of the FBI’s Boston field office notified the U.S. Attorney in the District of Massachusetts for the first time that Bulger and Flemmi had been informants for the FBI for much of the period covered by the indictment. In August 1995, the government disclosed to the presiding magistrate that Flemmi had been a confidential informant for the FBI and that Flemmi’s informant file was being reviewed by senior DOJ officials to determine whether it contained any exculpatory material discoverable under *Brady v. Maryland*, 373 U.S. 83 (1963), and its progeny.

In a 10-month evidentiary hearing that concluded in October 1998, after which the court denied Flemmi’s motion to dismiss the indictment, a federal judge heard evidence produced in response to Flemmi’s claim that the indictment against him should be dismissed based on “outrageous government misconduct,” including a claim that the government promised that he and Bulger would be protected from prosecution as long as they continued to cooperate with the FBI about La Cosa Nostra. The judge heard evidence that Connolly and FBI Supervisory Special Agent John Morris became increasingly close to their informants and had filed false reports of information purportedly provided to them by the informants, ignored evidence that the informants were extorting others, caused the submission of false and misleading applications for electronic surveillance, and disclosed other confidential law enforcement information to them. Among the district court’s findings of fact in its 661-page opinion was a condemnation of the FBI’s failure to follow the Informant Guidelines. The court found that:

- the informants’ handler and supervisors failed to fully inform the FBI Director as to why Bulger and Flemmi had been closed as FBI informants;
- Flemmi’s FBI handler failed to tell Flemmi that he was no longer an active FBI informant; during the 3-year period when he was administratively closed, the handler had over 40 contacts with him;
- contrary to FBI policy requiring the SAC to consult personally with the U.S. Attorney as to whether to authorize extraordinary criminal activity involving a “serious risk of violence” and to review all such criminal activity at least every 90 days, the SAC delegated this responsibility to the informant’s handler and his immediate supervisor;

- the FBI “ignored the essential point of the Attorney General’s Guidelines, which required consultation with the Assistant Attorney General for the Criminal Division when the FBI learns that an informant has engaged in criminal activity but wishes to continue to utilize the informant rather than share the pertinent information concerning the illegal activity with another law enforcement agency;” and
- an Assistant Special Agent in Charge in the Boston field office only considered the informant’s productivity and failed to weigh critical factors in considering the informant’s suitability, including the nature of the matter under investigation and the importance of the information being furnished as compared to the seriousness of past and contemporaneous criminal activity of which the informant may be suspected, or how closely the FBI would be able to monitor his activities acting on behalf of the FBI.

91 F. Supp. 2d at 201, 211, 216, 233, 249.

The government took an interlocutory appeal of the district court’s ruling that the FBI had made an enforceable promise of immunity with respect to the electronic surveillance evidence. The First Circuit reversed, holding that: (1) FBI agents lack authority to promise immunity to informants, and absent such authority, any promise made to Flemmi was unenforceable; (2) no prosecutor ratified the agents’ promise of immunity to Flemmi; (3) Flemmi’s reliance on a promise of immunity did not warrant suppression of evidence; and (4) any promise of immunity did not render Flemmi’s statements in connection with the surveillance involuntary. *United States v. Flemmi*, 225 F.3d 78 (1<sup>st</sup> Cir. 2000).

In December 1999, a grand jury convened by a special DOJ Task Force returned a RICO indictment against Connolly charging him with protecting Bulger and Flemmi through a pattern of obstruction of justice, including leaking to Bulger and Flemmi the names of several cooperating individuals who were later killed. Flemmi was also charged with racketeering, obstruction of justice, and conspiracy in the same indictment along with Bulger, against whom charges were dropped due to RICO Double Jeopardy concerns. In September 2001, Bulger and Flemmi were charged in a new indictment with committing 19 and 10 murders, respectively, and with conspiratorial liability for a total of 21 murders, all committed while they were providing information to the FBI. Flemmi pled guilty to the charges in the Connolly indictment at the same time he pled guilty in the new case. Connolly was tried and convicted in April 2002, the jury finding him guilty of multiple acts of obstruction of justice, including tipping Bulger to the 1995 indictment so he could flee. However, the jury acquitted Connolly on several of the racketeering acts, including those relating to the leaks of the identities of cooperating individuals leading to their deaths. Connolly received a 10-year sentence, which he is currently serving and which was upheld on appeal. On May 4, 2005, Connolly was indicted in Florida for first-degree murder and conspiring with Bulger and Flemmi to kill John Callahan, a Florida businessman who was a financial adviser to the Winter Hill Gang.

In addition, the Tulsa District Attorney’s Office charged another retired FBI agent, H. Paul Rico, who had been Flemmi’s original handler, with aiding and abetting murder. Rico died of natural causes at age 78 while awaiting trial.

Bulger remains a fugitive and is on the FBI’s Ten Most Wanted List.

**Civil Litigation Based on Claims by Informants and Third Parties.** By their terms, none of the Investigative Guidelines creates enforceable rights by CIs or anyone else. Specifically, the Informant Guidelines state:

Nothing in these Guidelines is intended to create or does create an enforceable legal right or private right of action by a CI or any other person.

CI Guidelines, § I.H. Despite this statement, private litigants – including confidential informants – have advanced alternative theories of liability against the United States, its law enforcement agencies, and individual agents and prosecutors based on informant or FBI misconduct, or some combination of the two. For example, the following types of claims have been litigated:

- *Manning v. Miller*, 355 F.3d 1028 (7<sup>th</sup> Cir. 2004), in which the court affirmed the denial of summary judgment requested by two FBI agents in a *Bivens* action where an informant convicted of murder and kidnapping claimed that FBI agents had framed him. In January 2005, a jury awarded a \$6.6 million judgment in favor of the informant.
- *Perri v. United States*, 53 Fed. Cl. 381 (2002), in which a former FBI informant claimed unsuccessfully that the United States breached a promise to pay him 25 percent of any sums forfeited in an investigation in which he assisted.
- *McIntyre v. United States*, 254 F. Supp. 2d 183 (D. Mass. 2003), and *Castucci Estate*, 311 F. Supp. 2d 184 (D. Mass. 2004), examples of a group of approximately 20 cases in the District of Massachusetts seeking damages for the actions of FBI informants Whitey Bulger and Stephen Flemmi alleging that murder, extortion, and other crimes of violence were committed at FBI direction or acquiescence.

**Other Informant Issues Arising During Federal Prosecutions.** Since the January 2001 revisions to the Confidential Informant Guidelines, critical decisions about the registration and oversight of certain types of confidential informants are made jointly by the FBI and the Department of Justice. Other developments concerning confidential informants and certain decisions made exclusively by the FBI regarding informants require notice to DOJ or the U.S. Attorneys' Offices.<sup>170</sup> In addition, § I.E of the Confidential

---

<sup>170</sup> The CI Guidelines impose other notification requirements in addition to the required notifications to the U.S. Attorney's Office when a CI is being prosecuted by or is the target of an investigation, is expected to become such a target, or has engaged in (continued)

Informant Guidelines provides that employees of the FBI and other Department of Justice Law Enforcement Agencies to which the Guidelines apply “have a duty of candor in the discharge of their responsibilities” under the Guidelines.

When the FBI fails to afford the required notice, fails to document activities or events involving informants in accordance with the Confidential Informant Guidelines, or is not candid with prosecutors concerning informant-related issues, the informants or other subjects of criminal prosecutions may claim that the government’s failure to provide exculpatory or impeachment information arising from the informant’s activities amounts to a violation of their constitutional rights. This was illustrated in *United States v. Blanco*, 392 F.3d 382 (9<sup>th</sup> Cir. 2004), in which the court held that the Government “wrongly suppressed” impeachment information about a confidential informant in violation of *Brady v. Maryland*, 373 U.S. 83 (1963) and *Giglio v. United States*, 405 U.S. 150 (1972), during a narcotics prosecution. In particular, the court ruled that the Government had suppressed information pertaining to the special immigration treatment provided to the confidential informant by the Immigration and Naturalization Service (INS) for his work with the Drug Enforcement Administration (DEA). The court found that the DEA was well aware of the informant’s immigration status, and the Government affirmatively represented that the informant’s sole reward for work was monetary compensation, but it was not clear whether the prosecutor knew of the informant’s immigration status because the DEA had been reluctant to provide information to the prosecutor. As a result, the appellate court issued an order requiring the district court to order the government to reveal all informant-related information.

Another issue that may arise is that the informant’s identity will be disclosed in the course of the prosecution. The common law “informer’s privilege” generally shields an informant’s identity, but countervailing constitutional or policy considerations may result in court-ordered disclosure. In *Roviaro v. United States*, 353 U.S. 53, 59 (1957), the Supreme Court recognized “the Government’s privilege to withhold from

---

unauthorized illegal activity. CI Guidelines § IV at B-31. These include the requirement to notify the U.S. Attorney’s Office when a CI is named as an interceptee or a violator in an application for electronic surveillance, *id.* at § III.D at B-30, and when the FBI “has reasonable grounds to believe that: 1) a current or former CI has been called to testify by the prosecution in any federal grand jury or judicial proceeding; 2) the statements of a current or former CI have been, or will be utilized by the prosecution in any federal judicial proceeding; or 3) a federal prosecutor intends to represent to a court or a jury that a current or former CI is or was a co-conspirator or other criminally culpable participant in any criminal activity.” *Id.* at § IV.C at B-32.

disclosure the identity of persons who furnish information of violations of law to officers charged with enforcement of the law.” The informer’s privilege is qualified, however, and the court may override the privilege and order disclosure of the informant’s identity if disclosure is “relevant and helpful to the defense of an accused, or is essential to a fair determination of a cause.” *Roviaro*, 353 U.S. at 60-61. The determination whether to disclose the identity of a confidential informant requires the court to balance “the public interest in protecting the flow of information against the individual’s right to prepare his defense.” *Id.* at 62.<sup>171</sup>

### **III. Significant Requirements of the Guidelines**

As the foregoing cases illustrate, when the FBI formalizes a relationship with a confidential informant, both the investigative benefits and the risks are substantial. Accordingly, the administrative and operational rules and procedures employed by the FBI ensure careful evaluation and oversight of informants and that appropriate expertise from both the FBI and DOJ is employed to evaluate informants who present the greatest risks and benefits to the interests of the government. The Confidential Informant Guidelines prescribe the process by which FBI Special Agents and their supervisors propose, approve, and operate confidential informants. We summarize below the major steps in that process.

#### **A. Suitability Reviews**

The Confidential Informant Guidelines prescribe how FBI agents are to obtain approval to evaluate and operate confidential informants. The period during which an individual is evaluated as a prospective informant is called the “Suitability Inquiry Period.” During this period, the Guidelines require that a case agent proposing to operate a confidential informant complete an Initial Suitability Report & Recommendation (ISR&R). The

---

<sup>171</sup> The informer’s privilege is litigated in both civil and criminal proceedings. See, e.g., *United States v. Gutierrez*, 931 F.2d 1482, 1490-91 (11th Cir. 1991) (refusing to order disclosure of an informant’s identity because the agent he was with during relevant periods could testify instead, and threats had been made against the informant); *United States v. Mathis*, 357 F.3d 1200, 1208 (10th Cir. 2004) (criminal defendant’s speculation about the possible relationship between two confidential informants insufficient to warrant disclosure); and *Cofield v. City of LaGrange*, 913 F. Supp. 608, 619 (D.D.C. 1996) (holding that defendants in the voting rights case failed to meet their burden to show that revealing identities of confidential informants was essential to preparation of their defense in light of public interest that weighed against disclosure which would substantially undermine the DOJ’s ability to administer its program).



ISR&R addresses 17 different factors, including the person's age, alien status, and the following particulars:

- a. whether the person is a public official, law enforcement officer, union official, employee of a financial institution or school, member of the military services, a representative or affiliate of the media, or a party to, or in a position to be a party to, privileged communications (e.g., a member of the clergy, a physician, or a lawyer);
- b. the extent to which the person would make use of his or her affiliations with legitimate organizations in order to provide information or assistance to the [FBI], and the ability of the [FBI] to ensure that the person's information or assistance is limited to criminal matters;
- c. the extent to which the person's information or assistance would be relevant to a present or potential investigation or prosecution and the importance of such investigation or prosecution;
- d. the nature of any relationship between the CI and the subject or target of an existing or potential investigation or prosecution, including but not limited to a current or former spousal relationship or other family tie, and any current or former employment or financial relationship;
- e. the person's motivation in providing information or assistance, including any consideration sought from the government for this assistance;
- f. the risk that the person might adversely affect a present or potential investigation or prosecution;
- g. the extent to which the person's information or assistance can be corroborated;
- h. the person's reliability and truthfulness;
- i. the person's prior record as a witness in any proceeding;
- j. whether the person has a criminal history, is reasonably believed to be the subject or target of a pending criminal investigation, is under arrest, or has been charged in a pending prosecution;
- k. whether the person is reasonably believed to pose a danger to the public or other criminal threat, or is reasonably believed to pose a risk of flight;
- l. whether the person is a substance abuser or has a history of substance abuse;

- m. whether the person is a relative of an employee of any law enforcement agency;
- n. the risk of physical harm that may occur to the person or his or her immediate family or close associates as a result of providing information or assistance to the [FBI]; and
- o. the record of the [FBI] and the record of any other law enforcement agency (if available to the FBI) regarding the person's prior or current service as a CI, Cooperating Defendant/Witness, or Source of Information, including, but not limited to, any information regarding whether the person was at any time terminated for cause.

#### CI Guidelines § II.A.1.

A proposed informant may remain in "suitability inquiry status" for up to 120 days with an extension of an additional 120 days.<sup>172</sup> Thereafter, if the case agent is satisfied that the person is suitable, the case agent may register the person as a confidential informant, subject to the field manager's approval. At this juncture, the case agent must document in the CI's files:

- a photograph of the CI;
- the [FBI's] efforts to establish the CI's true identity;
- the results of a criminal history check for the CI;
- the Initial Suitability Report and Recommendation;
- any promises or benefits, and the terms of such promises or benefits, that are given a CI by the [FBI] or any other law enforcement agency, if available to the [FBI];
- any promises or benefits, and the terms of such promises or benefits, that are given a CI by a federal prosecuting office or any state or local prosecuting office, if available to the [FBI]; and
- all information that is required to be documented in the CI's files pursuant to the CI Guidelines.

#### CI Guidelines § II.B.

The Guidelines also require that case agents complete and sign a Continuing Suitability Report & Recommendation (CSR&R) at least annually

---

<sup>172</sup> During fiscal year 2004, the FBI had approximately [SENSITIVE INFORMATION REDACTED] sources in "suitability inquiry status." The 120-day suitability inquiry period requirements are found in the MIOG (§ 137-5(2)), not the Confidential Informant Guidelines.

and forward the document to a field manager for approval. The CSR&R must address all the factors covered in the initial suitability review and, in addition, state the length of time the person has been a CI and the length of time the CI has been handled by the same agent or agents.

CI Guidelines § II.A.2.

The FBI's determination of a source's suitability to serve as a confidential informant is a pivotal judgment. Since the revisions to the CI Guidelines in January 2001, judgments about registering and retaining high-risk or particularly sensitive informants have been jointly made by the FBI and senior DOJ prosecutors. In addition, the Confidential Informant Guidelines require additional scrutiny and higher approval levels for confidential informants who fall into any of the following three categories:

*Long-term confidential informants*, defined as those who have been registered for more than six consecutive years;<sup>173</sup>

*High level confidential informants*, defined as individuals who are part of the senior leadership of an enterprise that (a) has (i) a national or international sphere of activities, or (ii) high significance to the FBI's national objectives, even if the enterprise's sphere of activities is local or regional, and (b) engages in or uses others to commit activity that qualifies as Tier 1 Otherwise Illegal Activity under the Guidelines;<sup>174</sup> and

*Privileged confidential informants*, defined as individuals who are under the obligation of a legal privilege of confidentiality (such as doctors, lawyers, and clergy) or individuals who are affiliated with the news media.<sup>175</sup>

For these categories of informants, approval must be secured from the Confidential Informant Review Committee (CIRC), which also provides ongoing oversight over these types of informants.<sup>176</sup> As we discuss in Chapter Seven, the CIRC focuses on critical aspects of the informant relationship through an exchange of information between the field offices that operate the informants and senior FBI and DOJ officials who test various assertions about the CI's reliability and productivity, the scope of

---

<sup>173</sup> CI Guidelines § II.A.3.a at B-16.

<sup>174</sup> CI Guidelines § I.B.9 at B-9.

<sup>175</sup> CI Guidelines § II.D.2 at B-20. Four other categories of informants require special approval: federal prisoners, parolees, detainees, and supervised releasees; current or former participants in the witness security program; state or local prisoners, probationers, parolees, or supervised releasees; and fugitives. CI Guidelines §§ II.D.3 - 6 at B-20-22.

<sup>176</sup> We discuss at greater length in Chapter Seven the operation of the CIRC.

any FBI-authorized “otherwise illegal activity,” the implications for the FBI’s relationship with the informant of any unauthorized illegal activity by the CI, and the various risks attendant to maintaining a relationship with particular informants.

## **B. Instructions**

Special Agents who handle CIs are required by the Guidelines (and the MIOG) to instruct or caution them at certain intervals. The instructions convey to the CI the scope of the informant’s authority, the limits on the FBI’s assurances of confidentiality, prohibitions against certain types of activity, and the possible consequences of violating these conditions. Upon registering a CI, the case agent, along with one other agent who must be present as a witness, is required to review with the CI the following written instructions:

- information provided by the CI to the FBI must be truthful;
- the CI’s assistance and the information provided are entirely voluntary;
- the United States Government will strive to protect the CI’s identity but cannot guarantee that it will not be divulged;
- the CI must abide by the instructions of the [FBI] and must not take or seek to take any independent action on behalf of the United States Government;
- the CI is not an employee of the United States Government and may not represent himself or herself as such;
- the CI may not enter into any contract or incur any obligation on behalf of the United States Government, except as specifically instructed and approved by the [FBI];
- the [FBI] cannot guarantee any rewards, payments, or other compensation to the CI; and
- in the event that the CI receives any rewards, payments, or other compensation from the [FBI], the CI is liable for any taxes that may be owed.

CI Guidelines § II.C.1.

In addition, if applicable, the case agent must add the following instructions:

- the FBI on its own cannot promise or agree to any immunity from prosecution or other consideration by a Federal Prosecutor’s Office or a Court in exchange for the CI’s cooperation, since the decision to confer any such benefit lies within the exclusive discretion of the

Federal Prosecutor's Office and the Court. However, the FBI will consider, but not necessarily act upon, a request by the CI to advise the appropriate Federal Prosecutor's Office or Court of the nature and extent of his or her assistance to the FBI;

- the CI has not been authorized to engage in any criminal activity and has no immunity from prosecution for any unauthorized criminal activity; and
- no promises or commitments can be made, except by the Department of Homeland Security, regarding the alien status of any person or the right of any person to enter or remain in the United States.

Id.

As described in the next section of this chapter, if the informant is authorized to engage in "otherwise illegal activity," the FBI must provide additional detailed instructions addressing the scope and limits of the authority. CI Guidelines § III.C.4.

For all categories of informants, the instructions formalize the relationship between the individual and the FBI. If the constraints within which the informant is to operate are not clear and well documented, unnecessary risk results. Failure to adhere to the Guidelines' provisions requiring periodic instructions can result in claims by informants that they had authority from the FBI to commit crimes and can thereby jeopardize investigations and prosecutions of informants and others or result in civil liability for the government.

### **C. Authority to Engage in Otherwise Illegal Activity (OIA)**

The Confidential Informant Guidelines permit the FBI to authorize confidential informants to engage in activities that would otherwise constitute crimes under state or federal law if engaged in by someone without such authorization. Such conduct is termed "otherwise illegal activity" or "OIA."

There are two types, or levels, of OIA: "Tier 1 OIA" and "Tier 2 OIA." Tier I OIA, the most serious, is defined as any activity that would constitute a misdemeanor or felony under federal, state, or local law if engaged in by a person acting without authorization and that involves the commission or the significant risk of the commission of certain offenses, including acts of violence; corrupt conduct by senior federal, state, or local public officials; or the manufacture, importing, exporting, possession, or trafficking in

controlled substances of certain quantities.<sup>177</sup> “Tier 2 OIA” is defined as any other activity that would constitute a misdemeanor or felony under federal, state, or local law if engaged in by a person acting without authorization.<sup>178</sup>

Both Tier 1 and Tier 2 OIA must be authorized in advance, in writing, for a specified period not to exceed 90 days. Tier 1 OIA must be approved by an FBI SAC and the “appropriate Chief Federal Prosecutor,” typically the U.S. Attorney in the district that is participating in the investigation utilizing the CI.<sup>179</sup> Tier 2 OIA may be approved by a senior FBI field manager (usually an Assistant Special Agent in Charge (ASAC) or a Supervisory Special Agent (SSA)), but does not require the approval of the U.S. Attorney.<sup>180</sup> The Guidelines state that the FBI is never permitted to authorize a CI to participate in an act of violence, obstruction of justice, or other enumerated unlawful activities. CI Guidelines § III.C.1.b.

Authorizing confidential informants to engage in otherwise illegal activity can facilitate their usefulness as a source of information to the government but may also have adverse consequences. As illustrated in the Bulger-Flemmi and Presser cases described earlier, the confidential informant’s criminal activity can hinder prosecution of the informant’s co-conspirators by prompting, for example, defenses of public authority or entrapment. Moreover, OIA authorizations may have unforeseen consequences. For example, a decision to authorize a confidential

---

<sup>177</sup> CI Guidelines § I.B.10 at B-9.

<sup>178</sup> CI Guidelines § I.B.11 at B-10.

<sup>179</sup> For purposes of authorizing OIA, the “appropriate Chief Federal Prosecutor” is the Chief Federal Prosecutor that “(i) is participating in the conduct of an investigation by a [Justice Law Enforcement Agency] that is utilizing that active CI, or is working with that active CI in connection with a prosecution; (ii) with respect to Otherwise Illegal Activity that would constitute a violation of federal law, would have primary jurisdiction to prosecute the Otherwise Illegal Activity; or (iii) with respect to Otherwise Illegal Activity that would constitute a violation only of state or local law, is located where the otherwise criminal activity is to occur.” CI Guidelines, § III.C.2.

<sup>180</sup> Before the Levi Guidelines were issued in 1976, an FBI special agent could authorize criminal conduct if the agent determined “that such participation is necessary to obtain information needed for purposes of federal prosecution.” In a widely publicized Kentucky state court case that was brought prior to the Levi Guidelines, an FBI informant, Delano Colvin, claimed that his contact agent or “handler,” FBI Special Agent Larry Long, authorized him to commit the burglary for which he was charged. The State indicted Long as an accomplice to the burglary. After removal to federal court, the court dismissed the indictment against Long under the Supremacy Clause, holding that provided Long reasonably believed the conduct was necessary and proper and part of his authorized duties, he was protected, even if he exercised poor judgment. *Kentucky v. Long*, 637 F. Supp. 1150, 1152 & n.5 (W.D. Ky. 1986). The decision was affirmed by the Sixth Circuit. See *Kentucky v. Long*, 837 F.2d 727, 741 (6<sup>th</sup> Cir. 1988).

informant to engage in bookmaking may create difficulties in prosecuting the informant or co-conspirators on charges related to the informant's activity.

Before either level of OIA may be authorized, the authorizing official must make certain findings as to why it is necessary for the CI to engage in the OIA and assess whether the benefits to be obtained from the FBI's authorization outweigh the risks. Specifically, the FBI must make a finding, documented in the CI's file, that the authorization for the CI to engage in the Tier 1 or Tier 2 OIA

- (i) is necessary either to
  - (A) obtain information or evidence essential for the success of an investigation that is not reasonably available without such authorization, or
  - (B) prevent death, serious bodily injury, or significant damage to property, and
- (ii) that in either case the benefits to be obtained from the CI's participation in the Tier 1 or Tier 2 OIA outweigh the risks.<sup>181</sup>

If the OIA is approved, at least one FBI agent and an alternate agent must review special written instructions with the CI that the CI must sign or initial and date the form. The instructions must address the limits of the authority, the specific conduct authorized, the time period specified, prohibitions on certain behavior, including acts of violence and obstruction of justice, and the consequences to the CI of operating outside the authority granted. In addition, if the OIA is extended past the initial authorized time period, the informants must receive and sign the instructions pertaining to the OIA every 90 days. CI Guidelines, § III.C.4; MIOG § 137-10(9).

#### **D. Unauthorized Illegal Activity (UIA)**

[SENSITIVE INFORMATION REDACTED],<sup>182</sup> [SENSITIVE INFORMATION REDACTED],<sup>183</sup> [SENSITIVE INFORMATION REDACTED].<sup>184</sup> If an informant has engaged in unauthorized illegal activity, the FBI's originating field office must respond to seven questions from the FBI's Human Intelligence Unit (HIU) (formerly the Asset/Informant Unit in the

---

<sup>181</sup> CI Guidelines § III.C.3.a at B-26.

<sup>182</sup> [SENSITIVE INFORMATION REDACTED]

<sup>183</sup> [SENSITIVE INFORMATION REDACTED]

<sup>184</sup> [SENSITIVE INFORMATION REDACTED]

Criminal Investigative Division) that focus on whether, in the judgment of the SAC, the informant nevertheless remains suitable. The SAC must also address other important issues triggered by the UIA, including whether the case agent or handler has attempted to intercede on behalf of the informant or to make any recommendations to state or local authorities regarding the informant's case. See MIOG § 137-11(4). FBI officials and prosecutors we interviewed during this review told us that when FBI agents get too close to their sources, they sometimes improperly intervene to assist their informants if they are arrested or run into other difficulties.<sup>185</sup>

The Guidelines recognize that if a confidential informant commits unauthorized illegal activity, the FBI and DOJ should immediately reevaluate the informant's continuing suitability. The Guidelines require that the unauthorized illegal activity must immediately be brought to the attention of senior FBI field office and Headquarters personnel, as well as the U.S. Attorney, so that a careful reevaluation is made of the informant's suitability in the following circumstances. First, if the FBI has reasonable grounds to believe that a confidential informant who has current authorization for Tier 1 or Tier 2 otherwise illegal activity has engaged in any criminal activity that is not authorized, the SAC must immediately notify the U.S. Attorney's Office of the CI's criminal activity and his or her status as a CI. CI Guidelines, § IV.B.1. Second, if the FBI knows that a confidential informant who has no current authority to engage in otherwise illegal activity has engaged in any criminal activity, the SAC must also immediately notify the U.S. Attorney. *Id.* Such notice is not required, however, when a state or local prosecuting office has filed charges against the informant for the illegal conduct, there is no clear basis for federal prosecution, and federal prosecutors have not previously authorized the CI to engage in Tier I OIA or been involved in an investigation that is utilizing the CI. CI Guidelines § IV.B.1.

If these steps are not taken and the informant continues to operate, serious complications may develop, including situations where prosecution of the informant is jeopardized because the informant claims the government acquiesced in the continuing illegal activity.<sup>186</sup> On the other hand, if the FBI makes the limits of the informant relationship clear and

---

<sup>185</sup> See generally, *United States v. Salemme*, 91 F. Supp. 2d 141, 199-200, 215-16 (D. Mass. 1999), rev'd sub nom. *United States v. Flemmi*, 225 F.3d 78 (1<sup>st</sup> Cir. 2000).

<sup>186</sup> See, e.g., *Commonwealth v. Ricci*, 57 Mass. App. Ct. 155, 781 N.E.2d 868, appeal denied, 439 Mass. 1102, 786 N.E.2d 395, review denied, 439 Mass. 1102, 786 N.E.2d 395 (2003).



documents its instructions to the informant, such claims are less likely to be sustained.<sup>187</sup>

The case of informant Gregory Scarpa, Sr. is an example of how an informant's unauthorized illegal activity can compromise criminal prosecutions. As described in the following case study, the FBI's informant relationship with Scarpa, a "capo" of a New York organized crime family, became controversial in several significant federal prosecutions in the 1990s. According to testimony presented in these cases, Scarpa's FBI handler ignored unauthorized criminal activity by Scarpa; revealed confidential law enforcement information to him, including the FBI's planned surveillance of a mob hangout; and helped Scarpa's son avoid arrest.

---

<sup>187</sup> See, e.g., *United States v. Robinson*, 830 F.2d 885, 890-91 (8<sup>th</sup> Cir. 1987) (affirming armed robbery conviction and rejecting defendant's claim that government's conduct was so outrageous as to violate Due Process Clause, citing evidence that FBI handlers repeatedly told defendant not to engage in criminal activity or commit robberies).

**Confidential Informant Case Study 2**  
**FBI Informant Gregory Scarpa, Sr. and his FBI Handler,**  
**R. Lindley DeVecchio**

Gregory Scarpa, Sr., who was involved in organized crime for most of his life, served as an FBI confidential informant at various times from 1980 until the early 1990s. His relationship with the FBI and, in particular, with his sole handler, R. Lindley DeVecchio, factored in a number of major prosecutions against New York members of La Cosa Nostra (LCN) in the 1990s. In some cases, Scarpa's status as an FBI informant was known during trial; in another, it was not revealed until post-conviction motions were filed and Scarpa had died.

*Victor Orena and Pasquale Amato.* In two separate federal trials in 1992 and 1993, juries found Victor J. Orena, the "acting boss" of the Colombo Family, and Pasquale Amato guilty of racketeering, conspiracy, and firearms charges. The events leading to the convictions of Orena and Amato stemmed from the "Colombo Wars," a power struggle between two Colombo factions, the Persicos and the Orenas that lasted from the fall of 1991 through the spring of 1992. At Orena's trial, DeVecchio, who headed the Colombo LCN squad in the FBI's New York Field Office, testified as an expert witness about the nature and structure of organized crime. Both defendants were sentenced to life in prison, and the Second Circuit affirmed both convictions and sentences.

Years after their convictions and following exhaustion of all appeals, Orena and Amato filed motions for dismissal of their indictments or for new trials alleging a violation of the government's disclosure obligations under *Brady v. Maryland*, 373 U.S. 83 (1963). Their motions were based upon DeVecchio's "questionable ethics and judgments" as revealed in proceedings in another case. After learning that Scarpa was a long-time FBI informant, Orena and Amato contended that it was not they, but DeVecchio, who conspired with Scarpa to instigate the Mafia war and caused the killing of their partner and loan shark, Thomas Ocera, one of the murders for which Orena and Amato were convicted.

The trial court denied the post-trial motions. *Orena v. United States*, 956 F. Supp. 1071 (E.D.N.Y. 1997). However, the court closely examined the relationship between DeVecchio and Scarpa, who rose to the position of a "capo" or captain in the Colombo family. According to the trial court, in the 1970s and perhaps as early as the 1960s, Scarpa had been regularly in touch with an FBI agent. The relationship was broken off until DeVecchio succeeded in renewing Scarpa's informant status in December 1980. DeVecchio acted as Scarpa's sole FBI handler from that time until Scarpa was finally terminated as an FBI informant after the Colombo Wars were over in 1992, despite an FBI protocol which required informants to be handled by two agents at a time.

As a "top echelon" informant, Scarpa initially provided the FBI with information pertaining to organizational activity and personnel movements within the Colombo Family. After the Colombo Wars commenced in late 1991, he provided detailed reports of perpetrators and strategic planning of the opposing factions.

The court found that DeVecchio reciprocated by passing along unauthorized information to Scarpa. For example, evidence was presented indicating that DeVecchio warned Scarpa of his pending arrest on federal credit card fraud charges and may have intervened with the sentencing judge to request lenient treatment. There also was suspicion that in 1987 DeVecchio leaked to Scarpa information that the Wimpy Boys Social Club, a favorite Colombo gathering place, was subject to court-ordered electronic surveillance; that he tipped off Scarpa to the planned DEA arrest of his son, Gregory Scarpa Jr., and others in connection with the criminal activity at the social club; and that, as a result of the warning, Gregory Scarpa, Jr. became a fugitive. With respect to the Confidential Informant Guidelines, the court also found that:

- On March 3, 1992, Scarpa was closed as an informant after the ASAC of the Criminal Division of the New York FBI Division, Donald North, “found credible allegations that Scarpa was involved in planning violent criminal activity.” In informal conversations with North, DeVecchio was allegedly “adamant” that Scarpa was not involved in violent activity. In early April 1992, DeVecchio initiated the process of having Scarpa re-opened, and the FBI granted authority to re-open Scarpa on April 8, 1992, pending completion of a suitability inquiry. On April 22, 1992, DeVecchio notified FBI Headquarters that such an inquiry had been conducted and that Scarpa was deemed suitable.
- During the summer of 1992, Special Agent Christopher Favo, who was working with DeVecchio during the investigation, became strongly suspicious of DeVecchio. Believing that DeVecchio was engaged in misconduct and fearing that he might disrupt current investigations, Favo began to withhold information from DeVecchio pertaining to Scarpa. Other subordinates of DeVecchio's suspected that Scarpa was a murderer, but none of them reported their suspicions about Scarpa or DeVecchio to superiors or to the United States Attorney despite the fact that the Informant Guidelines required agents to report any knowledge of an informant committing violent crimes.
- Scarpa was arrested by the New York City Police in August 1992 on a firearms charge. Shortly thereafter, a federal indictment charging Scarpa with the commission of the three murders, among other crimes, was handed down. Scarpa was released on bail under strict house confinement as one of the conditions of release because of failing health. In late December 1992, his bail was revoked because of his involvement in a shooting. Scarpa was sentenced to ten years in prison in December 1993 after pleading guilty to two counts of murder.
- In January 1994, Favo and other agents approached ASAC North to report their concerns about DeVecchio's relationship with Scarpa. Consistent with FBI policy, North immediately submitted a report to the FBI's Office of Professional Responsibility (OPR). OPR determined that DeVecchio was appropriately a subject of investigation. In September 1996, the Public Integrity Section determined that prosecution of DeVecchio was not warranted, and the OPR investigation was closed. DeVecchio retired from the FBI in October 1996. Scarpa died in a federal prison in June 1994.

In its ruling on Orena's and Amato's motions for dismissal of their indictments or new trials, the district court held that (1) the defendants either knew or should have known that a member of the organized crime family to which they belonged had acted as an informant, so the government's failure to disclose that fact did not warrant a new trial; (2) evidence that a government agent had leaked information to an informant and that a second government agent had concerns regarding the relationship between the first agent and the informant was not material to the Government's charges, so the Government's failure to disclose did not warrant relief under *Brady*; and (3) newly discovered evidence did not warrant a new trial.

On the issue of leaking information to an informant and the relationship between DeVecchio and Scarpa, the district court observed that while the CI Guidelines provide guidance on "sanctioning criminal conduct on the part of informants where necessary 'to establish and maintain credibility or cover with persons associated with criminal activity under investigation,'" the "line between the value of an informer and the unreasonable risks of encouraging serious criminal activity requires judgment of senior supervisors with sound ethical compasses; people in the field are often not in a position to provide the necessary direction." *Orena v. United States*, 956 F. Supp. 1071, 1102 (E.D.N.Y. 1997). The court noted that, according to the Attorney General Guidelines, the FBI does exercise control at the supervisory level in Washington and locally. In the case of Scarpa, however, "these administrative controls failed to work because DeVecchio was not properly supervised locally and because . . . he failed to inform his supervisors in Washington of the probability that Scarpa was engaged in violence." *Id.* at 1103.

*Victor Orena, Jr., John Orena, Thomas Petrizzo, et al.* In June 1995, a jury acquitted seven reputed associates of the Orena wing of the Colombo family of conspiring to murder members of the rival Persico faction of the family. Scarpa's status as an FBI informant became a pivotal issue during the trial. Fellow FBI agents testified that they had become suspicious of DeVecchio and were particularly concerned that he had fed confidential information to Scarpa which helped him to evade arrest.

*Anthony Russo, Joseph Russo and Joseph Monteleone.* Scarpa's relationship with the FBI generated post-trial motions in another case following the conviction of LCN defendants on murder and conspiracy to murder charges. In that case, in March 1997, the trial judge granted a motion for a new trial to Anthony Russo, Joseph Russo, and Joseph Monteleone, finding that the Government had improperly failed to disclose evidence bearing on Scarpa's credibility. The Court of Appeals reversed that portion of the district court's order that granted a new trial, rejecting the trial court's conclusion that evidence that Scarpa lied to the FBI about his involvement in certain other murders gave rise to an inference that he lied to his co-conspirators about the murders in question.

## **E. Deactivation of Confidential Informants**

Due to the risks involved in operating informants and the corresponding need to closely supervise their status and operation, the Guidelines prescribe that certain steps be taken in the event a confidential informant is deactivated or “closed.”<sup>188</sup> If a determination is made to close a confidential informant, whether for “cause” or for any other reason, the case agent must document the reasons for deactivation in the CI’s file. The MIOG defines “cause” as:

any grievous action by or set of previously unknown facts/circumstances that deem the individual not suitable for use as a CI. Such actions that might give “cause” include but are not limited to: disbarment; unauthorized criminal activity; incarceration; failure to follow instructions; violation of any parole, release guidelines or agreements; providing unreliable information, etc.<sup>189</sup>

When an informant is closed, the agent must also notify the CI that he or she has been deactivated and document this notification.<sup>190</sup> Moreover, if the CI is authorized to engage in otherwise illegal activity (Tier 1 or Tier 2), the case agent must revoke this authorization, and document its revocation. CI Guidelines § V.A.4. If a U.S. Attorney’s Office is either “participating in the conduct of an investigation” that is utilizing a CI or “working with a CI in connection with a prosecution,” the FBI must coordinate with the prosecuting attorney assigned to the matter, “in advance whenever possible,” regarding specified decisions relating to the CI, including a decision to deactivate a CI. CI Guidelines § V.D.

There have been many cases in which the confidential informant’s status was unknown to the prosecution, among them the Bulger-Flemmi matter described above in CI Case Study No. 1. Flemmi and Bulger were opened, then deactivated or closed for various periods of time when they became suspects or targets of other investigations. According to prosecutors who are familiar with their FBI informant files, one could not tell looking at their files when they were opened, active, or closed as

---

<sup>188</sup> It is not uncommon for the FBI to close an informant, and then open the informant months or years later in connection with the same or other investigations in the originating field office’s jurisdiction or elsewhere.

<sup>189</sup> MIOG § 137-15(13).

<sup>190</sup> CI Guidelines § V.A at B-33. Delayed notification to the CI is permitted if timely notification “might jeopardize an ongoing investigation or prosecution or might cause the flight from prosecution of any person.” CI Guidelines § V.B at B-34.

informants.<sup>191</sup> Unless the informant's status is clear, the government may not be able to fully meet its discovery obligations. Moreover, if informants are closed but the FBI cannot document this fact along with any required revocation of OIA authority, the government becomes vulnerable to the defense that the FBI authorized the informant's illegal activities.

#### **IV. Major Revisions to the Guidelines**

As described in Chapter Two, major revisions of the Confidential Informant Guidelines were approved by Attorney General Reno on January 8, 2001. The 2001 revisions were the product of a 2-year effort by a joint FBI-DOJ committee known as the "Resolution 18 Committee." The 2001 revisions included significant modifications to the provisions regarding suitability, authorization to engage in otherwise illegal activity, the prohibition against making commitments to the CI regarding immunity from prosecution, and notifying the prosecutor of the confidential informant's true identity. As we discussed in Chapter Two, many of the modifications to the previous version of the Guidelines attempted to address administrative and management weaknesses that came to light during the Bulger-Flemmi matter.

Further revisions in May 2002 made only minor modifications to the Confidential Informant Guidelines.<sup>192</sup> Under the January 2001 Guidelines, case agents who worked with confidential informants were required to read to CIs verbatim certain instructions about the constraints imposed on their activities. This provision was replaced in May 2002 by a requirement that the contact agent or "handler," along with an additional agent present as a witness, review the written instructions with the CI. CI Guidelines § II.C.1. The removal of the verbatim requirement was needed, according to FBI Director Mueller, because "the verbatim instructions, written in often

---

<sup>191</sup> According to a prosecutor who reviewed Flemmi's informant file, the fact that Flemmi was a murderer and planned to commit additional murders was not noted in his FBI informant file. Flemmi was eventually closed as an informant not because of concerns that he would commit additional homicides. Rather, in September of 1965 he was charged by state authorities with Assault with a Dangerous Weapon with Intent to Murder after he shot another person. The FBI decided to close him as an informant "[i]n view of the fact that informant is presently a local fugitive" and "any contacts with him might prove to be difficult and embarrassing." House Committee on Government Reform, *Everything Secret Degenerates: The FBI's Use of Murderers as Informants*, 3<sup>rd</sup> Report, H.R. Rep. No. 108-414, at 17 (2004), available at: <http://www.gpo.gov/hreports/108-414.html>.

<sup>192</sup> A table illustrating the May 30, 2002, revisions to the Confidential Informant Guidelines and the other revised Investigative Guidelines is attached at Appendix C.

intimidating legalese, were proving to have a chilling effect, causing confidential informants to leave the program.”<sup>193</sup>

Under the May 2002 revisions, an agent may now adapt the instructions – including the instructions on protecting the confidentiality of the CI’s identity – to the CI’s particular circumstances. Nonetheless, agents must clearly convey the content and meaning of each applicable instruction and document that the instructions were reviewed and that the CI acknowledged the CI’s understanding of them.<sup>194</sup>

Under the Confidential Informant Guidelines issued in January 2001, case agents who worked with CIs were required to give an instruction to the CIs (even if they had no relevance to the CI’s situation), relating to the inability of investigative agencies to promise immunity from prosecution. The revised Guidelines emphasize that regardless of whether these instructions are given, the FBI has no authority to confer immunity, and agents must avoid giving CIs the erroneous impression that they have such authority. CI Guidelines §§ II.C.1 (d), (e), and (k).

## **V. The OIG Review of the FBI’s Compliance with the Confidential Informant Guidelines**

To test compliance with key provisions of the Informant Guidelines in the investigative files we reviewed, we selected a judgmental sample of 120 individual confidential informant files from 12 FBI field offices we visited between June and August 2004. The CI files we reviewed fit into at least one of four categories: long-term CIs, CIs authorized to perform otherwise illegal activity, privileged or media-affiliated CIs, and CIs who are not reviewed at FBI Headquarters.<sup>195</sup> The files included some CIs who were reviewed by the CIRC and some who were authorized only at the field

---

<sup>193</sup> *Oversight Hearing on Counterterrorism*: Hearing Before the Senate Committee on the Judiciary, 107<sup>th</sup> Cong. 187 (2003) (Responses by Robert S. Mueller, III, Director, Federal Bureau of Investigation, to Committee’s written questions).

<sup>194</sup> CI Guidelines §§ II.C.1 and II.C.2 at B-19. Agents must, however, continue to obtain the informant’s written acknowledgement of instructions relating to authorization for otherwise illegal activity and in connection with payments to the informant. CI Guidelines §§ III.C.4.b and III.B.6, respectively, at B-28 & B-24.

<sup>195</sup> To accommodate the FBI’s concerns about preserving the identity of its CIs, and because the OIG did not need to know the names of the CIs to complete its review, the OIG examined copies of documents maintained in the original CI files with the CI’s name and other identifying information redacted. To ensure that our compliance findings accurately reflected all the data in the original files, FBI Headquarters personnel, working in conjunction with Informant Coordinators, confirmed the facts supporting our CI compliance findings from our field office visits.

level.<sup>196</sup> Among the “non-CIRC” CIs we reviewed, we chose CIs who were opened for over one year, CIs from different squads and programs, CIs who had been paid substantial sums, and CIs who were closed more than six months after the May 2002 revisions became effective.<sup>197</sup>

In examining individual informant files, we collected data on: suitability determinations, instructions, documentation and notifications to U.S. Attorneys’ Offices of unauthorized illegal activity, approval of otherwise illegal activity, and deactivations.<sup>198</sup> We sought to answer the following key questions.

- Were the Initial and Continuing Suitability reviews of confidential informants conducted within the required time period and was the required information provided?
- Were the required instructions or cautions given to CIs at registration and periodically thereafter?
- Were applications to permit confidential informants to engage in OIA complete and timely, was the proposed OIA described in sufficient detail, and was the requisite approval obtained from the U.S. Attorney’s Office?
- Was unauthorized illegal activity by confidential informants reported when required by the SAC to the U.S. Attorney?

---

<sup>196</sup> As noted earlier, the CIRC reviews and approves long-term CIs, high level CIs, and CIs who are under the obligation of a legal privilege of confidentiality or are affiliated with the media. CI Guidelines §§ II.A.3 and II.D at B-16 & B-19.

<sup>197</sup> We randomly chose between 9 and 11 of the pertinent files to examine in each field office, except in offices where there were only a small number of files within a certain category of informants, in which case we reviewed all files. We did not pre-select CI files that had been identified as non-compliant by internal FBI inspections or other internal compliance mechanisms, nor did we base our selection of field offices on the compliance record of those field offices or on any other criteria that would produce a bias or skewing of the judgmental sample.

As is the case, however, with any judgmental sample, one cannot extrapolate with statistical certainty that the non-compliance rate of the entire population of FBI confidential informant files would be identical to the non-compliance rate we found in our sample.

<sup>198</sup> We did not concentrate on compliance issues relating to payments to informants because such payments are the subject of multiple layers of oversight by the field divisions, HIU, the Finance Unit within CID, and the Inspection Division. As we discuss in Chapter Seven, many of the elements we reviewed are also reviewed by the Inspection Division during its triennial inspections of each FBI division.



- If confidential informants were deactivated “for cause” or other reasons, was the deactivation appropriately documented; was the informant notified of the deactivation; and, if the informant was authorized to engage in OIA, was the OIA authorization revoked and the revocation documented?

Taken together, we believe these five factors address critical judgments the FBI must make under the existing Confidential Informant Guidelines to ensure that those registered as confidential informants are suitable and understand the limits of the relationship, and that responsible DOJ officials approve, concur in, or are notified of significant developments in the informant relationship. The requirements we tested became effective 120 days after issuance of the revised Confidential Informant Guidelines in January 2001. These requirements were unaffected by the May 2002 Guidelines revisions.

In addition to our review of informant files, we also examined field guidance distributed by the FBI’s Criminal Investigative Division (CID) and the results of various reviews of the Criminal Informant Program. The reviews included inspection reports generated by the FBI’s Inspection Division and reinspections coordinated by the Asset/Informant Unit (A/IU) in the Criminal Intelligence Section of the CID. We also examined the role played by Confidential Informant Coordinators, who are GS-10 through GS-13 non-supervisory Special Agents who have the responsibility, as their principal assignment or as collateral duty, to assist FBI agents with issues associated with the administration and operation of human sources.<sup>199</sup> Confidential Informant Coordinators also work with confidential file room analysts in managing the special recordkeeping and document management requirements of the Criminal Informant Program, troubleshoot problems, and assist in the training and administrative aspects of informant operations.<sup>200</sup> We surveyed these Coordinators about the work they do in supporting the Criminal Informant Program and solicited their views on FBI

---

<sup>199</sup> MIOG § 137-1(5). Many Confidential Informant Coordinators also provide equivalent guidance and support for the operation of the FBI’s assets.

<sup>200</sup> The confidential file room analyst collects and records information and provides support for the Criminal Informant Program. Analysts also prepare statistical information to evaluate the assistance provided by confidential informants, known as “statistical accomplishments.” They also work closely with the Informant Coordinators on the paperwork associated with informant operation, promote compliance with the FBI’s policies and regulations regarding informants, and bring issues to the attention of the Informant Coordinator for resolution.

compliance with the Guidelines.<sup>201</sup> To supplement these findings, we also surveyed FBI Division Counsel and the Chiefs of the Criminal Division of the U.S. Attorneys' Offices for their perspectives on compliance-related aspects of the Confidential Informant Guidelines.<sup>202</sup>

## **VI. Compliance Findings**

Overall, we found one or more Guidelines deficiencies in 104 of the 120 confidential informant files, or 87 percent of those we examined. The deficiencies included failure to document the agent's evaluation of one or more suitability factors in the initial or continuing suitability evaluations, failure to give the required instructions to CIs or to do so at the required intervals, failure to obtain proper authority to permit CIs to engage in otherwise illegal activities, issuance of retroactive approvals of otherwise illegal activities, failure to report unauthorized illegal activity in accordance with the Guidelines, and failure to document deactivation of CIs.

The following table summarizes our compliance findings by category.

---

<sup>201</sup> We received a 100 percent response rate to our survey of Confidential Informant Coordinators.

<sup>202</sup> We received a 98 percent response rate to our survey of Criminal Division Chiefs of the U.S. Attorneys' Offices. We received a 92 percent response rate to our survey of FBI Division Counsel.

**TABLE 3.1**

**OIG Findings on Confidential Informant Guidelines  
Compliance Deficiencies in Select FBI Field Offices**

	<b>OIG Selection Criteria<sup>203</sup></b>	<b>Files Meeting Selection Criteria</b>	<b>Number of Non-compliant Files</b>	<b>Percent Non-compliant</b>
1	Initial Suitability Reports & Recommendations (ISR&Rs) – Required Elements Not Addressed <sup>204</sup>	44	15	34%
2	Instructions	120	59	49%
a	Missing One Or More Instructions		27	23%
b	Untimely Instructions		33	28%
3	Continuing Suitability Reports & Recommendations (CSR&Rs)	96	74	77%
a	Missing One Or More Reports		57	59%
b	Untimely Reports		12	13%
c	Required Element(s) Not Addressed		20	21%

<sup>203</sup> In the following categories, each file we examined could have one or more deficiencies in a single file: instructions, continuing suitability report and recommendation, otherwise illegal activity, unauthorized illegal activity, and deactivation. The only deficiency we found in the ISR&Rs was the failure to address all required suitability elements.

<sup>204</sup> As discussed above, FBI agents proposing to operate confidential informants are required to address various factors bearing upon the source's suitability by entering the relevant information on a standardized form called an Initial Suitability Report and Recommendation (ISR&R). The ISR&R must be approved in writing by a field manager. CI Guidelines, § II.A.1 at B-14.

Compliance deficiencies noted in this table for ISR&Rs are either that the field office form did not list all the required elements or the agent did not address one or more elements on the suitability form.

	<b>OIG Selection Criteria<sup>203</sup></b>	<b>Files Meeting Selection Criteria</b>	<b>Number of Non-compliant Files</b>	<b>Percent Non-compliant</b>
4	Otherwise Illegal Activity (OIA)	25	15	60%
a	OIA Authorized Prior to Source's Conversion to CI Status		4	16%
b	Tier 1 Not Authorized by USAO	2	2	100%
c	CI Did Not Sign Acknowledgement		7	28%
d	Instructions Not Timely Provided to CI After Authorization		1	4%
e	Instructions Not Provided to CI Upon Renewal		2	8%
f	Description of OIA Not Specific		7	28%
g	Not Authorized in Advance (Retroactive Authorization)		5	20%
5	UNAUTHORIZED ILLEGAL ACTIVITY	12	5	42%
a	Notification from FBI - SAC to U.S. Attorney	5	5	100%
a(1)	Not at SAC-USA Level <sup>205</sup>		3	60%
a(2)	Not Provided to USAO		2	40%
6	DEACTIVATION	46	17	37%
a	Notification to CI		16	35%
a(1)	No Documentation of Notification to CI		15	33%
a(2)	Did Not Notify CI		1	2%
b	Reasons Not Documented		1	2%
c	No Coordination With USAO		1	2%
	<b>TOTAL<sup>206</sup></b>	<b>120</b>	<b>104</b>	<b>87%</b>

<sup>205</sup> For this deficiency, either the SAC notified someone other than the U.S. Attorney, a subordinate FBI field manager notified the U.S. Attorney, or a subordinate FBI field manager notified someone other than the U.S. Attorney.

<sup>206</sup> Of the 120 CI files, 104 contained 1 or more compliance errors. However, a single file could have more than 1 error.

We set forth below our findings for each of the five compliance categories we tested in our review of 120 individual confidential informant files. Due to the critical interaction mandated by the Guidelines between the FBI and the U.S. Attorneys' Offices, we separately address compliance findings relating to those exchanges.

#### **A. Initial and Continuing Suitability Reviews**

As we discussed above, suitability reviews are the initial and periodic reviews undertaken by FBI Special Agents and their supervisors to evaluate the suitability of those whom they propose to operate or to continue operating as confidential informants. In one form or another, suitability reviews have been required for all confidential informants since the first set of Attorney General Guidelines issued in 1976.

Since January 2001, Special Agents proposing to designate a source of information as a confidential informant have been required to research at least 17 different factors which, collectively, will inform the *initial* suitability determination. Prospective confidential informants are initially placed in Suitability Inquiry Status (SIS) for up to 120 days, during which these factors are researched and evaluated by the Special Agent who is proposing to "run" or operate the confidential informant. If the case agent proposes, and the field manager approves, the suitability of an individual to serve as a confidential informant, the informant is "registered" as a confidential informant, at which point certain identifying and other information is placed in the informant's file. CI Guidelines § II.B.

The suitability elements listed in § II.A of the CI Guidelines address several concerns, including whether the CI's information can be corroborated and is relevant to an investigation's objectives. If the informant's information cannot be corroborated, it is likely to be insufficient for critical purposes (e.g., the informant will not establish probable cause for a search warrant or Title III wiretap under either *Aguilar v. Texas*, 378 U.S. 108 (1964), *Spinelli v. United States*, 393 U.S. 410 (1969), or *Illinois v. Gates*, 459 U.S. 1028 (1982)), and, at worst, part of an effort by the informant to serve the informant's own purposes at law enforcement expense.

Agents must also address the nature of the CI's relationship to the subject or target of the investigation. This is another means by which to assess the potential relevance of the confidential informant's information and also flag potential negative suitability issues. For instance, if the prospective confidential informant is a bookmaker who has been taken into the confidence of a mafia boss, he would be a potentially ideal informant from the standpoint of a cost/benefit analysis. The confidential informant presumably will have valuable information about an important target but is not committing crimes nearly as serious as the target's. If the situation is

the reverse, however, it may not be a productive arrangement for the government. For example, confidential informants Bulger and Flemmi were mob bosses who were providing information about lower-level criminals and crimes while using law enforcement to serve their criminal purposes and preserving the possibility of an informant defense if prosecuted themselves for murder and other serious crimes.<sup>207</sup>

Of the 120 CI files we reviewed, 44 required an Initial Suitability Report & Recommendation (ISR&R) during the period of our review.<sup>208</sup> Of those 44 CI files, we found that:

- 15 of the 44 files, or 34 percent, did not contain documentation of at least 1 required suitability factor;
- the most frequently omitted suitability factors were the extent to which the CI's information or assistance could be corroborated (missing in 12 files); the extent to which the CI's information or assistance would be relevant to a present or potential investigation or prosecution and the importance of such an investigation or prosecution (missing in 11 files); and the nature of any relationship between the CI and the subject or target of an existing or potential investigation or prosecution (missing in 11 files);
- at 6 of the 12 field offices we visited, ISR&R field office-generated forms called "ponies" did not require documentation of at least 1 of the required suitability factors.<sup>209</sup>

Case agents who operate confidential informants are also required to make *continuing* suitability reviews at least annually and to forward their reports and recommendations to their field managers for approval. CI Guidelines § II.A.2. Case agents must address all of the applicable factors required for the initial suitability determination and, in addition, indicate the length of time the individual has been registered as a confidential

---

<sup>207</sup> Other relationships might suggest additional reasons to suspect the confidential informant's motives (e.g., an ex-spouse or former business partner currently involved in civil litigation with the target) or present a sensitive circumstance (e.g., a CI who is a disbarred attorney but used to represent the target).

<sup>208</sup> We did not review ISR&Rs for the remaining 76 CIs because they were registered prior to May 30, 2002, the effective date of the revised Confidential Informant Guidelines.

<sup>209</sup> The ISR&Rs used in 3 field divisions we visited did not list 11 suitability factors in their ponies, including questions pertaining to the CI's reliability and truthfulness. Twelve elements were missing from another field offices' pony, including the same elements missing from ponies of the three offices listed above. Ten elements missing from ponies of the three offices listed above were also missing from yet another field office's ISR&R pony. Another field office's ISR&R pony had one missing element. See Table 3.7, *infra*.

informant and the length of time the individual has been handled by the same agent or agents.

We found that 2 of the 12 field offices we visited did not require case agents to perform the continuing suitability reviews required by § II.A.2 of the Confidential Informant Guidelines.<sup>210</sup> Of the 120 CI files we reviewed, 96 required a Continuing Suitability Report & Recommendation (CSR&R) during the period of our review. Of the 96 CI files (including files from the 2 offices that did not complete CSR&Rs), we found that 57 of the 96 files, or 59 percent, did not contain 1 or more required CSR&Rs. The breakdown of the 57 files that did not contain a required CSR&R is as follows:

- 34 of the 96 files, or 35 percent, did not contain 1 required CSR&R;
- 16 of the 96 files, or 17 percent, did not contain 2 required CSR&Rs; and
- 7 of the 96 files, or 7 percent, did not contain 3 required CSR&Rs.

Our surveys of Informant Coordinators also revealed concerns about agents' compliance with the suitability assessment requirements. With regard to the critical initial evaluation of CIs' suitability, 27 percent of the Coordinators said they believe that insufficiently rigorous suitability determinations are an occasional concern in their respective field offices, and 43 percent said they believe that agents' failure to devote adequate time to complete the paperwork associated with confidential informants is an occasional concern.<sup>211</sup>

## **B. Instructions**

As described earlier, when a confidential informant is registered, the case agent must review with the CI, in the presence of another agent, written instructions or admonishments detailing the constraints under which the CI is to operate. The Guidelines require that the content and meaning of the instructions must be clearly conveyed, but as of May 2002, they no longer require that the instructions be read verbatim. After the instructions are given, the case agent must obtain the CI's acknowledgement of the CI's receipt and understanding of the instructions

---

<sup>210</sup> Following our site visits, these two field divisions sent communications to their employees reiterating the requirement to conduct continuing suitability reviews.

<sup>211</sup> Our survey revealed that 2 percent of Informant Coordinators said they considered insufficiently rigorous suitability determinations to be "somewhat serious," 4 percent regarded this a "very serious" concern, 32 percent said it was "no concern," and 36 percent said it was a "minor concern."

and must document that the instructions were reviewed with the CI and that the CI acknowledged his or her understanding of them.

CI Guidelines § II.C.

The 120 CI files we reviewed all involved informants who were supposed to be instructed by the assigned case agents at registration, annually, or both. Of those 120 CI files, we found that:

- 93 of the 120 files, or 78 percent, contained documentation that all required instructions were given and acknowledged;
- all but 1 file contained documentation that the required instructions were given at registration;
- 22 of the 120 files, or 18 percent, did not contain documentation of 1 required annual instruction;
- 3 of the 120 files, or 3 percent, did not contain documentation of 2 required annual instructions;
- 1 file did not contain documentation of 3 annual instructions; and
- 33 of the 120 files, or 28 percent, contained documentation indicating that the instructions were given, but were not timely; on average, the instructions were given 72 days late, and ranged from 4 to 270 days late.<sup>212</sup>

---

<sup>212</sup> There were 34 instances in the 33 files of late instructions. Two files had late instructions at registration, 30 files had 1 late annual instruction, and 1 file had 2 late annual instructions.



The following table illustrates our field office compliance findings with respect to documentation of the requirement to provide instructions to confidential informants.

**TABLE 3.2**

**Compliance with Confidential Informant Guidelines Instruction Requirements in Select FBI Field Offices**

Field Office	Number of CI Files That Required Instructions	Compliant CI Files	Deficient CI Files	
		Number Compliant With Instruction Requirements	Number in Which at Least One Instruction Was Missing	Number in Which Instructions Were Untimely
Field Office 1	10	5	1	4
Field Office 2	10	6	2	2
Field Office 3	10	9		1
Field Office 4	10	5	4	1
Field Office 5	10	3	4	3
Field Office 6	9	4	3	2
Field Office 7	10	7		3
Field Office 8	10	4	3	3
Field Office 9	10	7		3
Field Office 10	9	2	4	3
Field Office 11	11	4	4	3
Field Office 12	11	5	2	5

The following table illustrates the significant disparity in the number of days the FBI was late in providing the required instructions, either upon registration of the CI or in giving the annual instructions.

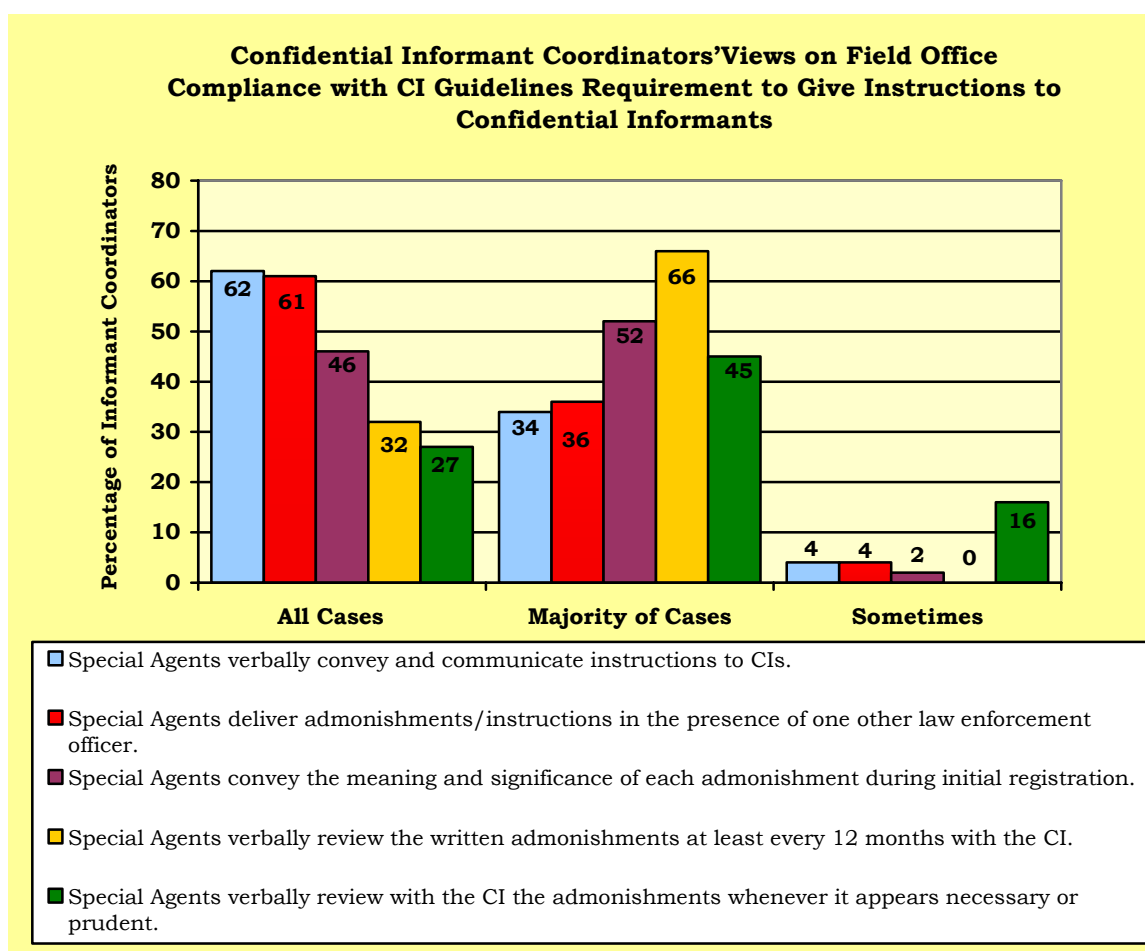
**TABLE 3.3**

**Timeliness of Instructions Given to Confidential Informants  
in Select FBI Field Offices**

FIELD OFFICE	TOTAL NUMBER LATE	DAYS LATE	
		REGISTRATION	ANNUAL
FIELD OFFICE 1	4	33	11
			108
			178
FIELD OFFICE 2	2		38
			69
FIELD OFFICE 3	1		4
FIELD OFFICE 4	1		29
FIELD OFFICE 5	4		10
			21
			86
			144
FIELD OFFICE 6	2		45
			64
FIELD OFFICE 7	3	90	36
			46
FIELD OFFICE 8	3		11
			46
			215
FIELD OFFICE 9	3		6
			19
			97
FIELD OFFICE 10	3		4
			43
			174
FIELD OFFICE 11	3		21
			159
			270
FIELD OFFICE 12	5		25
			43
			65
			91
			146

Our findings that all required instructions were not given in a substantial percentage of the sampled CI files were corroborated by the survey responses from Confidential Informant Coordinators. As reflected in the following diagram, Informant Coordinators told us that they believed case agents in their field offices are communicating the required instructions and are delivering them in the presence of another law enforcement officer in all cases less than two-thirds of the time. Informant Coordinators further reported that adherence to the requirement that instructions be repeated every 12 months is even lower. As the following diagram illustrates, only 32 percent of Informant Coordinators said the annual instructions are given in all cases, and 66 percent stated they are given in a majority of cases.'

**DIAGRAM 3.1**



### **C. Authority to Engage in Otherwise Illegal Activity (OIA)**

As described earlier in this chapter, under some circumstances the Confidential Informant Guidelines permit confidential informants to engage in otherwise illegal activity (OIA). The most serious OIA is called “Tier 1 OIA,” which must be authorized by the FBI Assistant Director in Charge or Special Agent in Charge of the Field Office or Division and the appropriate U.S. Attorney in advance and in writing. The authorization is effective for a period not to exceed 90 days.<sup>213</sup> “Tier 2 OIA” may be authorized for a period not to exceed 90 days by a senior field manager<sup>214</sup> and must also be in writing.<sup>215</sup>

In order to be authorized to engage in either Tier 1 or Tier 2 OIA, the informant must be a fully operational CI, a status obtained only when the CI is “registered” at the conclusion of a successful suitability inquiry period.<sup>216</sup> In addition, the authorizing official must make a finding that the authorization to engage in OIA is necessary either to obtain information or evidence that is essential for the success of the investigation and that is not reasonably available without the authorization, or to prevent death, serious bodily injury, or significant property damage, and that, in either case, the benefits to be obtained from the informant’s participation in OIA outweigh the risks.

According to a senior HIU official, in a typical drug investigation Tier 1 OIA is usually limited to negotiating the purchase of drugs in quantities that exceed the Federal Sentencing Guidelines’ provision referenced in the definition of Tier 1 OIA in § I.B.10.b.iii of the Confidential Informant Guidelines, or engaging in activities that involve a significant risk of violence. The official said that Tier 2 OIA typically involves similar activities to Tier 1 OIA but drug amounts below the sentencing guidelines thresholds

---

<sup>213</sup> CI Guidelines § III.C.2.a at B-26.

<sup>214</sup> A “senior field manager” is a second-line supervisor, typically a GS-15 rank or higher. CI Guidelines § I.B.3 at B-8. A “field manager” is a first-line supervisor, typically a GS-14 rank supervisor or higher. CI Guidelines § I.B.2 at B-8.

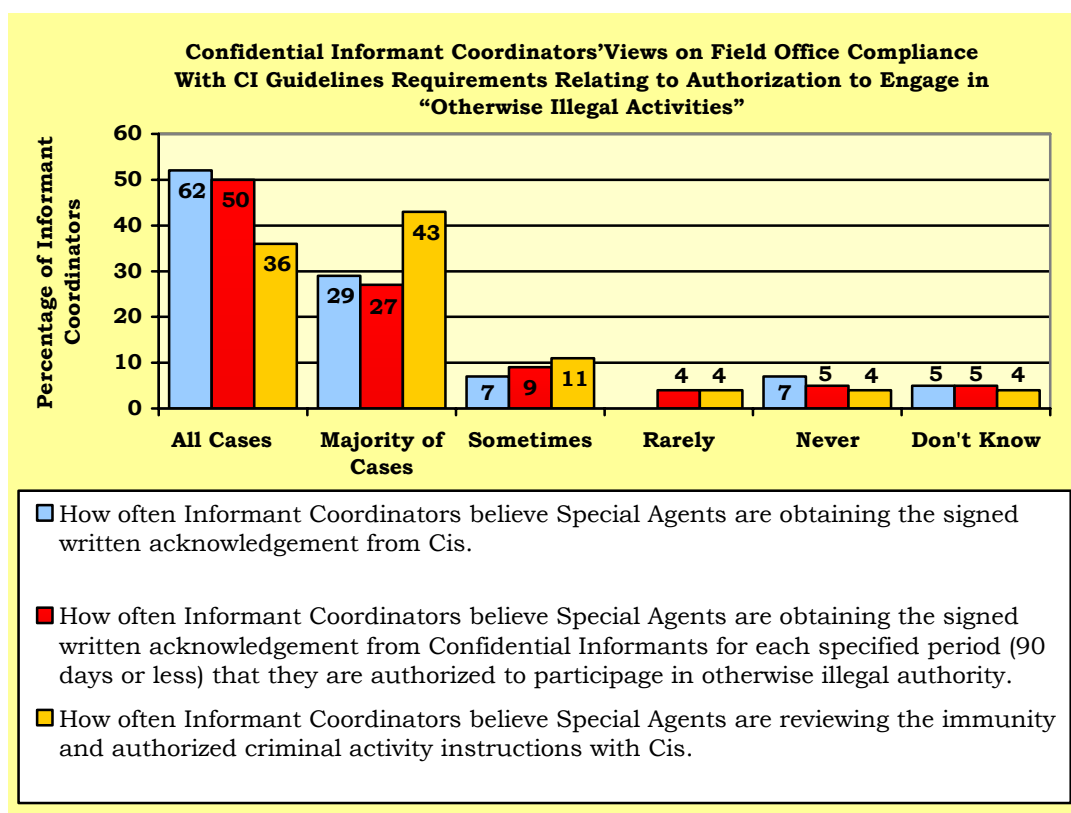
<sup>215</sup> CI Guidelines § III.C.2.a at B-26. Both Tier 1 and Tier 2 OIA can be renewed. CI Guidelines § III.C.8 at B-23.

<sup>216</sup> The Guidelines provide that a CI may be registered only after a field manager has approved the source’s suitability. CI Guidelines §§ II.B at B-17. The provisions relating to OIA by their terms apply only to CIs. *Id.* at III.C at B-25. Similarly, the MIOG explicitly forbids the FBI from authorizing OIA during the suitability inquiry period: “[T]he CI may NOT be authorized to conduct Tier 1 or Tier 2 Otherwise Illegal Activity . . . during the SI period.” MIOG I § 137-5.2.c (emphasis in original).

and with no significant risk of violence.<sup>217</sup> In a public corruption investigation, Tier 1 OIA might involve conspiratorial conversations involving bribery of a high level public official, while Tier 2 OIA would involve similar conversations about a lower level official.

We surveyed Confidential Informant Coordinators to see if they believed case agents in their field offices were complying with the Guidelines' requirement to obtain the informant's written acknowledgement of instructions relating to authority to engage in otherwise illegal activity.<sup>218</sup> Only 52 percent of the Coordinators reported that they believed agents in their field offices obtain the required written acknowledgements in all cases, and only 36 percent said they believed that agents in their field offices are conveying in all cases the instructions indicating that the CIs have not been authorized to engage in any criminal activity and have no immunity from prosecution.

**DIAGRAM 3.2**



<sup>217</sup> See MIOG § § 137-2(7) and 137-2(13), respectively.

<sup>218</sup> The instructions are summarized supra, and are set forth in the CI Guidelines § III.C.4 at B-27.

We reviewed 25 informant files in which OIA was authorized, of which 2 included Tier 1 OIA and 23 were exclusively Tier 2 OIA.<sup>219</sup> With respect to the Guidelines' requirements governing the authorization of OIA, our findings confirmed the views of the Confidential Informant Coordinators. We found that 15 of the 25 files, or 60 percent, reflected compliance deficiencies. The deficiencies included OIA authorizations for sources who had not yet been registered as CIs, retroactive authorizations of OIA, authorizations of Tier 2 OIA that should have been denominated as Tier 1 and therefore required DOJ approval, insufficiently specific descriptions of OIA, failures to obtain the CI's written acknowledgment of instructions regarding the limits of OIA activities, and failures to provide required instructions.

Four of the 25 files, or 16 percent, indicate that sources were authorized by field supervisors to engage in Tier 2 OIA from 45 to 154 days before the source was approved for conversion to a fully operational confidential informant. Although these four files do not indicate when the OIA was actually performed, we consider this to be a Guidelines violation since the period during which the CI was authorized to engage in OIA preceded the period for which the CI was eligible to engage in OIA under the Guidelines. The Tier 2 OIA that was authorized for these sources included making controlled buys of cocaine, paying over \$10,000 to establish the CI's credibility in a racketeering investigation, and engaging in conspiratorial conversations relating to a drug trafficking investigation.

Five of the 25 files that contained OIA authorization, or 20 percent, indicate that the field supervisors retroactively authorized confidential informants to engage in Tier 2 OIA anywhere from 17 to 63 days after the start of the authorization period. In these cases, field supervisors authorized the OIA retroactively to the first day of the 90-day authorization period. The OIA in these cases included engaging in conspiratorial conversations in connection with a domestic terrorism investigation, engaging in telephone conversations and face-to-face meetings with targeted subjects of a drug trafficking investigation, and purchasing drug paraphernalia as a drug broker. We could not determine from our limited file reviews the reason why the case agents sought OIA authority for the

---

<sup>219</sup> Of the two CI files we reviewed that contained Tier 1 OIA, one CI was authorized to perform both Tier 1 and Tier 2 OIA, while the other was authorized to perform only Tier 2 OIA. One file indicated that the CI was properly authorized to perform Tier 1 OIA for only a limited period, while the second file indicated that the CI was authorized to perform only Tier 2 OIA. We believe the second CI's OIA activities should have been classified as Tier 1 OIA for the reasons discussed in the analysis that follows. We believe the field characterizations of the Tier 2 activities in the remaining 23 files were appropriate.

earlier period, whether the CIs in fact engaged in OIA prior to the retroactive authorization, or whether the field supervisors were aware of either the specific criminal activities that were retroactively authorized or the reason for the agents' delay in seeking approval.

We also identified two instances in which the FBI failed to obtain proper authorization from the U.S. Attorney with respect to Tier 1 OIA. Both matters originated in the same field office, and the OIA in question was treated as Tier 2.<sup>220</sup> In the first case, the FBI's authorization included conspiracy to commit robbery, a crime of violence. In the second case, the risk of violence justified the Tier 1 status.

The files for 7 of the 25 CI files (28 percent) that contained OIA authorizations did not include sufficiently specific descriptions of the authorized OIA in that they failed to specify the time period or "specific conduct" authorized. For example, authorizations of Tier 2 OIA were based upon the following broad descriptions of the otherwise illegal activity:

- "Negotiate for, purchase/receive, and possess narcotics, to include cocaine, heroin, marijuana, and/or ecstasy;"
- "Transport, store, and sell drugs; transport drug money, conduct counter-surveillance, purchase drug paraphernalia, act as a drug broker, facilitate drug purchases, purchase cellular telephones to be utilized by drug traffickers, and general money laundering activities."<sup>221</sup>

In addition, 7 of the 25 files, or 28 percent, did not include the CI's signature or initials acknowledging that the CI had reviewed the written instructions on the limits of OIA activities. The files for 2 CIs indicated that the OIA admonishments were not given every 90 days as required by the Guidelines.

The following table illustrates our findings regarding premature, retroactive, and insufficiently specific authorizations, and authorizations of persons for whom the FBI had no basis to authorize OIA.

---

<sup>220</sup> As noted supra, the Informant Guidelines distinguish between Tier 1 and Tier 2 OIA based on the criteria set forth in §§ I.B.10 and I.B.11.

<sup>221</sup> In contrast, the descriptions of OIA in the balance of the CI files we examined included greater detail about the illegal conduct and typically specified the time, place, and manner in which the OIA was to be performed. In drug cases, for example, the OIA description often specified the type of drugs, the amount, and the individuals with whom the transaction was to take place. In public corruption cases, the OIA description identified the particular work to be performed for specified subjects of the investigation.

**TABLE 3.4**

**Compliance Deficiencies Involving FBI Authorization  
of Otherwise Illegal Activity in Select FBI Field Offices**

Field Office CI File Numbers		OIA Authorized Prior to Conversion of Source (Number of Days)	OIA Authorized, but Source Never Converted	OIA Description Not Sufficiently Specific	OIA Retroactively Approved (Number of Days Retroactively Authorized)	Total Number of Deficiencies
Field Office 1	8			1		1
Field Office 1	9			1		1
Field Office 1	10			1		1
Field Office 1	11			1	1 (22)	2
Field Office 3	13			1		1
Field Office 3	14	1(154)		1		2
Field Office 6	7		1		1 (63)	2
Field Office 6	9				1 (63)	1
Field Office 6	11		1			1
Field Office 6	15				1 (41)	1
Field Office 10	6	1 (45)				1
Field Office 12	8			1		1
Field Office 12	10	1(66)				1
Field Office 12	11	1(129)			1 (17)	2
<b>Total</b>		<b>4</b>	<b>2</b>	<b>7</b>	<b>5</b>	<b>18</b>
Total Non-compliant Files						14
Total Number of Files With OIA						25
Percent Non-compliant Files						56%



#### **D. Unauthorized Illegal Activity (UIA)**

The FBI is required to notify either a U.S. Attorney or the head of a DOJ litigating component when a CI engages in illegal activity which was not previously authorized, known as unauthorized illegal activity or “UIA.” CI Guidelines, § IV.B.1. The Confidential Informant Guidelines require that notice of the unauthorized illegal activity be provided by the Special Agent in Charge of the field office operating the CI to the U.S. Attorney or DOJ component head, not by subordinate FBI field office personnel to other U.S. Attorneys’ Offices or DOJ personnel.

The FBI is not required to provide such notice when a state or local prosecuting office has filed charges against the informant for the illegal conduct, there is no clear basis for federal prosecution, and federal prosecutors have not previously authorized the CI to engage in Tier 1 OIA or been involved in an investigation that is utilizing the CI. *Id.*

Of the 120 informant files we examined during our review, we identified 12 instances, or 10 percent, where the CI engaged in unauthorized illegal activity. Under the Guidelines, the FBI was not required to notify the U.S. Attorney in 3 of the 12 cases.

In 4 of the 12 cases, the CI case files did not include sufficient information for us to determine whether charges had been filed by state or local prosecutors following arrest of the CI, and thus it was not possible to determine whether the Guidelines’ notification requirement was triggered. Our review also found that neither the field nor FBI Headquarters typically monitors whether charges are filed by state or local prosecutors following a CI’s arrest. We identified one field office that did not have any forms to record the occurrence of unauthorized illegal activity.<sup>222</sup>

The remaining five cases required notification to the U.S. Attorney’s Office. In two of the five cases, the FBI failed to provide any notification to the U.S. Attorney’s Office, in violation of the CI Guidelines. The UIA in these cases were a state arrest relating to purchasing heroin and a misdemeanor charge of manufacturing unauthorized records. The other three files contained documentation indicating that notice was provided to the U.S. Attorney’s Office by FBI field personnel, but was not provided by the Special Agent in Charge to the U.S. Attorney as required by the Guidelines.

---

<sup>222</sup> Most field offices recorded information regarding unauthorized illegal activity on either a Continuing Suitability Report and Recommendation form or a customized 90-day file review form. The FBI advised the OIG that FD-302s can also be used to capture such information; however, the FBI did not provide FD-302s recording UIA information during our field office visits.

### **E. Deactivation of Confidential Informants**

When a confidential informant is deactivated or closed, the Confidential Informant Guidelines require the FBI to maintain appropriate documentation in the CI's file of certain notifications to the informants and to FBI Headquarters and DOJ personnel. In our review of 46 informant files indicating that the informant had been deactivated, we found:

- 17 of the 46 files, or 37 percent, contained 1 or more deficiencies;
- there was no documentation in 15 of the 46 files (33 percent) indicating that the CI was notified of the deactivation;
- in one CI file, there was no documentation that the field office coordinated with the Assistant U.S. Attorney assigned to the matter regarding the deactivation; and
- one CI file had no documentation of the deactivation itself.<sup>223</sup>

None of the 46 CIs who were deactivated was authorized at the time of deactivation to engage in OIA, so we had no findings on this issue.

### **F. Seeking Approval or Concurrence from, and Providing Notification to, the United States Attorney's Office**

As we discussed in Chapter Two, the significant revisions made to the Confidential Informant Guidelines in January 2001 changed the role of the U.S. Attorneys' Offices with respect to the approval and management of confidential informants.

To assist in determining whether the FBI is compliant with the Confidential Informant Guidelines' provisions that call for DOJ oversight, we surveyed the Chiefs of the Criminal Division in all 93 U.S. Attorneys' Offices throughout the country. Ninety-one Criminal Division Chiefs or their designees responded to our survey in February 2004. The results show that the Criminal Division Chiefs are overwhelmingly satisfied with the FBI's communication with them regarding confidential informants. The survey results included the following:

- with respect to the FBI's obligation to obtain the U.S. Attorney's advance written approval of Tier 1 OIA, the Criminal Division Chiefs said they were not aware of any circumstance when the FBI failed to comply since May 30, 2002;

---

<sup>223</sup> This CI was arrested on two federal felony drug offenses in November 2003. The documentation of the deactivation occurred on June 15, 2004, following notification that the OIG had included this file in the list of CI files we wished to review.

- of the 27 percent of surveyed Criminal Division Chiefs who stated that confidential informants had been named in electronic surveillance affidavits in their field offices since May 30, 2002, 88 percent told us that U.S. Attorneys' Offices have been notified in all appropriate cases;
- only 1 Criminal Division Chief cited as a serious concern the FBI's failure to notify the appropriate federal prosecutor of unauthorized illegal activity by confidential informants and failure to share information with the U.S. Attorney's Office about confidential informants' activities in investigations in which the U.S. Attorney's Office is participating; and
- as a group, the Criminal Division Chiefs did not express concerns about receiving timely notice of unauthorized illegal activity by CIs operated in their Districts since May 30, 2002. However, 35 percent stated that the *impact* of unauthorized illegal activity by CIs has been either a minor or occasional concern since May 30, 2002, while 25 percent reported that notice deficiencies have been either a minor or occasional concern. In addition, 10 percent of the surveyed Criminal Division Chiefs said they believed that FBI agents in their District do not have the same understanding as the U.S. Attorney's Office of the Guidelines' requirement to notify the U.S. Attorney of any unauthorized illegal activity by CIs.<sup>224</sup>

Detailed findings from our survey are presented in Appendix D. These results were one of the several areas in which the Criminal Division Chiefs indicated that the required interaction between FBI and DOJ personnel on informant matters is working well.

However, some of our findings and the results of our file reviews are in conflict with the Criminal Division Chiefs' positive assessment. As discussed above, in the course of our file reviews we identified Guidelines violations with respect to the required notifications regarding otherwise

---

<sup>224</sup> There were a few exceptions to the overwhelmingly positive assessments by Criminal Division Chiefs. For example, one of the Criminal Division Chiefs told us in a survey response that, "We receive inadequate information from FBI regarding their use of CIs."

It is important to note that the Criminal Division Chiefs may not know when they were *not* given required notifications. FBI officials and DOJ prosecutors acknowledged to us that these types of Guidelines violations likely would not become known unless there was a major event disrupting the informant relationship, such as those that are discussed in this chapter and in Chapter Two. Even in these situations, however, the U.S. Attorney's Office may not be aware that a problem exists unless the informant issue directly impacts on a case being investigated or prosecuted by the U.S. Attorney's Office.

illegal activity, unauthorized illegal activity, and events surrounding the deactivation of confidential informants. We also identified two cases in which the FBI failed to obtain proper authorization from the U.S. Attorney with respect to Tier 1 OIA.

Moreover, the Criminal Division Chiefs indicated that they believe additional training for FBI Special Agents and supervisors and other measures are needed to promote adherence to the Confidential Informant Guidelines. Half of the Criminal Division Chiefs told us that the FBI and DOJ should sponsor periodic joint or cross-training with FBI agents and prosecutors. The following table describes the type of additional training they think is needed.

**TABLE 3.5**

**Training and Other Measures Proposed by USAO Criminal Division  
Criminal Chiefs to Promote Adherence to the  
Confidential Informant Guidelines**

	<b>Response</b>	<b>Number</b>	<b>Percent</b>
a) Originating from FBIHQ	Provide standardized electronic forms related to the Confidential Informant Program (CIP) that can be completed online	35	38%
	Create a web site on the FBI Intranet displaying all current AG Guidelines with automatic e-mail notification of updates	36	40%
	Consolidate all guidance related to the CIP (AG Guidelines, MIOG, ECs, OGC training) and make available online at one Intranet web site	49	54%
	Hold annual CIP Coordinator conferences on the AG Guidelines	30	33%
	Other	3	3%
	None of the above	24	26%
b) Originating from the Field Divisions	Provide additional training to Special Agents and Supervisors by the CDCs	36	40%
	Conduct informal field office reviews of confidential informants	23	26%
	Have SAC/ASAC conduct file reviews with greater frequency	8	9%
	Other	1	1%
	None of the above	44	49%

	<b>Response</b>	<b>Number</b>	<b>Percent</b>
c) Originating from the USAOs	Sponsor periodic cross-training <i>within the District</i> with experienced agents who regularly participate in the CIP program	46	50%
	Sponsor periodic <i>regional</i> cross-training with experienced agents who regularly participate in the CIP program	22	24%
	Sponsor participation by experienced agents who regularly participate in the CIP program in all appropriate NAC courses that deal with confidential informants	48	52%
	Other	1	1%
	None of the above	26	28%
d) Originating from Main Justice	Periodically circulate to all FBI Field Office “lessons learned” from CIRC meetings and training sessions	49	54%
	Provide standardized letters of approval that can be completed online	36	40%
	Other	3	3%
	None of the above	32	36%

## VII. OIG Analysis

Human sources are critical to the success of the FBI’s criminal investigative mission and of other law enforcement and intelligence efforts aligned with that mission, including the efforts to prevent terrorism and address other emerging national security threats. Our review focused on the FBI’s implementation of Attorney General Guidelines for one category of human sources, confidential informants. The authorities and activities of other human sources, including assets and cooperating witnesses, are governed by different Attorney General Guidelines. Nor did our review examine how the FBI coordinates all of its human sources who, since November 5, 2004, have operated under the FBI’s unified Directorate of Intelligence.<sup>225</sup>

---

<sup>225</sup> See Testimony of Robert S. Mueller, III, Director, Federal Bureau of Investigation, Before the Subcommittee on the Department of Commerce, Justice, and State, the Judiciary, and Related Agencies, of the House Appropriations Committee, June 3, 2004, available at: <http://www.fbi.gov/congress/congress04/mueller060304.htm>; Statement of Maureen A. Baginski, Executive Assistant Director, Intelligence, Before the Senate Committee on the Judiciary, Aug. 19, 2004, available at: <http://www.fbi.gov/congress/congress04/baginski081904.htm>.

The Confidential Informant Guidelines were revised in January 2001 largely in response to the adverse consequences arising from the FBI's operation of informants by its Boston Field Office and a few other informant problems in other offices. Some senior FBI officials and many field personnel we interviewed believe the revisions were an overreaction and that the resulting Guidelines have generated widespread resentment among field personnel. Nonetheless, there is widespread recognition by FBI personnel we interviewed that criminal informants are vital to the success of the FBI's criminal investigative mission, and that the challenge for the government is to appropriately weigh the informant's value against the risk that the informant will commit unauthorized crimes or otherwise prejudice the government, and to monitor and supervise the relationship closely.

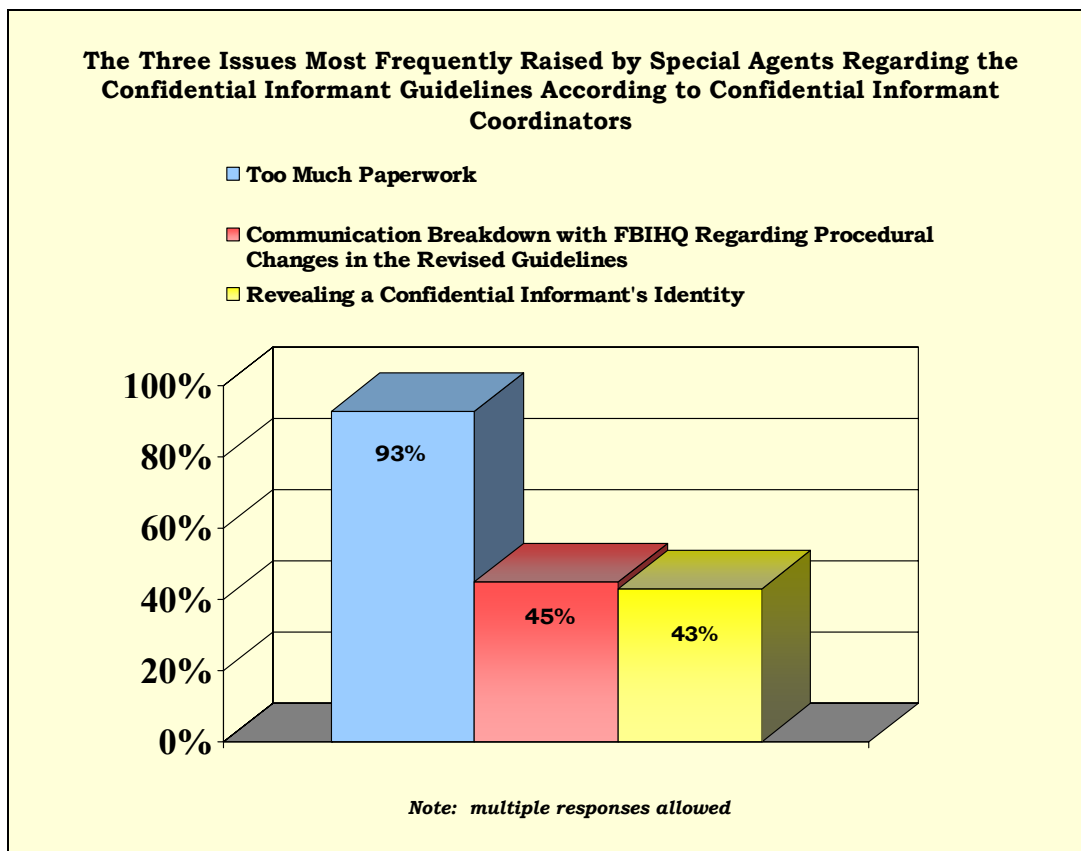
FBI personnel ranging from new agents to the Director told us that agents find the paperwork associated with opening and operating informants to be excessively burdensome and time-consuming. In addition, personnel in HIU stated that the current version of the Confidential Informant Guidelines is phrased in dense "legalese" that is hard for case agents to absorb, remember, and follow. Although we were unable to quantify the precise impact of these issues, some of the field and Headquarters personnel we interviewed told us that some FBI agents are now reluctant to open informants because of these and other administrative and operational burdens.<sup>226</sup> Others expressed concern that agents may shift toward operating "hip pocket" informants in contravention of FBI and Guidelines mandates so they will not have to complete the paperwork, obtain required approvals, or risk disclosing their informants' identities to prosecutors or others.

Our survey of Confidential Informant Coordinators revealed that the burden on case agents to complete the paperwork associated with the Criminal Informant Program is a major concern. Approximately 70 percent of the Coordinators reported that case agents fail to devote adequate time to completing their paperwork or resist doing so. In addition, as the following diagram illustrates, the paperwork burdens of operating informants is one of the most frequently raised issues in their field offices.

---

<sup>226</sup> For example, in responding to our survey, Criminal Division Chiefs of the U.S. Attorneys' Offices said they believe the complexity of the Confidential Informant Guidelines may discourage agents from opening CIs. One Criminal Division Chief commented, "The heightened rules and procedures have probably caused a reduction in the use of confidential informants." A senior field manager in one of the FBI's largest field offices stated, however, that "no good agent is going to let a good informant slip through the cracks because of paperwork."

**DIAGRAM 3.3**



The view that the paperwork requirements associated with handling informants excessively burden field agents was also cited in our interviews of FBI Headquarters personnel from the Criminal Investigative Division, Counterterrorism Division, Office of Intelligence, and Inspections Division. FBI Director Mueller told us that he frequently hears agents complain about the “burdensome” procedures for opening and operating informants.

In contrast, 10 of the 12 SACs in the field offices we visited said they believe the CI Guidelines are workable as written.<sup>227</sup> One senior field office manager said that “[t]he Guidelines are good, reasonable, and not a hindrance. They keep agents on track. Because of the Bureau’s past fiascos, we need controls. Sometimes agents get sidetracked.” Another senior manager told us that there was no excuse for agents in his office not

---

<sup>227</sup> In one field office, the SAC in place during the period of our review retired prior to our interviews. We therefore interviewed the ASAC responsible for the Criminal Informant Program. In another office, due to an emergency, the SAC was not available and we interviewed an ASAC.

to properly document compliance with the Informant Guidelines and that the Guidelines were not too complex. He stated that his informant program personnel complete the necessary documentation for the agents if asked and were prepared to answer any questions regarding the operation of informants. He characterized his agents as being “spoon-fed” on informant compliance issues. Notwithstanding the support available to agents in this field office, our review found that 100 percent of the informant files we reviewed in that office contained one or more Guidelines violations.

**TABLE 3.6**

**Views of 12 FBI Senior Field Managers  
on the Confidential Informant Guidelines**

<b>Question</b>	<b>Yes</b>	<b>No</b>	<b>Don't Know</b>	<b>No Response</b>
- Are the CI Guidelines well understood in the field?	10	2		
> Are the Guidelines workable?	10	0		2
> Are the Guidelines too complex?	6	5		1
- Is the paperwork needed to comply with the CI Guidelines and MIOG too cumbersome?	8	4		
- Do agents complain about the CI Guidelines?	9	0	3	
- Do you think if Headquarters provided standardized forms like they do travel vouchers that could be completed on-line, it would make life easier and achieve better compliance?	12	0		

In the course of reviewing 120 informant files in 12 field offices, we were mindful of these concerns and sought to examine whether the reason for the complaints is the Guidelines themselves; other reasons that make compliance overly complex, time-consuming, and difficult; or a combination of these factors. After evaluating the requirements of the Confidential Informant Guidelines and how they work in the field, we share the view of the majority of SACs we interviewed that the Guidelines themselves are not overly burdensome. Instead, we believe that the significant reasons for non-compliance are:

1. inadequate administrative support for the Criminal Informant Program, including the failure to provide standardized forms, a field guide, and Intranet tools;
2. failure by executive managers to hold first-line supervisors accountable for compliance deficiencies and to exercise effective oversight of agents operating confidential informants;



3. inadequate training at every level (new agents, probationary agents, experienced agents, Confidential Informant Coordinators, Supervisory Special Agents, senior field managers, and key Headquarters personnel), including periodic training on the Guidelines themselves and joint training with the U.S. Attorneys' Offices on appropriate methods to operate confidential informants;
4. inadequate support of Confidential Informant Coordinators and assignment of this responsibility as a collateral duty;
5. failure to take compliance performance into account in personnel and promotion decisions and policies; and
6. lingering differences between the FBI and DOJ over informant issues.

Below we address each of these issues.

**1. Inadequate Administrative Support.** As has been well documented, the FBI has struggled to upgrade its antiquated computer systems for many years.<sup>228</sup> However, we found that a principal reason for the serious compliance deficiencies in the Criminal Informant Program is the FBI's failure to use its currently available automated support tools to enable agents and their supervisors to complete the necessary paperwork for operating their confidential informants on a consistent and timely basis.

Our interviews, field office site visits, and analysis of documents produced by the FBI reveal that three years after the May 2002 revised Investigative Guidelines were issued, FBI agents do not have FBI-wide, standardized forms to support the administrative steps required to operate confidential informants. The FBI is capable of producing such forms; indeed, there is widespread use of automated forms throughout the FBI to support a host of administrative and operational programs.<sup>229</sup> Nonetheless, in seeking approval for and operating informants, field agents in May 2005 still use hand-me-down forms (called "ponies") developed by either their field office or another field office. Some of these forms are out of date and some

---

<sup>228</sup> See OIG Audit Report, *The Federal Bureau of Investigation's Management of the Trilogy Information Technology Modernization Project*, Report No. 05-07 (Feb. 2005); OIG Audit Report, *Federal Bureau of Investigation's Management of Information Technology Investments*, Report No. 03-09, December 2002; OIG Audit Report, *Federal Bureau of Investigation's Implementation of Information Technology Recommendations*, Report No. 03-36, September 2003.

<sup>229</sup> For example, case agents and Headquarters personnel use standardized and automated forms to submit applications for consensual recordings and for approval of myriad administrative tasks such as leave and expense reimbursement requests.

are under-inclusive or over-inclusive in what they require.<sup>230</sup> In addition, field agents and supervisors routinely are transferred from one field office to another throughout their careers. Because of the different practices used by the FBI's field divisions to administer the Criminal Informant Program, transferred agents must make needless, time-consuming adjustments to the unique, sometimes outdated, requirements of their new offices.

The following table illustrates the wide discrepancies in data pertaining to Confidential Informant Guidelines' requirements that is collected in various forms maintained in 7 of the 12 field offices we visited.<sup>231</sup>

---

<sup>230</sup> For example, CI instruction forms or "ponies" used since May 30, 2002, from three field offices still required the agent to read the instructions to the CI verbatim, a provision that was relaxed in the May 2002 Confidential Informant Guidelines. Also, virtually all field offices cite the MIOG exclusively as authority for various requirements in their "ponies," but the MIOG is still not yet fully compliant with the Guidelines, as we document in Chapter Eight.

<sup>231</sup> In four of the remaining five field offices, the ISR&R ponies contained all the required suitability elements. In the fifth field office, none of the files we examined required an ISR&R.

**TABLE 3.7**

**Suitability Elements Missing from Initial Suitability Reports & Recommendations (ISR&Rs)  
in Select FBI Field Offices**

Field Office CI File Numbers	PONY DATE	Date Form Completed	Extent CI's information would be relevant	Nature of relationship between CI & investigation's subject	CI's motivation to provide information	Risk CI might have on investigation, prosecution	Extent the CI's information can be corroborated	CI's reliability & truthfulness	CI's prior record as a witness	CI pose a danger to the public or risk of flight	CI history of substance abuse	Does CI have relative who is a law enforcement employee	Any risk of harm to CI or family due to providing information	Any record of prior or current CI, CW service	CI's criminal history, target investigation, under arrest or charged
Field Office 1	12	07/31/01	11/14/02	X	X	X	X	X	X	X	√	X	X	√	√
Field Office 2	4	03/31/95	12/08/03	X	X	X	X	X	X	X	X	X	X	√	√
Field Office 2	7	03/31/95	01/28/03	X	X	X	X	X	X	X	X	X	X	√	√
Field Office 6	11	08/28/00	06/14/02	X	X	X	X	X	X	X	X	X	X	X	√
Field Office 6	13	02/01/03	06/06/03	X	X	X	X	X	X	X	X	X	X	X	√
Field Office 6	15	08/28/00	08/09/02	X	X	X	X	X	X	X	X	X	X	X	√
Field Office 7	12*	02/11/02	01/15/03	√	√	√	√	√	√	√	√	√	√	√	√
Field Office 8	12	06/19/01	12/18/02	X	√	√	√	√	√	√	√	√	√	√	√
Field Office 9	19	10/01/99	08/15/02	X	X	X	X	X	X	X	X	X	X	√	√
Field Office 9	20	10/01/99	07/30/02	X	X	X	X	X	X	X	X	X	X	√	√
Field Office 10	6	12/31/95	03/07/03	X	X	X	X	X	X	X	X	X	X	√	√
Field Office 10	10	12/31/95	06/05/02	X	X	X	X	X	X	X	X	X	X	√	√
Field Office 10	12	12/31/95	10/09/02	X	X	X	X	X	X	X	X	X	X	√	√

\*Field Office 7 had 2 ISR&R forms in File Number 12 - one was dated 02/11/02, but the date on the other form was illegible

X

Element was missing from the pony

√

Element was on the pony

Complicating the agent's task even further is the fact that there is no one place on the FBI's Intranet where an agent who wants to initiate the registration of an informant can look for guidance regarding the approval and operation of CIs. During the period of our review, the current Confidential Informant Guidelines were available on the OGC's web site, an outdated version of the Informant Guidelines was on the Asset/Informant Unit's web site, the MIOG was on another FBI Intranet site, and agents had to search for forms on their field office's local computer system. Consequently, it is easy to understand the frustration expressed by field office personnel in explaining compliance deficiencies when it is so difficult for agents to find the various requirements, and standardized administrative tools are not available.

Another impediment to compliance with the Guidelines is the absence of a field manual comparable to the one provided for undercover operations by the Undercover and Sensitive Operations Unit (USOU), which we discuss in Chapter Four.<sup>232</sup> Instead of having a useful document which captures the key Guidelines' and MIOG requirements for opening and operating informants, agents must depend on the initiative of their Informant Coordinators, Division Counsel, or other field personnel to obtain necessary paperwork and guidance in opening and operating informants. Several field offices, including Newark and Knoxville, have generated their own handbooks or manuals to fill this void. However, the best practices and time-saving devices that have evolved over the years in the field have not led to the development of a uniform field guide for all agents.<sup>233</sup>

Confidential file room analysts, whose role supporting the administration of all human sources is discussed above, play a critical role in assisting field agents in complying with the Guidelines. Some analysts have instituted tickler systems and other mechanisms to promote timely compliance. While this support is helpful, we believe the FBI needs an agency-wide, standardized system which can be accessed at Headquarters and in the field.

As noted in the FBI's response to the OIG's recommendations (provided in Appendix G), the FBI states that the Directorate of Intelligence

---

<sup>232</sup> The MIOG is no substitute for such a manual. The current MIOG provisions regarding confidential informants span 67 pages of single-spaced text. Many agents and supervisors told us during this review that the MIOG is so unwieldy that it is either not used or is not a "user-friendly" tool to find guidance on registering or operating informants.

<sup>233</sup> One other shortcoming in Headquarters' administrative support deserves mention. The file review cover sheets used by the field offices we visited do not consistently provide adequate space to capture Guidelines and MIOG violations and do not provide space to facilitate follow-up entries to record whether the violations persisted or were resolved.

(DI) has initiated a “re-engineering” of its Confidential Human Source Program. Because its internal human source policies, practices, and manuals must account for and comply with the Attorney General’s Guidelines, the FBI enlisted DOJ to assist in the re-engineering effort. In December 2004, the FBI established a working group, including representatives from DOJ, to revise FBI policies regarding human sources (including confidential informants.) The working group’s goals are to develop new guidelines, policies, and processes for the utilization of confidential human sources that are designed to reduce burdensome paperwork, standardize source administration procedures, clarify compliance requirements, and improve Guidelines compliance.

**2. Failure by Executive Managers to Hold First-Line Supervisors Accountable for Compliance Deficiencies and Exercise Effective Oversight of Agents Operating Informants.** Headquarters officials, field managers, Informant Coordinators, and Division Counsel we interviewed identified the first-level supervisor as the linchpin to ensuring FBI agents are held accountable for compliance with the Confidential Informant Guidelines. Our review indicated, however, that some field supervisors have failed to identify risks associated with operating informants.

For example, Supervisory Special Agents (SSAs) are required every 90 days to conduct reviews of all confidential informant files, or, in the case of privileged informants, every 60 days. During this review, they are to note a variety of information, including Guidelines compliance deficiencies pertaining to payments, criminal history checks, authority to engage in otherwise illegal activity, and continuing suitability. MIOG § 137-4(3). We saw many instances where file reviews were not performed timely and deficiencies were not resolved promptly. In addition, we found some instances where the requests of the Informant Coordinator and/or SSA were not responded to by agents, as evidenced by repeated notations of non-compliance during file reviews. See also Chapter 7, Case Study 7.2 (describing conduct of SSAs in the San Francisco Field Office).

Beyond the general issue of timely compliance with the Guidelines, we believe, based on our field and Headquarters interviews and survey responses, that some field supervisors have historically failed to be as fully engaged as needed to identify risks associated with operating informants. Our findings with respect to supervisory approval and monitoring of “otherwise illegal activity” and notifications regarding the occurrence of unauthorized illegal activity are particularly notable in this regard.

With respect to otherwise illegal activity, as illustrated in Table 3.4 above, we found instances in which supervisors improperly authorized OIA prior to the source being converted to a registered informant (four files), authorized OIA for sources who were never registered as CIs (two files),

retroactively authorized OIA in contravention of the Guidelines (five files), or authorized OIA which did not meet the Guidelines' specificity requirements (seven files). In each of these instances, field supervisors failed to exercise their responsibility to ensure that, as supervisors, they followed these Guidelines' provisions.

The FBI's Criminal Investigative Division (CID) has also expressed concern about non-compliance issues identified by the OIG in the course of this review. Personnel from FBI Headquarters' Asset/Informant Unit accompanied the OIG during our field office site visits from May to August 2004 and reviewed the same data we reviewed with respect to confidential informant files. On November 8, 2004, the Assistant Director of CID sent a candid self-assessment to all FBI field offices, the apparent purpose of which was to communicate the Division's concerns about these compliance deficiencies and to clarify related field guidance. Among its conclusions, the CID stated that one of the factors contributing to the present state of the Criminal Informant Program was "a failure on the part of field office managers to effectively exercise oversight" of the program. In particular, with respect to the critical role executive managers and supervisors play in approving otherwise illegal activity, CID made the following observation:

[Executive managers] and Supervisors, when reviewing reauthorizations, must ensure OIA authority requested is commensurate with the completed activity, for example, the previous OIA was to purchase drugs; however, during the authorization period, the source also purchased weapons. Subsequent justification, authority and concurrence must extend to weapons. Given the guideline definition and the role of CIs, [Executive Managers] and Supervisors must closely scrutinize the use of CIs in OIA or any other operational activity.

The CID's November 8, 2004, memorandum also noted a variety of other compliance errors uncovered by the OIG review regarding authorizations of OIA that should have been noted and corrected by the contact agents' supervisors:

There were instances noted wherein OIA authority was not current, commensurate and/or specific to the operational activity actually being conducted. There were instances noted wherein requests for OIA authorization did not include sufficient justification and failed to note, with specificity, the activity(ies) authorized for the source. There were instances wherein AUSA concurrence was not obtained and/or not confirmed by letter to the United States Attorney's Office (USAO). There were instances in which OIA admonishments were backdated, completed by an agent other than the agent

administering the admonishments, not administered within the authorized time frame, or simply not administered.

Cause: The assessment identified the following as factors contributing to the rate of non-compliance in this area: Lack of familiarity with guidelines' requirement; a deficiency on the part of Executive Managers to exercise adherence to and oversight of guidelines requirements; and a failure to recognize the implications of providing a "blank check" endorsement for a source to participate in criminal activity. (Emphasis in original).

Among CID's general conclusions were that "despite the identification of non-compliance issues, there was a high rate of recurrence or failure to remedy those identified issues" and that "outside of mitigation, there was no accountability for identified non-compliance in the program."

With regard to unauthorized illegal activity, first-line supervisors play an important role in responding to CI participation in unauthorized illegal activity and ensuring that appropriate notifications are made either to a U.S. Attorney or to the DOJ Criminal Division. We found two instances in which required notifications did not go to the U.S. Attorney's Office at all and three occasions when the required notification either did not go from the SAC or to the U.S. Attorney, or both. This deficiency was also noted in the CID's November 8, 2004, memorandum which found that "files were devoid of any FBI/USAO interaction." Moreover, it was not possible to ascertain from the case file in approximately one-third of the cases we examined that involved unauthorized illegal activity whether notification to the U.S. Attorney was required. This was due primarily to the lack of information concerning whether a state or local prosecuting office had filed charges against the informant.

We believe it is critically important for FBI supervisors and Headquarters officials to be aware when CIs engage in unauthorized illegal activity and to exercise oversight to ensure that agents do not inappropriately insert themselves into state or local proceedings against the informant or otherwise act inappropriately when FBI informants are at risk. In addition, it is important that the FBI not continue its relationship with informants who, on balance, present greater risks than benefits. Because the Guidelines provide that the U.S. Attorneys' Offices and the DOJ's Criminal Division are to bring their judgments to bear on whether the FBI should continue to utilize CIs who have committed unauthorized illegal activity, it is important that FBI supervisors ensure that prosecutors are notified as required. The FBI's failure to track whether state or local

charges have been filed against CIs who commit unauthorized crimes is a significant gap in its oversight of confidential informants.<sup>234</sup>

The Guidelines deficiencies noted above demonstrate that some supervisors are not properly conducting file reviews, are not resolving deficiencies promptly, and, with respect to certain of the FBI's most consequential decisions involving the authorization of otherwise illegal activity and continuation of the informant relationship in the event the informant commits unauthorized crimes, are not providing requisite notice to the prosecuting authorities. We believe that the failure of some executive managers to ensure that first-line supervisors and ASACs are held accountable for Guidelines violations by those under their supervision should be remedied promptly.

**3. Inadequate Training at Every Level.** We believe that another reason for the FBI's high non-compliance rate with the Confidential Informant Guidelines is the absence of regular training of field agents and supervisors on the risks of handling confidential informants, failure to identify best practices to use in managing informants, and the absence of joint training with the U.S. Attorneys' Offices.

We outline in Chapter Eight our concerns about the FBI's failure to develop and implement a comprehensive training program to acquaint field agents, their supervisors, and Headquarters personnel with the requirements of the four Investigative Guidelines. With respect to the Confidential Informant Guidelines in particular, the FBI was provided specific direction concerning training. Section I.I.1 of the May 30, 2002, CI Guidelines states:

- I. Compliance
1. Within 120 days of the approval of these Guidelines by the Attorney General, each JLEA shall develop agency-specific guidelines that comply with these Guidelines, and

---

<sup>234</sup> We were told by field agents and the A/IU that one source of confusion about when notification of the U.S. Attorney's Office is required is the meaning of the phrase "participating in the conduct of an investigation that is utilizing that active CI, or is working with that active CI in connection with a prosecution" in § IV.B.1 of the CI Guidelines. In its November 8, 2004, memorandum, CID acknowledged the confusion and issued clarifying guidance stating that the phrase meant "that stage when a prosecutor begins providing **prosecutorial** guidance/direction, and not the stage of an initial investigatory or prosecutorial opinion (emphasis in original)." See also *Genzler v. Longanbach*, 384 F.3d 1092 (9<sup>th</sup> Cir. 2004) (affirming district court finding that a prosecutor and investigator were not entitled to absolute immunity from § 1983 claims arising from their actions during a joint meeting with a witness because they were performing an investigatory rather than an advocacy function).



submit such agency-specific guidelines to the AAG for the Criminal Division for review. The agency specific guidelines must ensure, at a minimum, that the JLEA's agents receive sufficient initial and in service training in the use of CIs consistent with these Guidelines, and that compliance with these Guidelines is considered in the annual performance appraisal of its agents. As part of such compliance the JLEA shall designate a senior official to oversee all aspects of its CI program, including the training of agents; registration, review and termination of CIs; and notifications to outside entities.

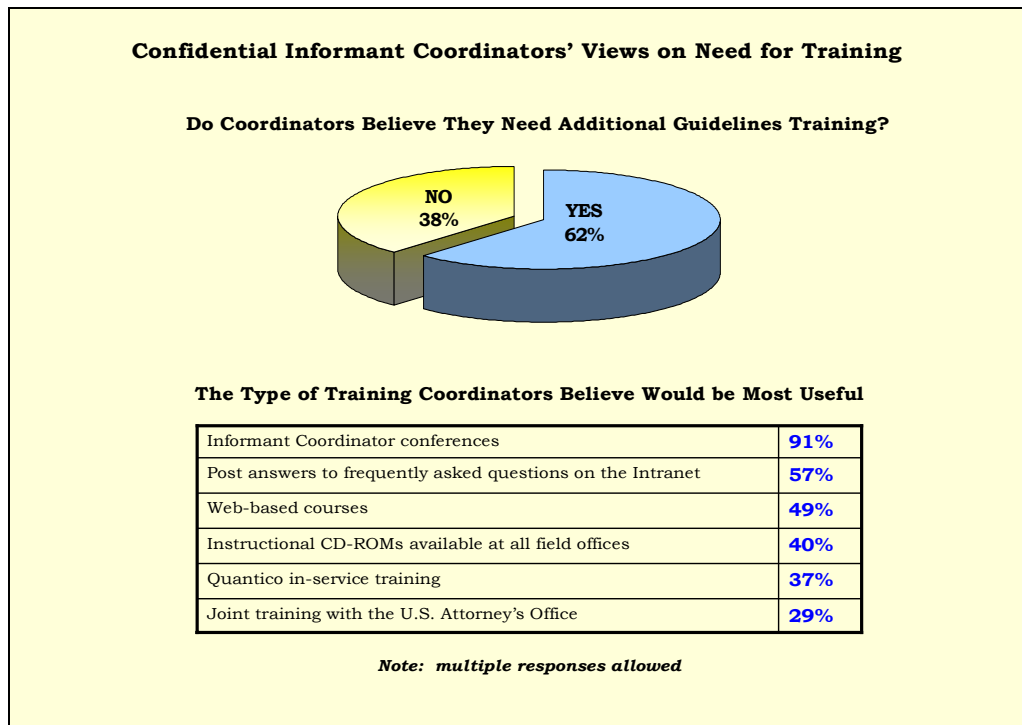
The FBI has taken some steps to provide training to its employees on the CI Guidelines. In November 2003, FBI Headquarters initiated a mandatory "Back to Basics" lesson plan for all assigned Special Agents, including managers, on the operation of human sources. The A/IU told us that it has provided 33 training sessions in support of the Criminal Informant Program from October 2003 to March 2005. These sessions included 80 hours of training for approximately 15 Confidential Informant Coordinators and other field personnel who were assigned to Headquarters about the administrative oversight of informants and other human sources. The FBI provided blocks of instruction on source administration in nine regional training sessions for a total of approximately 500 Supervisory Special Agents, Special Agents, and task force officers between May 2003 and October 2003, and five Informant Development in-service training sessions between January 2003 and February 2004 for a total of approximately 200 experienced Special Agents. Prior to the June 2003 training session, the last in-service advanced training provided on informant development was in September 1999.

In addition, from June 2002 through June 2003, the Office of the General Counsel (OGC) provided training on all four Investigative Guidelines to one field division. It also provided a block of training on the CI Guidelines at a specialized conference on health care fraud and at a white collar crime conference for ASACs. OGC provided training on the Informant Guidelines at the Informant Development in-service course in June 2003, noted above. In addition, Chief Division Counsel received training from OGC on the revised CI Guidelines in January 2003, at a Chief Division Counsel conference at FBI Headquarters.

At the field level, Informant Coordinators told us that they have conducted formal and informal training sessions, posted information about the revised Guidelines on field office computer systems, and distributed answers to frequently asked questions.

Yet, despite these training efforts, our review found that more training is needed to improve compliance with the Guidelines. For example, Confidential Informant Coordinators do not have a regular training regimen. They do not meet on an annual basis, and there are no regional or local training opportunities that focus on Guidelines issues.<sup>235</sup> When we asked Confidential Informant Coordinators whether they believe they need additional training on the Guidelines, the majority reported that they did, as the following diagram shows.

**DIAGRAM 3.4**



Informant Coordinators also believe that FBI personnel need additional training on the Confidential Informant Guidelines. Seventy-two percent of the Informant Coordinators indicated that Division Counsel should provide additional training on the CI Guidelines to Special Agents and supervisors in their field offices. Several Informant Coordinators suggested that training go beyond simple instruction on what the Guidelines require. For example, one Informant Coordinator said:

---

<sup>235</sup> The first Confidential Informant Coordinator Conference held after the May 2002 Guidelines was in January 2003. The next conference was in August 2004.

We have many new agents in the Bureau. Most of them, I feel, look at a source as a necessary evil instead of a valuable tool towards investigative success. I try to counsel new agents that working sources can be interesting and somewhat enjoyable, and certainly can be a huge help to any investigation. Training towards that end, i.e., helping the new agents to look at sources as an interesting and maybe even fun part of the job could help bring new agents along the right path.

The Informant Coordinators' views on the need for additional training were shared by Division Counsel, whose responses to our survey indicated a need for additional training of agents, supervisors, and Division Counsel.

**TABLE 3.8**

**Division Counsel's Views on Need for Training  
on Confidential Informant Guidelines**

Question	Response	
Indicate who you believe needs additional training in your field office for each of the revised Guidelines.	<b>Attorney General's Guidelines on the Use of Confidential Informants (Check all that apply.)</b>	
	All Special Agents	30 59%
	All squad supervisors	21 41%
	None	17 33%
	SACs	8 16%
	Other	5 10%
Indicate the type of additional training you believe would be most useful in your field office for each of the revised Guidelines.	<b>Attorney General's Guidelines on the Use of Confidential Informants (Check all that apply.)</b>	
	Virtual Academy Training (Web-Based)	21 41%
	Communications posted on the Intranet	19 37%
	Post FAQs on the Intranet	14 27%
	Training by FBIHQ Program Managers	14 27%
	Training by the CDC/ADC	13 25%
	CD-ROMs available in all field offices	13 25%
	Other	9 18%
	None	8 16%
	Training by FBIHQ OGC	4 8%
Do you believe that CDCs/ADCs now need additional training on the revised Guidelines?	<b>Attorney General's Guidelines on the Use of Confidential Informants (Check all that apply.)</b>	
	Training by FBIHQ OGC	33 67%
	Communications posted on the Intranet	23 47%
	CD-ROMs available in all field offices	22 45%
	Virtual Academy Training (Web-Based)	20 41%
	Post FAQs on the Intranet	18 37%
	Training by FBIHQ Program Managers	12 24%
	Other	3 6%
	None	1 2%

In addition to these survey findings, some FBI personnel believed that ambiguities or lack of sufficient detail in some of the Guidelines' requirements were impediments to compliance, and that clarification and supplemental guidance are needed. For example, field and Headquarters personnel indicated in response to our survey and in interviews that the FBI should issue clarifying guidance regarding the following issues.

- Does the notification requirement triggered by the phrase “participating in the conduct of an investigation” in § IV.B of the Guidelines relating to unauthorized illegal activity (UIA) apply to UIA occurring in the initial investigative stages or only when the U.S. Attorney’s Office begins to exert direction and control of the investigation?
- Should CIs who are physicians or in other “privileged” categories under § II.D.2 of the Guidelines require Headquarters approval if the sole basis for them providing information has nothing to do with their privileged status?
- What controls should be instituted to maximize the reliability of online communication with confidential informants?
- What is the appropriate use of illegal aliens as confidential informants?

In addition, the CID’s November 8, 2004, self-assessment acknowledged that specific shortcomings in FBI training have impacted the operation of confidential informants. The CID assessment concluded that agents were not well-informed about the need to comply with time-sensitive Guideline requirements such as instructions, initial suitability inquiry periods, and the annual continuing suitability reviews. CID concluded that agents had a “misconception regarding the flexibility of time-sensitive issues” and wrongly “assumed that there is a ‘grace period’ associated with deadlines in the Asset and Informant Programs.” The CID assessment also noted a “lack of familiarity” with the Guidelines’ requirements regarding otherwise illegal activity.

**4. Collateral Duties and Inadequate Support of Confidential Informant Coordinators.** Confidential Informant Coordinators play a critical role in ensuring that the Guidelines are followed. However, we learned that 28 of 56 Informant Coordinators, or 50 percent, perform these duties as a “collateral duty” while handling other assignments. A prominent issue that arose in our survey was the frustration of some Coordinators with the competing demands of these other duties. In our survey, 41 percent of Informant Coordinators reported that they do not have sufficient time to manage the Criminal Informant Program in their field offices, and 78 percent of these Coordinators attributed this to “too many collateral duties.”

Moreover, 50 percent of the Informant Coordinators responded that the FBI should direct SACs in large field offices not to assign additional collateral duties to Informant Coordinators. While we believe that not all field offices can justify having a full-time Informant Coordinator, the FBI should consider the workload of Informant Coordinators in large field offices and whether they have sufficient time to handle their critical duties as Informant Coordinators.

We also heard from both Informant Coordinators and executive managers that it would substantially assist the effectiveness of Informant Coordinators in larger field offices if executive managers had the discretion to elevate the Informant Coordinator position to a GS-14 supervisory position. Particularly in larger field offices, the challenges confronting Informant Coordinators in assisting agents and in being available to address problems and mitigate risks involving informants, may be sufficiently complex and sophisticated that they merit a GS-14 supervisory level appointment.<sup>236</sup> Of the 12 SACs we interviewed at the conclusion of our review, two-thirds favored giving executive managers in large field offices the discretion to elevate the position to a GS-14 supervisory position. One SAC of a large field office commented that unless this option is available, it will be difficult to attract and retain good Informant Coordinators.

We also found that the effectiveness of the Informant Coordinator varied greatly depending on a variety of factors. We observed that the most successful Informant Coordinators were those who had sought the job, had credible experience handling informants as case agents, had good working relationships with their SACs and ASACs, had strong organizational skills, and remained in the position for a sufficient period of time. In contrast, some Informant Coordinators selected for the position had no particular experience with informants or interest in the position. Moreover, there is notable turnover in these positions; according to A/IU, approximately

---

<sup>236</sup> Effective September 12, 2003, Informant Coordinators report to the head of the Field Intelligence Group (FIG), which consolidates all intelligence capability at the field level. In some instances, the head of the FIG is a supervisor who has no criminal investigative experience. As a result, some field offices have adopted a dual reporting requirement for Informant Coordinators: they report to the FIG for intelligence-related duties and to the ASAC-Criminal for informant duties.

It was beyond the scope of this review to offer recommendations on the impact of this new chain of command on the effectiveness of Informant Coordinators. However, we believe that any managerial steps that diminish the attractiveness or importance of the position could have an adverse impact on Guidelines compliance. We believe that executive managers should, at a minimum, be certain that the Informant Coordinators report to a supervisor with adequate experience in the Criminal Informant Program to provide effective guidance, oversight, and support.

one-third of Informant Coordinators today are different from those in place on May 30, 2002.

One SAC expressed concern that resource constraints were prompting discussion about appointing non-agents to be Informant Coordinators, a move that he did not believe would be consistent with Guidelines compliance.<sup>237</sup>

**5. Failure to take Account of Compliance Performance in Personnel and Promotion Decisions and Policies.** The January 2001 revisions to the Confidential Informant Guidelines mandated that agency-specific guidelines “ensure, at a minimum . . . that ‘compliance with these Guidelines is considered in the annual performance appraisal of its agents.’”<sup>238</sup> This requirement was unchanged in the May 30, 2002, revisions. CI Guidelines, § I.I.

We examined the performance plans for Special Agents that were in effect from May 30, 2002, to April 1, 2005, and found that the FBI’s annual performance appraisals did not contain this mandated critical element. The only reference to the Attorney General Guidelines in the performance plans for GS-10 to 15 Special Agents (and a corresponding provision for Senior Level Special Agents) during this period is a generic reference in the first critical element, which states:

Makes decisions in accordance with existing policies and procedures (e.g., follows Attorney General guidelines).<sup>239</sup>

During this same period, the “intelligence base” critical element for GS-15 and Senior Level Special Agents required these agents to “review suitability assessments of individuals for use in investigative or covert operations (e.g., informants, cooperating witnesses, assets) and ensures compliance with appropriate policies and procedures.”

As our review was being completed, the performance plan for Special Agents was revised effective April 1, 2005, to contain a critical element for

---

<sup>237</sup> Because the pool of possible candidates for the Informant Coordinator position is often limited, we heard widespread support for the suggestion that the FBI bring back retired FBI agents with strong, credible “street” experience in handling informants to serve as Informant Coordinators.

<sup>238</sup> January 2001 Informant Guidelines § I.I.

<sup>239</sup> By contrast, during this same period, the “intelligence base” critical element for GS-15 and Senior Level Special Agents required these agents to “review suitability assessments of individuals for use in investigative or covert operations (e.g., informants, cooperating witnesses, assets) and ensure compliance with appropriate policies and procedures.”

all GS-10 through 13 Special Agents that references compliance with the “Attorney General Guidelines.”<sup>240</sup> Similar performance standards were added in April 2005 for GS-14/15 Special Agents. However, the performance standards for Senior Level Special Agents do not incorporate any requirement to effectively manage and oversee compliance with the CI Guidelines.

Thus, since the January 2001 Confidential Informant Guidelines became effective, and today, the FBI is still not in compliance with § I.I of the CI Guidelines because there is no provision in the performance standards for all FBI agents and supervisors stating that compliance with the CI Guidelines will be considered in their annual performance appraisals.

FBI agents who operate informants are credited with “statistical accomplishments” for the contributions the CIs make to investigative activities. We learned that some Informant Coordinators, SACs, and Headquarters officials are not satisfied with the manner in which personnel policies account for the operation of human sources. Throughout the period of this review and until 2005, FBI personnel were subject to a two-tiered evaluation system that limited supervisors to rating their subordinates as “meeting expectations” or “not meeting expectations.”<sup>241</sup> Several Headquarters officials and executive managers told us that when using this rating system, they would evaluate supervisors as “meeting expectations” even though they failed to properly discharge their duties under the CI Guidelines.

As noted below, notwithstanding the generic critical element relating to the “Attorney General Guidelines” for GS-14 and Senior Level Special

---

<sup>240</sup> The performance plan now provides:

Critical Element 7: Intelligence

Performance Standards:

With appropriate guidance, collects, processes, documents and disseminates intelligence related to FBI investigative and national intelligence priorities, in accordance with the authorities and mandates governing the intelligence functions of the FBI (National Security Act of 1947, Executive Order 12333, **Attorney General Guidelines**, Intelligence Reform and Terrorism Prevention Act of 2004, etc.).

With proper direction, produces and/or supports the production of appropriate intelligence products (e.g., assessments, bulletins, Intelligence Information Reports (IIRs)) in accordance with established guidelines, while ensuring the dissemination of the products to relevant customers (emphasis added).

<sup>241</sup> Effective November 1, 2004 and April 1, 2005, respectively, the rating levels for Supervisory Special Agents and Special Agents contain the following gradations: outstanding, excellent, fully successful, minimally satisfactory, and unacceptable.

Agents in effect for the last five years, we found that senior field managers do not consistently hold first-line supervisors accountable for Guidelines violations or even for persistent non-compliance. We were told in our interviews of the 12 SACs whose field offices we visited that most have taken or would take into account in weighing an SSA's promotion potential whether the supervisor was ineffective in promoting compliance with the Guidelines by agents under their command. However, judging by the number and range of CI Guidelines violations we found, we do not believe that Headquarters management has made compliance performance a sufficiently visible issue at either the agent or supervisory level by integrating a satisfactory compliance record into the FBI's performance reviews and promotion policies. We believe that the FBI should explicitly state in the performance plans for GS-15 and Senior Level Special Agents that compliance or overseeing compliance with the CI Guidelines is a critical element. In addition, we believe that the performance plans for GS-15 and Senior Level Special Agents should be modified to evaluate senior managers on their own compliance with the requirements of the CI Guidelines and their effectiveness in ensuring compliance by their subordinates.

Another issue we explored was the reward and incentive structure for Informant Coordinators. Most of the SACs we interviewed said that the current system for providing incentives to Informant Coordinators through quality step increases, awards, and promotions is adequate. Other SACs said they believed it would be helpful to supplement the current recognition methods by affording them the authority to make annual awards of \$1,000 to Informant Coordinators, similar to their authority to award "principal relief supervisors." See MAOP § 5-15.5. Some Informant Coordinators said the task of promoting compliance with the Guidelines is time-consuming, often thankless, and tedious work, and should be recognized more often. Many suggested that the FBI should make greater use of recognition ceremonies, Quality Step Increases, and cash awards both for highly effective Informant Coordinators and for agents who are exceptional performers in handling informants.

**6. Lingering Differences Between the FBI and DOJ Over Informant Issues.** The revisions to the Confidential Informant Guidelines in January 2001 introduced wholesale changes into the manner in which informants are evaluated, approved, and operated. DOJ's role became much more significant, particularly through the establishment of the joint FBI-DOJ Confidential Informant Review Committee (CIRC), which approves certain sensitive types of informants.

As we discuss in Chapter Seven, the confidential informants who are vetted by the CIRC undergo thorough scrutiny that assesses the risk-to-reward considerations in operating high-level, long term, privileged, media-affiliated, and certain other informants. But the CIRC reviews only a small



percentage of the confidential informants opened and operated by the FBI. As for the balance of the FBI's informants and the day-to-day decisions agents must make to ensure they are compliant with the oversight mechanisms in the Guidelines, we believe another reason for the compliance irregularities we observed is the attitude towards DOJ oversight that persists with some FBI employees, coupled with a belief that the Guidelines are complex and burdensome.

We observed different perspectives on this phenomenon throughout this review. Most FBI executive managers and Headquarters officials we interviewed said they believe the Informant Guidelines are an essential tool for constraining the FBI's operation of informants, and most SACs and Headquarters officials we spoke with during this review defend the current version of the Confidential Informant Guidelines. However, some Informant Coordinators and field personnel we spoke to blame the DOJ for, in effect, punishing the FBI by imposing the burdensome Guidelines on the entire organization when there have been only a few aberrant episodes. In addition, we were told that some FBI agents continue to believe that the FBI "owns" its informants and resent any obligation to disclose their identities to prosecutors or be told that they should close an informant in some circumstances.<sup>242</sup>

When we asked a senior FBI official in the Office of the General Counsel about the utility of joint training on informant management so that agents would appreciate the complications that can arise if prosecutors are kept "in the dark" and prosecutors could appreciate the FBI's challenges, the idea was greeted with mixed reaction. The FBI official said it might be a good idea, as long as the U.S. Attorney's Office representatives were not "nervous Nellies." An experienced federal prosecutor told us that the FBI has the erroneous impression that the DOJ is too skittish about working with informants involved in criminal activity, and that this view perpetuates the FBI's reluctance to share information with prosecutors.

We were told by some FBI officials that the roots of this distrust stem from the FBI's historic concern that informants' identities may be jeopardized when prosecutors leave DOJ for jobs in the private sector, often as criminal defense counsel. Whatever its roots, it is critical that the FBI and DOJ continue their ongoing efforts to work collaboratively in managing

---

<sup>242</sup> A senior Headquarters official said that it makes sense operationally to document the occurrence of unauthorized illegal activity but the FBI should not be told by the U.S. Attorneys' Offices to close a source since the source still might be able to obtain quality information that would justify opening another investigation.

the FBI's Criminal Informant Program in accordance with the Confidential Informant Guidelines.

## **VIII. Recommendations**

As this report was being completed, the FBI was in the process of considering significant changes to the FBI's human source program. Regardless of whether the FBI retains the Criminal Informant Program as a separate program or integrates it into a more generic human source program, we believe the FBI needs to address the compliance deficiencies outlined in this report. We also believe that some of the case agents' frustration with the Informant Guidelines would be reduced if agents and their supervisors had better administrative support, management tools, and periodic training. We therefore recommend that the FBI take the following steps.

### **Develop and Implement a Compliance Plan**

(1) Develop a compliance plan for its human source program and an implementation plan to put the plan into practice. The compliance plan should specify the strategies that the FBI will employ to ensure compliance with applicable Guidelines governing the recruitment, validation, and operation of human sources and address issues such as administrative support (e.g., field guides, standardized forms, and "user-friendly" Intranet resources), training, technology, guidance, and accountability.

### **Provide Enhanced Administrative and Technical Support/Automation**

(2) Develop standardized forms to capture the most significant requirements of the Confidential Informant Guidelines and the FBI's Manual of Investigative Operations and Guidelines (MIOG) for operating confidential informants, including a standardized "file review" cover sheet for Supervisory Special Agents to use in examining the files for adherence to the Confidential Informant Guidelines and MIOG provisions relating to confidential informants. The FBI should also create an electronic Confidential Informant User's Manual comparable to the Field Guide for Undercover and Sensitive Operations. That manual should include compliance checklists and the standardized forms recommended above. The FBI should consider other administrative improvements to support the Criminal Informant Program, including a standard electronic Criminal Informant Program tickler system that can be deployed in all field divisions to generate non-compliance notifications to field and Headquarters managers, and an updated Intranet web page that includes the current version of the Confidential Informant Guidelines and key Office of the General Counsel guidance memoranda concerning confidential informants.

(3) Institute procedures to determine whether state or local prosecuting offices have filed charges against confidential informants who engage in unauthorized illegal activity to determine whether notification must be provided to the U.S. Attorney's Office in accordance with Section IV.B.1.a of the Confidential Informant Guidelines.

(4) Amend the forms used to authorize "otherwise illegal activity" to specify the thresholds referenced in Section I.B.10 that distinguish Tier 1 from Tier 2 otherwise illegal activity.

### **Make Personnel and Performance Plan Adjustments to Promote Adherence to the CI Guidelines**

(5) Revise the promotion policies and the performance plans for Special Agents and executive managers to indicate, where applicable, that compliance or overseeing compliance with the Confidential Informant Guidelines will be considered in employees' annual performance appraisals (in accordance with Section I.I.1 of the Confidential Informant Guidelines) and in promotion decisions.

(6) Evaluate the grade level of Special Agents who serve as Confidential Informant Coordinators and consider allowing Confidential Informant Coordinators to be elevated to a GS-14 supervisory level, particularly in larger field offices where the Coordinator is a full-time position. The FBI should also ensure that Confidential Informant Coordinators are supervised by personnel of a higher grade level who are familiar with the Criminal Informant Program and who have received training on the Confidential Informant Guidelines.

### **Provide Necessary Training**

(7) Consider holding annual Informant Coordinator Conferences similar to those provided to Undercover Coordinators. The FBI should also consider opportunities for local, joint training with representatives from U.S. Attorneys' Offices, which could address topics such as Guidelines provisions requiring approval, concurrence, or notice to the U.S. Attorneys' Offices; the adverse consequences of Guidelines' violations from the standpoint of the prosecution and the FBI; and "lessons learned" from past cases.

(8) Review the training modules now used in New Agent Training, probationary training, and in-service training for Special Agents and Supervisory Special Agents to ensure that the Confidential Informant Guidelines' requirements and risks of operating confidential informants are explained.

(9) Include in the periodic training of Supervisory Special Agents a component or module on the importance of file reviews to the Criminal Informant Program. The training should also address frequently occurring

violations of the Guidelines and MIOG provisions. A key objective of supervisory training should be on predictors of problems with confidential informants, such as long term confidential informants, confidential informants who have been assigned the same contact agents for an extensive period, confidential informants who are authorized to engage in otherwise illegal activity, confidential informants who have previously been deactivated “for cause,” and confidential informants who have been arrested or engaged in other unauthorized illegal activity while working as confidential informants.<sup>243</sup>

---

<sup>243</sup> A list of all the OIG’s recommendations made in Chapters Three through Eight of the report is attached at Appendix E.

[BLANK PAGE]

## **CHAPTER FOUR**

### **THE ATTORNEY GENERAL'S GUIDELINES ON FBI UNDERCOVER OPERATIONS**

Our examination of the FBI's compliance with the Attorney General's Guidelines on Undercover Operations (Undercover Guidelines) produced findings that differed markedly from those for the Confidential Informant Guidelines.<sup>244</sup> In contrast to the many compliance deficiencies we found in the Criminal Informant Program, our examination of the FBI's undercover operations identified comparatively few instances of non-compliance with the Undercover Guidelines. Although we noted several issues that merit further review by the FBI, we found that the FBI's organization and oversight of its undercover operations generally was effective.

Before discussing our compliance findings and our recommendations, we provide an overview of FBI undercover operations, the requirements of the Undercover Guidelines, and the May 2002 revisions to those Guidelines.

#### **I. Role of FBI Undercover Operations**

##### **A. The Need for Undercover Operations**

The Undercover Guidelines describe the importance of FBI undercover operations:

The use of undercover techniques, including proprietary business entities, is essential to the detection, prevention, and prosecution of white collar crime, public corruption, terrorism, organized crime, offenses involving controlled substances, and other priority areas of investigation.<sup>245</sup>

As we detailed in Chapter Two, the Undercover Guidelines were revised in 1982 following congressional hearings and press accounts critical of the FBI's ABSCAM undercover operation targeting official corruption in the early 1980s. At that time, FBI Director William Webster discussed the importance of undercover operations:

The kinds of crimes the FBI is giving high priority today – bribery, gambling, narcotics, theft of technology, other white collar violations – often require undercover work. They are so-called consensual crimes. There is a willing participant on each

---

<sup>244</sup> We provide in Appendix B a copy of the Undercover Guidelines.

<sup>245</sup> Undercover Guidelines § I at B-39.

side, so it is difficult to come up with someone willing to be a material witness to the crime. . . .

Undercover operations, usually coupled with a cooperating witness or an informant, permit us to get inside a criminal apparatus and stay there long enough to find out how it works and who the players are. Undercover work is an exceedingly cost effective method of getting at problems that could not be solved in any other way.<sup>246</sup>

According to Philip B. Heymann, former Assistant Attorney General in charge of the Criminal Division who later served as Deputy Attorney General:

From the prosecutor's perspective, undercover operations are extremely effective in aiding us to identify, prosecute and convict the guilty and to reduce the chances that innocent parties will be caught up in the criminal process. Undercover operations permit us to prove our cases with direct, as opposed to circumstantial, evidence. Instead of having to rely on . . . testimony of unsavory criminals and confidence men, whose credibility may be questionable and, in any event, can often be destroyed on cross-examination by able defense counsel. Instead, through undercover techniques, we can muster the testimony of credible law enforcement agents, often augmented by unimpeachable video and oral taps which graphically reveal the defendant's image and voice engaged in the commission of crime. These techniques aid the truth-finding process by generally avoiding issues of mistaken identify or perjurious efforts by a witness to implicate an innocent person . . . .<sup>247</sup>

---

<sup>246</sup> *Why the FBI Uses Undercover Agents*, U.S. News and World Report, Aug. 16, 1982, at 50. In the early 1980s, the FBI conducted about 400 undercover operations per year. The dangers involved in undercover operations are discussed in *FBI Undercover Guidelines: Oversight Hearings Before the Subcommittee on Civil and Constitutional Rights of the House Judiciary Committee, 97<sup>th</sup> Cong. 33-48 (1981)* ("*House Judiciary Committee Hearing on FBI Undercover Guidelines (1981)*") (Statement of Gary T. Marx, Professor of Sociology, Massachusetts Institute of Technology); *Hearing Before the Senate Permanent Subcommittee on Investigations, Senate Government Affairs Committee, 100<sup>th</sup> Cong. 13 (1988)* (Statement of Oliver B. Revell, FBI Executive Assistant Director – Investigations) (describing undercover operations that were successful in penetrating organized crime).

<sup>247</sup> *House Judiciary Committee Hearing on FBI Undercover Guidelines (1981)*, supra n.246 at 130 (statement of Philip B. Heymann, Assistant Attorney General, Criminal Division, Department of Justice).

Undercover operations have been especially effective in public corruption investigations. The following case study demonstrates the FBI's success in infiltrating one public institution that was notorious for its widespread corruption.

#### **Case Study 4.1: Operation Greylord**

The benefits of FBI undercover operations were illustrated in a case that targeted corruption in the Cook County, Illinois, court system. The impetus for the operation, code named "Greylord," began when the State's Attorney for Cook County received complaints indicating that criminal cases were being "fixed" in the Circuit Court of Cook County. These complaints were supported by a pattern of acquittals in cases involving particular judges and attorneys. After the U.S. Attorney was notified, the FBI initiated plans to conduct an undercover operation regarding these allegations. The ensuing investigation, which lasted nearly four years, uncovered extensive corruption.

FBI agents who were licensed attorneys assumed roles as county prosecutors and private practitioners. In addition, the FBI recruited a state prosecutor and a judge from southern Illinois who were temporally assigned to Cook County to deal with the backlog of cases there. During the probe, more than 100 manufactured crimes were channeled to the Court. Equipped with electronic surveillance devices, the undercover agents were able to record hundreds of incriminating conversations with judges and attorneys which revealed that judges routinely accepted bribes to dismiss cases and received kickbacks from attorneys for assigning cases to them. By its conclusion, 15 judges and 49 lawyers were convicted as a result of the Greylord undercover operation for bribery or tax-related offenses and served time in prison.

Under the current Undercover Guidelines, the FBI may employ undercover operations in preliminary inquiries, general crimes investigations, and both types of criminal intelligence investigations: racketeering enterprise investigations and terrorism enterprise investigations. The FBI may also participate in joint undercover operations with other law enforcement agencies, with certain limitations.<sup>248</sup>

---

<sup>248</sup> If a joint undercover operation is under the direction and control of another federal agency, the FBI does not need to comply with the Attorney General's Undercover Guidelines provided the other agency's process with respect to "sensitive operations" is "substantially comparable" to the process established under the Guidelines for the review of undercover operations by the Criminal Undercover Operations Review Committee (CUORC). Undercover Guidelines § III at B-40.



## **B. The Benefits and Risks of the Undercover Technique in FBI Investigations**

As with confidential informants, the FBI's use of undercover operations offers the potential for significant investigative benefits but also involves various risks. The Guidelines acknowledge that, "these techniques inherently involve an element of deception and may require cooperation with persons whose motivation and conduct are open to question, and so should be carefully considered and monitored."<sup>249</sup>

Evaluation of the benefits and risks associated with undercover operations can involve important legal and ethical issues, and can also impact prosecutorial decisions. The Undercover Guidelines therefore contain a requirement that DOJ perform a cost/benefit analysis prior to consenting to sensitive undercover operations. Section IV.F.2.b of the Undercover Guidelines states that the "appropriate Federal prosecutor" must furnish a letter in support of the Group I application to FBI Headquarters that "should include a finding that the proposed investigation would be an appropriate use of the undercover technique and that the potential benefits in detecting, preventing, or prosecuting criminal activity outweigh any direct costs or risks of other harm."

As described in Chapter Two, the Senate Select Committee to Study Undercover Activities of Components of the Department of Justice, convened in the wake of the ABSCAM investigation, highlighted the competing considerations associated with use of undercover operations:

The Select Committee finds that undercover operations of the United States Department of Justice have substantially contributed to the detection, investigation, and prosecution of criminal activity, especially organized crime and consensual crimes such as narcotics trafficking, fencing of stolen property, and political corruption. In this era of increasingly powerful and sophisticated criminals, some use of the undercover technique is indispensable to the achievement of effective law enforcement. . . .

The Select Committee also finds that use of the undercover technique creates serious risks to citizens' property, privacy, and civil liberties, and may compromise law enforcement itself. Even when used by law enforcement officials with the most honorable motives and the greatest integrity, the undercover

---

<sup>249</sup> Undercover Guidelines § I at B-39.

technique may on occasion create crime where none would otherwise have existed.<sup>250</sup>

After the Senate's report on ABSCAM in 1982, the FBI strengthened its controls on undercover operations. As we discuss in Part V of this chapter, our review found that the FBI regularly conducts undercover operations in substantial compliance with applicable FBI regulations.

The FBI uses the undercover technique in a broad array of cases, as the following examples illustrate.

- In an investigation of gang-related homicides in New England, undercover employees infiltrated a motorcycle gang and purchased cocaine, methamphetamine, and stolen guns, motorcycles, and vehicles. The undercover operation resulted in 17 convictions, the solving of a homicide, and the recovery of 11 stolen vehicles and 17 motorcycles.
- In an investigation of organized crime, 32 defendants were indicted in March 2005 and charged with numerous racketeering crimes and other offenses committed over more than a decade, including violent assault, extortion, loansharking, union embezzlement, illegal gambling, trafficking in stolen property and counterfeit goods, and mail fraud. Most of the defendants were members or associates of the Gambino Organized Crime Family of La Cosa Nostra, including its acting boss and underboss. Evidence developed during the investigation resulted from the undercover activities of an FBI agent who infiltrated the crime organization and was offered induction as a "made member."
- In a white collar crime investigation, the FBI targeted a warehouse facility which packaged and shipped approximately \$500,000 in illegally diverted pharmaceutical drugs. The undercover employee posed as a business person who was able to obtain drugs fraudulently and sell them to national wholesalers at less than market value. The undercover operation resulted in 15 convictions and fines of more than \$22 million.
- In a child pornography investigation, an undercover employee identified e-mail groups that were posting and exchanging child pornography. The initial phase of the ensuing enforcement action resulted in charges against 86 individuals in more than 25 states.

---

<sup>250</sup> See *Final Report of the Senate Select Committee to Study Undercover Activities of Components of the Department of Justice*, S. Rep. No. 97-862, at 11 (2d Sess. 1982).

While the FBI has achieved significant benefits through undercover operations, the potential risks are also present.<sup>251</sup> The Undercover Guidelines require the FBI and DOJ to routinely address risk factors in undercover operations such as:

- agent safety;
- damage to public institutions through manipulation of, or interference with, political and administrative processes;
- injury to the targets of undercover operations by, for example, needlessly harming their reputations;
- improper execution of the undercover operation that establishes a defense to prosecution, such as entrapment or outrageous government conduct;<sup>252</sup> and
- damage to third parties, such as financial loss and criminal victimization caused by the undercover operation's generation of crime.

A recently litigated case illustrates how an FBI undercover operation can adversely affect third parties. As explained in Case Study 4.2 below, in *Brown v. Nationsbank Corp.*, 188 F.3d 579 (5<sup>th</sup> Cir. 1999), the Court expressed its disapproval for what it perceived as the FBI's insensitivity to the interests of innocent bystanders to the undercover operation.

---

<sup>251</sup> See also *FBI Undercover Operations: Final Report of the Subcommittee on Civil and Constitutional Rights, Committee on the Judiciary, 98<sup>th</sup> Cong. 14-35 (1984)* (discussing the dangers of undercover operations).

<sup>252</sup> With entrapment, defendants claim that the undercover agents induced them to commit crimes for which they were not predisposed. Undercover Guidelines § V.A at B-54. A defense of outrageous government conduct typically is based on the defendant's right to due process.

#### **Case Study 4.2: Operation “Lightning Strike”**

The litigation in *Brown* resulted from an FBI undercover operation called “Lightning Strike,” which was initiated in 1991 to investigate contract procurement fraud and other illegal activity in the aerospace industry. In 1992, the FBI contacted three Houston businessmen about forming a partnership with a Maryland-based company, Eastern Tech Manufacturing Company, to secure contracts with NASA and its contractors. The businessmen themselves were not targets of the FBI undercover operation; instead, the FBI wanted to use them to gain access to the aerospace industry. 188 F.3d at 583. As the undercover operation unfolded, the FBI offered one of the businessmen a job as Chief Financial Officer and Vice President of Marketing of another company, Space Inc., and promised multi-million dollar loans to all three in support of their existing businesses. During 1992 and 1993, the businessmen were extensively involved in the preparation of bids for Space, Inc., and introduced FBI agents to managers at NASA and many leading aerospace manufacturers. According to the Court, the businessmen “were unaware that they and their companies were being set up by the FBI as tools of deception in an undercover operation.” *Id.* at 583.

At the end of 1992, the FBI offered one of the businessmen, Brown, an opportunity to develop an exclusive resort in the Bahamas. After he dissolved his business relationship with his partners and made arrangements to sell his home, the FBI tried to persuade Brown to become an unpaid informant. The FBI directed one of his associates to deliver a sealed envelope to him with “entertainment funds” with instructions to meet another party at a hotel. Brown complied, and the FBI recorded the transaction. In its opinion, the Court stated:

Attempting to convince Brown to work as an unpaid undercover informant to set up stings, the FBI agents physically and psychologically intimidated Brown. On numerous occasions throughout August and September, 1993, the agents questioned Brown for multiple hours without the presence of an attorney and detained him against his will. Brown was threatened with prosecution of twenty-one different crimes, which could result in sixty years imprisonment and over a million dollars in fines.

*Id.*

In 1994, the FBI shut down Lightning Strike. Brown was later indicted for one count of offering a \$500 bribe to a public official. His trial on that charge resulted in a mistrial. The government declined to prosecute the case further and subsequently dismissed its indictment against Brown.

In 1996, Brown and his two associates filed suit against the FBI in U.S. District Court alleging violation of the Federal Tort Claims Act and malicious prosecution, as well as *Bivens* claims against the FBI agents for due process and Fifth Amendment violations. The district court dismissed the action, and the plaintiffs appealed. Although the Court of Appeals affirmed the district court's dismissal, it included the following analysis addressing the qualified immunity defense to *Bivens* claims:

No court has addressed the particular issue presented by this case: the specific limits on federal agents' authority in undercover operations. The district court found no limits on the power of federal agents operating undercover, reasoning that if Appellants are allowed to pursue state law causes of action it would 'effectively stop' federal undercover operations because, 'by their very nature [they] seek to invade the privacy of those who violate the law.' . . . The district court should have asked whether it was constitutionally permissible for federal agents to inflict damages on innocent non-targets during an undercover operation and refuse them compensation. Because the Fifth Amendment due process guarantee against conscience-shocking injury imposes clear limits on law enforcement conduct, we conclude that it was neither necessary nor proper for the defendants in this case to destroy the lives and businesses of innocent non-targets in the name of law enforcement. . . . [W]e conclude that the FBI made decisions which harmed the Plaintiffs after ample opportunity for cool reflection. In fact, they invested almost two years and thousands of man hours in developing the sting operation. Thus, the due process clause protects the Plaintiffs from any harm that arose from the officers' deliberate indifference. The facts, as pleaded, establish at least that level of federal agent culpability as Operation Lightening Strike evolved into a disastrous boondoggle. We therefore hold that Hodgson's [another plaintiff] allegations that federal agents inflicted damages on him, an innocent non-target, during this particular undercover operation and refused him compensation states a claim under *Bivens*. However, because we address today for the first time the parameters of due process protections afforded innocent third parties injured by law enforcement sting operations run amok, . . . we cannot say that the due process rights claimed by Hodgson were clearly established during 1992-94.

188 F.3d at 590-92.

As explained later in this Chapter, our review found no undercover operations that involved the sort of adverse consequences described by the court in *Brown*. Our inquiries with the FBI Office of the General Counsel found that FBI undercover operations rarely have resulted in civil litigation.

## **II. Significant Requirements of the Undercover Guidelines**

The Undercover Guidelines prescribe the authority level and approval process for FBI undercover operations based upon the type of undercover

operation being proposed. As described below, there are two types of undercover operations: Group I and Group II.<sup>253</sup>

#### **A. Group I Undercover Operations**

Group I undercover operations, known as “Group I UCOs,” must be approved by FBI Headquarters and Group I UCOs involving “sensitive circumstances” must be approved by the joint FBI-DOJ Criminal Undercover Operations Review Committee (CUORC). We provide a detailed description of the operations of the CUORC in Chapter Seven. The major categories of Group I UCOs are those in which there is a reasonable expectation of involving either “sensitive circumstances” or “fiscal circumstances.” The types of operations that involve “sensitive circumstances” are:

- investigations of possible criminal conduct by any elected or appointed official, or political candidate for a judicial, legislative, management, or executive-level position of trust in a federal, state, or local governmental entity or political subdivision thereof;
- investigations of any public official at the federal, state, or local level in any matter involving systemic corruption of any governmental function; and
- investigations of possible criminal conduct by any foreign official or government, religious organization, political organization, or the news media.

In addition, the following activities constitute sensitive circumstances:

- engaging in activity having a significant effect on or constituting a significant intrusion into the legitimate operation of a federal, state, or local governmental entity;
- establishing, acquiring, or operating a proprietary business;
- providing goods or services that are essential to the commission of a crime and that are reasonably unavailable to a subject of the investigation except from the government;
- activity by an undercover employee that is proscribed by federal, state, or local law as a felony or that is otherwise a serious crime;

---

<sup>253</sup> The Undercover Guidelines do not use the terms “Group I” and “Group II” but, instead, refer to operations that do or do not require FBI Headquarters approval. The Group I/Group II designation is found in the FBI’s Field Guide for Undercover and Sensitive Operations (FGUSO).

- activities involving a request to an attorney, physician, member of the clergy, or other persons for information that would ordinarily be privileged, or to a member of the news media concerning an individual with whom the news media is known to have a professional or confidential relationship; and
- activities that present a significant risk of violence, risk of financial loss, or a realistic potential for significant claims against the United States.<sup>254</sup>

The types of activities that qualify as “fiscal circumstances” are those in which there is a reasonable expectation that the operation will:

- require the purchase or lease of property, equipment, buildings, or facilities; the alteration of buildings or facilities; or prepayment of more than one month’s rent;
- require the deposit of appropriated funds or proceeds generated by the undercover operation into banks or other financial institutions;
- use the proceeds generated by the undercover operation to offset necessary and reasonable expenses of the operation;
- require a reimbursement, compensation, or indemnification agreement with cooperating individuals or entities for services or losses incurred by them in aid of the operation; or
- exceed the limitations on duration or commitment of resources established by the FBI Director for operations initiated in the field.<sup>255</sup>

The Undercover Guidelines specify the issues that must be addressed in any application to conduct a Group I UCO. The application must include: a description of the proposed objective, scope, duration, and cost of the operation; how, if the operation involves “sensitive circumstances,” the operation merits approval in light of the involvement of “otherwise illegal activity” (OIA), if any; procedures to minimize the acquisition, retention, and dissemination of any information which does not relate to the matter under investigation; and an explanation of how potential constitutional or other legal concerns are being addressed. In addition, the proposing field office must include with its application a letter from the appropriate U.S. Attorney

---

<sup>254</sup> The complete list of “sensitive circumstances” is at Undercover Guidelines § IV.C.2 at B-44.

<sup>255</sup> The complete list of “fiscal circumstances” is at Undercover Guidelines § IV.C.1 at B-43.

indicating that he or she has reviewed the proposed operation, agrees with the proposal and that it is legal, will prosecute any meritorious cases, and has made a finding that the proposed investigation “would be an appropriate use of the undercover technique, and that the potential benefits in detecting, preventing, or prosecuting criminal activity outweigh any direct costs or risks of other harm.” Undercover Guidelines § IV.F.2.b. Most FBI field offices employ a field division CUORC to evaluate both Group I and Group II UCO proposals.

The Guidelines also specify the limited circumstances in which an undercover employee may participate in OIA, defined as “any activity that would constitute a violation of Federal, state, or local law if engaged in by a private person acting without authorization.” Undercover Guidelines § IV.H.<sup>256</sup> An FBI Assistant Director must approve certain types of OIA after review by the CUORC. *Id.* § III.H.5.

To avoid entrapment of innocent persons caught up in undercover operations, the Guidelines require that any undercover activities that involve an inducement to engage in crime be authorized only upon a finding that the illegal nature of the activity is reasonably clear to potential subjects; the nature of the inducement is justifiable in view of the character of the illegal transaction; there is a reasonable expectation that offering the inducement will reveal illegal activity; and there is either a reasonable indication that the subject is engaging, has engaged, or is likely to engage in the proposed or similar illegal activity, or the opportunity for illegal activity has been structured so that there is reason to believe that any persons drawn to the opportunity or brought to it are predisposed to engage in the contemplated illegal conduct.<sup>257</sup> Undercover Guidelines § V.B.

With respect to applications for the extension or renewal of a Group I UCO, the Guidelines require an explanation of the expected results to be obtained from the operation or an explanation of any failure to obtain significant results. At the end of 2004, the FBI had [SENSITIVE INFORMATION REDACTED] open Group I undercover operations that were governed by the Undercover Guidelines.

---

<sup>256</sup> See parallel discussion in Chapter Three of “otherwise illegal activity” by FBI confidential informants.

<sup>257</sup> According to the Guidelines, entrapment occurs “when the Government implants in the mind of a person who is not otherwise disposed to commit the offense the disposition to commit the offense and then induces the commission of the offense in order to prosecute.” Undercover Guidelines § V.A at B-54. See also *United States v. Jacobson*, 503 U.S. 540, 548-554 (1992).



## **B. Group II Undercover Operations**

Undercover operations that may be approved by the Special Agent in Charge (SAC) in FBI field offices without FBI Headquarters' review are known as Group II undercover operations, or "Group II UCOs." A Group II UCO is defined as an undercover operation that does not involve either "sensitive circumstances" or "fiscal circumstances." Currently, SACs have the authority to approve Group II UCOs involving the expenditure of up to \$100,000 (or \$150,000 in drug cases of which a maximum of \$100,000 is for operational expenses) for up to 6 months, and to renew the operation for one additional 6-month period, not to exceed 1 year.<sup>258</sup> Thereafter, extensions or renewals must be approved by FBI Headquarters following review by the CUORC. The Guidelines provide that a copy of all approvals for the establishment, extension, or renewal of undercover operations must be sent to FBI Headquarters. Undercover Guidelines § IV.B.

In approving the establishment, extension, or renewal of a Group II UCO, the SAC must make a written determination referencing the facts and circumstances indicating that initiation of the investigative activity is warranted under departmental guidelines; the proposed undercover operation appears to be an effective means of obtaining evidence or necessary information; the operation will be conducted with minimal intrusion consistent with the need to collect evidence or information in a timely and effective manner; approval for the use of confidential informants has been obtained pursuant to the relevant Guidelines; any foreseeable participation by an undercover employee in illegal activity that can be approved by the SAC is justified by the pertinent factors; and there is no present expectation of the occurrence of any of the sensitive or fiscal circumstances that would render the operation a Group I UCO. Undercover Guidelines § IV.B. At the end of 2004, the FBI had [SENSITIVE INFORMATION REDACTED] open Group II undercover operations that were governed by the Undercover Guidelines.

## **III. Major Revisions to the Guidelines**

The May 2002 revisions to the Undercover Guidelines broadened the FBI's authority to use undercover techniques in a wider variety of investigations, increased monetary limits, expanded SAC approval authority

---

<sup>258</sup> The SAC's authority to establish, extend, or renew a Group II UCO can be delegated to designated Assistant Special Agents in Charge (ASACs). The delegation must be in writing. Undercover Guidelines § IV.B.3 at B-42.

On April 29, 2004, the Criminal Investigative Division issued an internal electronic communication stating that confidential expenditure approval limits for Group II UCOs were increased effective immediately from \$50,000 to \$100,000 for Assistant Directors in Charge and Special Agents in Charge.

for Group II UCOs, and clarified several terms in the previous Guidelines. The major changes were:

### **Counterterrorism-related Revisions**

- emphasizing the “prevention of terrorism” as a permissible objective of undercover operations;
- making explicit and emphasizing the FBI’s authority to use undercover techniques to further the objectives of both types of criminal intelligence investigations: racketeering enterprise investigations and terrorism enterprise investigations;
- authorizing SACs to grant emergency approval for the initiation of terrorism-related Group I UCOs if the SAC determines that the UCO is necessary to avoid the loss of a “significant investigative opportunity;”
- adding “potential constitutional concerns” as a factor the SAC must consider in approving any Group II UCO and requiring an explanation of how such concerns have been addressed in an application for a Group I UCO involving the infiltration of a group as part of a terrorism enterprise or recruitment of an informant from such a group;

### **Other Revisions**

- clarifying that only substantive contacts with an undercover employee, as distinguished from incidental or passive contact, count toward the rule defining a “series of related undercover activities” as three or more substantive contacts with the individual(s) under investigation;
- clarifying the FBI’s authority to participate in joint operations with other federal agencies by authorizing the FBI’s participation without complying with the Attorney General’s Guidelines on FBI Undercover Operations as long as the lead agency’s sensitive case review process is substantially comparable to the FBI’s CUORC review process;
- raising from \$40,000 to \$50,000 the operational expenditure limits for Group II UCOs which may be approved at the field level;
- clarifying that felony activity by an FBI undercover employee and potential civil actions against FBI employees under *Bivens* is a “sensitive circumstance,” thereby requiring CUORC approval;

- extending the authority of SACs to approve low-level money laundering not to exceed five transactions and \$1 million without requiring Group I authority from the CUORC;
- authorizing SACs to approve the continuation of covert online contact with subjects for a 30-day period pending approval of a Group I UCO at FBI Headquarters if necessary to maintain credibility or to avoid permanent loss of contact; and
- requiring that the FBI immediately notify the Deputy Attorney General whenever FBI Headquarters disapproves an application for approval of an undercover operation and whenever the CUORC is unable to reach consensus concerning an application.

#### **IV. The OIG Review of the FBI's Compliance with the Undercover Guidelines**

The focus of our review of the Undercover Guidelines was on two of the three substantive Guideline sections: Authorization of Undercover Operations (Part IV), and Monitoring and Control of Undercover Operations (Part VI). We did not directly examine the third substantive section, Entrapment (Part V), because it largely addresses authorization issues that we analyzed through examination of the Guidelines' general authorization provisions.

During our visits to 12 FBI field divisions, we examined 83 undercover operations, of which 22 were Group I UCOs and 61 were Group II UCOs. We collected Guidelines-related data on more than 75 variables for Group I UCOs that we evaluated, and 50 variables for Group II UCOs that we evaluated.<sup>259</sup> As part of this assessment we examined the following questions.

- Was the initiation of the undercover operation authorized?
- Was authority to extend the undercover operation obtained?
- Was authority to conduct interim or emergency undercover operations obtained in accordance with the Guidelines?

---

<sup>259</sup> We examined undercover operations that either were pending on May 1, 2002, or opened after that date. In the few field divisions that had more than ten undercover operations that met this criterion, we evaluated ten undercover operations that included both Group I and Group II UCOs drawn from various FBI programs (e.g., Cyber Crime, White Collar Crime, and Violent Crime and Major Offenders). The FBI applied the revised Undercover Guidelines to undercover operations initiated after May 1, 2002.

- Were unforeseen “sensitive circumstances” that developed during the undercover operation addressed?
- Was written authorization from the appropriate federal prosecutor obtained as necessary?
- Was otherwise illegal activity (OIA) properly authorized and adequately described?
- Did FBI management adequately supervise the undercover operation?
- Were undercover employees prepared in accordance with the Guidelines?
- Did the SAC review the conduct of the undercover employees as required?

In addition to our evaluation of the FBI’s undercover operations, we also examined the results of the FBI’s undercover operation audits. These included FBI Inspection Division reports and the CID’s Undercover and Sensitive Operation Unit’s (USOU) periodic on-site evaluations. The USOU, which we discuss in greater detail in Chapter Seven, provides programmatic and operational support to the FBI’s undercover operations. Finally, we surveyed the FBI’s Undercover Coordinators and Division Counsel regarding the operation of the undercover program.<sup>260</sup>

## **V. Compliance Findings**

Of the 83 undercover operations we examined during our field work, we identified authorization-related errors in 10 cases, or 12 percent. Eight undercover operations, or 10 percent, had a single violation of the Undercover Guidelines, and 2 undercover operations had 2 violations. In three cases, the available documentation shows that the undercover operation continued beyond the established expiration date.<sup>261</sup> Three cases involved task force undercover operations in which the FBI was participating with state and local law enforcement; in these cases, the undercover operations exceeded the scope of the FBI’s authorization for its

---

<sup>260</sup> Undercover Coordinators are the field divisions’ on-site experts concerning undercover matters, and they perform duties such as evaluating proposals for undercover operations, maintaining familiarity with all policies and requirements that apply to undercover operations, and working with USOU. FGUSO § 10.1 (2).

<sup>261</sup> See Undercover Guidelines §§ IV.B.2 & IV.G at B-42 & B-49, which set forth the applicable authorization periods.

agents' participation.<sup>262</sup> In two cases, the undercover operation was approved by an FBI manager who lacked authority to do so.<sup>263</sup> Finally, in two cases FBI Headquarters approval was not obtained for matters involving "sensitive circumstances" within the meaning of § IV.C.2 of the Undercover Guidelines. These two violations both occurred in public corruption cases – one involving the payment of a bribe without following Headquarters' review procedures, and the other involving the "systemic corruption of [a] governmental function."<sup>264</sup>

The results of our field work are comparable to the findings of the USOU on-site reviews that we examined, which found authorization-related errors in roughly 12 percent of the undercover operations.

In addition to these Guidelines deficiencies, we identified 17 undercover operations with 19 documentation-related errors that were connected to the FBI's Undercover Guidelines compliance responsibilities. As discussed in detail below, the issues in these matters concerned the lack of or insufficient documentation addressing the SAC's review of undercover employee conduct, authorizations of OIA, and certain required elements of U.S. Attorney authorizations for Group I UCOs. We also identified inconsistencies relating to the evaluation of the risk of violence in undercover operations, a "sensitive circumstance" within the meaning of § IV.C.2 of the Undercover Guidelines.

Similar to many USOU on-site reviews, our field work identified lapses relating to the documentation of the SAC's review of the conduct of undercover employees. Section VI.A of the Undercover Guidelines requires the SAC or Supervisory Special Agent (SSA) to meet with the undercover employees and to discuss their expected conduct during the undercover

---

<sup>262</sup> Section III of the Undercover Guidelines states: "The FBI may participate in joint undercover activities with other law enforcement agencies. . . . Joint undercover operations are to be conducted pursuant to these Guidelines." See Undercover Guidelines § III at B-40. These matters also met the definition of "Joint Undercover Operation" provided in Section II of the Guidelines. Undercover Guidelines § II.F at B-40.

<sup>263</sup> In one field division, the approving ASAC authorized two undercover operations without obtaining a written delegation of authority from the SAC as required by the Undercover Guidelines § IV.B.3 at B-42.

<sup>264</sup> The determination whether a public corruption matter will be presented to the CUORC can depend upon decisions made by FBI managers outside of USOU. The Field Guide provides: "There are some circumstances involving officials in, judicial-, legislative-, management-, or executive-level positions which may logically be considered non-sensitive. In such instances, the Section Chief, Integrity Government/Civil Rights Section, CID, FBIHQ, who is a member of the CUORC and has a national perspective on matters involving public officials, must be consulted for a determination as to whether the undercover operation should be presented to the CUORC." FGUSO § 3.2.A(3).

operation and provide instructions included in the Guidelines. Section VI.B requires the SAC to review the conduct of the undercover employees “from time to time.” Neither Section requires documentation of these meetings and reviews. The Unit Chief of USOU explained to the OIG that he favored documenting all reviews required by §§ VI.A and B in order to demonstrate compliance with the Guidelines, and that this could be satisfied simply by having the case agent or supervisor include an e-mail in the case file.<sup>265</sup> However, the FBI’s Field Guide for Undercover and Sensitive Operations (Field Guide or FGUSO) requires documentation only of meetings with undercover employees whose undercover responsibilities require them to work outside field division offices.<sup>266</sup> Field Guide §10.1(1)A.

Of the 83 undercover operations we examined, 21 lacked documentation of the SAC’s review of the undercover employees’ conduct. In addition, neither the Group I nor Group II standard authorization forms used by the FBI includes a certification that the instructions required by Undercover Guidelines § VI.A have been given, though both forms require the Undercover Coordinator to certify that he or she has “apprised the members of the undercover operation investigative team . . . of undercover program policy.” Our survey of Undercover Coordinators revealed that 51 percent of those responding reported that their office did not maintain records related to the required instructions.<sup>267</sup>

As we found with respect to the FBI’s use of its authority to approve a confidential informant’s participation in OIA in the Criminal Informant Program, we identified deficiencies in the sufficiency of the descriptions of OIA authorized for undercover employees. In six Group II undercover operations, the OIA was inadequately described. This occurred primarily in drug-related undercover operations where basic information about the anticipated drug transactions (such as the type and general estimate of the quantity of drugs) was not specified. For example, in one undercover operation the quantity of drugs that was authorized for purchase was identified as “that which will be needed to maintain sufficient leverage on

---

<sup>265</sup> Our references to the Unit Chief of USOU refer to the SSA who served in that position through January 2005.

<sup>266</sup> The FBI presently does not require documentation of compliance with § VI.B of the Undercover Guidelines for undercover employees who are not required to work outside field division offices. Our review identified 15 undercover operations where we were unable to verify from the case files whether the SAC had reviewed the conduct of undercover employees who were working from FBI offices. The current Unit Chief of USOU told the OIG that USOU will henceforth require SACs to meet with all undercover employees at least once during each authorization period and to document the meeting.

<sup>267</sup> We received responses from 54 of the 58 Undercover Coordinators or 93 percent.

the subjects in order to persuade them to cooperate with law enforcement.” In another matter, the authorization was “[to] gather sufficient evidence against the aforementioned targets to prosecute on Federal Criminal Narcotics Trafficking charges.” Two successive Unit Chiefs of USOU disagreed as to whether such descriptions of OIA were adequate.

We also identified six Group I UCOs where the required letter from DOJ did not satisfy § IV.F.2.b of the Undercover Guidelines. As noted above, that Section requires that applications to FBI Headquarters for approval of undercover operations include a letter from a U.S. Attorney or Section Chief in the Criminal Division of the DOJ that indicates that he or she:

1. has reviewed the proposed operation, including any sensitive circumstances reasonably expected to occur;
2. agrees with the proposal and its legality;
3. finds that the proposed investigation would be an appropriate use of the undercover technique;
4. believes that the potential benefits in detecting, preventing, or prosecuting criminal activity outweigh any direct costs or risks of other harm; and
5. will prosecute any meritorious case that is developed.

Four of the letters omitted two or more factors. All of the letters omitted factor number four.

We also did not find a consistent practice of highlighting in the proposal materials the potential risk of violence or physical harm that could result from the undercover operations. Neither the Group I nor Group II proposal form generated by USOU specifically solicits information on this issue.<sup>268</sup>

The following table summarizes these findings.

---

<sup>268</sup> The Group I proposal form requires an explanation of any “sensitive circumstances.” The Guidelines definition of sensitive circumstances includes “a significant risk of violence or physical injury to individuals.” Undercover Guidelines § IV.C.2.m at B-45.

**TABLE 4.1**

<b>OIG Compliance Findings from 83 Group I and Group II Undercover Operations in Select Field Offices</b>			
<b>Authorization-Related Errors</b>	<b>Number of Group I</b>	<b>Number of Group II</b>	<b>Total</b>
The undercover operation continued beyond the established expiration date	1	2	3
Task Force undercover operations exceeded the scope of the FBI's authorization for its participation	1	2	3
The undercover operation was approved by an FBI manager who lacked authority to do so	--	2	2
FBI Headquarters approval was not obtained for matters involving "sensitive circumstances"	1	1	2
<b>Documentation-Related Errors</b>	<b>Number Of Group I</b>	<b>Number Of Group II</b>	<b>Total</b>
The undercover operation lacked documentation of the SAC's review of the undercover operation	2	4	6
The required letter from USAO or DOJ did not address all required issues	6	--	6
The OIA was described inadequately	--	6	6

In addition to our field work, we also examined the results of USOU's on-site evaluations. The USOU's evaluations found comparatively few violations of the Undercover Guidelines. Of [SENSITIVE INFORMATION REDACTED] on-sites conducted by USOU from May 2002 through October 2004, the following Guidelines-related deficiencies were identified:

- in seven undercover operations, agents failed to obtain proper authorization for undercover activity;
- in two undercover operations, division management failed to meet with undercover employees and in five other undercover operations documentation of such meetings was lacking;<sup>269</sup> and
- in one undercover operation, a financial transaction was conducted in violation of the Guidelines.

---

<sup>269</sup> These seven undercover operations were in different field divisions.



Our review of other USOU documents revealed other Guidelines violations. The CUORC's fiscal year 2003 report noted the lack of proper authorization in one undercover operation, and a USOU electronic communication to the field in 2003 described the failure of certain field divisions to provide prompt notification to FBI Headquarters of the approval of Group II UCOs, a requirement of the Undercover Guidelines. Undercover Guidelines § IV.B.4. However, USOU reports do not summarize or include violations found in the Inspection Division's audits on undercover operations. According to the Unit Chief of USOU, the Inspection Division does not routinely share its undercover inspection findings with USOU. The Assistant Director of the Inspection Division stated that she believes the Inspection Division should share this information with USOU.

Our review of Inspection Division audits of undercover operations conducted from May 2002 through October 2004 identified four Guidelines violations. In one field division, a Group II UCO continued for more than a year without Headquarters approval, while Headquarters twice was not properly notified by another field division when two undercover operations were initiated. Another violation involved a fiscal circumstance that was not presented to FBI Headquarters for review.

## **VI. OIG Analysis**

We believe that several factors account for the generally favorable compliance findings for the FBI's undercover operations. First, the FBI's use of undercover operations is not as widespread as its use of confidential informants. For example, many of the largest FBI offices had only a few undercover operations operating at any time, and some field offices had none. According to the Unit Chief of USOU, the small number of undercover operations allows the FBI to devote sufficient resources and attention to supervising them. Second, unlike with the confidential informant program, USOU has developed a field guide, standardized forms, and a user-friendly web site to assist with administration of undercover operations. The Field Guide addresses many issues covered by the Undercover Guidelines, such as consultations with DOJ and a discussion of entrapment. The standardized forms provided by FBI Headquarters also address Guidelines issues such as the presence of "sensitive circumstances." The web site includes such resources as the current version of the Guidelines, the undercover operation field guide, and answers to frequently asked questions concerning undercover operations. With few

exceptions, we did not detect significant confusion in the field regarding Undercover Guidelines' requirements and procedures.<sup>270</sup>

Third, according to the Unit Chief of USOU, field agents are able to draw upon the expertise of personnel assigned to USOU, Undercover Coordinators, and experienced undercover-certified agents to promote compliance with FBI and DOJ requirements. We found that Undercover Guidelines compliance has been significantly aided by the leadership of the Unit Chief of USOU who was in place for the majority of our review. During his tenure, which ended in March 2004, he took several actions to significantly improve the operation of USOU and promote compliance with the Guidelines. These included reinstituting preparation of the annual report of the CUORC, improving the USOU on-site review process,

---

<sup>270</sup> One noteworthy exception is the handling of undercover operations in international terrorism cases. Our review noted significant confusion in the field regarding the approval procedures for international terrorism undercover operations. In early 2004, 51 percent of the Undercover Coordinators we surveyed stated that there was confusion over which division at FBI Headquarters supervises such operations. When asked to identify the Headquarters division which is the initial point of contact to review criminal international terrorism undercover operations, 43 percent of the surveyed Undercover Coordinators failed to identify the Counterterrorism Division (CTD). Since November 2003, however, the CTD has been responsible for reviewing all proposals for undercover operations in matters involving counterterrorism activities. Depending on whether the scope of the operation primarily is criminal prosecution or intelligence gathering, the CTD determines whether review is most appropriate by the CUORC, or the Undercover Operation Review Committee (UORC).

As explained by one Coordinator, “[u]nder the current arrangement there is lack of communication and lack of cooperation between CID and CTD. There is also confusion in the field, since there is a great deal of overlap between the two investigative entities. Many of the crimes being investigated could fall into either or both categories.” Our survey revealed that 81 percent of Undercover Coordinators believed that it would be beneficial to have one operating division at FBI Headquarters approve all aspects of undercover operations, regardless of which substantive program is involved.

According to the USOU Unit Chief, the FBI has made progress since our survey to standardize review procedures for undercover operations and to integrate aspects of the undercover program between the CID and CTD. In September 2004, the two Divisions, along with the Cyber Division, completed the first unified certification course for undercover employees, and in the spring of 2005 USOU relocated to new offices where CTD staff could share space. According to the Unit Chief, with the addition of CTD staff, the personnel assigned to this new space would function in practical terms as an undercover operations center, allowing the field to resolve questions with a single call to Headquarters. However, the OIG learned in August 2005 that this integration was delayed due to a reorganization associated with the creation of a National Security Service within the FBI. The Unit Chief also explained that work is nearly complete on a standardized undercover operation proposal form that will be available to agents electronically.

identifying Guidelines compliance issues in Unit reports, and promptly rewriting the Field Guide to account for the May 2002 Guidelines revisions.

Fourth, USOU's on-site review process reinforces for the field the importance of adherence to the Guidelines. Although the focus of the on-site reviews is operational success and safety, the reviews include assessments of compliance issues that assist with the identification and correction of Undercover Guidelines violations.

With regard to the causes of the limited Undercover Guidelines violations that we identified in our field work, the violations involved errors that we believe could have been avoided had there been closer coordination between the undercover investigative teams and the Undercover Coordinators and Chief Division Counsel. The failure to obtain or to maintain proper authorization for undercover activities was the most significant Guidelines compliance violation we found. These included continuing undercover activities beyond the approved authorization period, failing to obtain FBI Headquarters approval because of a misinterpretation of "sensitive circumstances," and participating in task forces that exceed FBI undercover operation authorizations. Although the frequency of these violations was not as common as for other kinds of Guidelines non-compliance identified during this review, it nonetheless occurred in 10 to 12 percent of the cases examined by the OIG and USOU. According to the USOU Unit Chief, the cause of the non-compliance is simply lack of knowledge by agents regarding the Guideline requirements.

Our surveys of Undercover Coordinators and Division Counsel revealed two significant findings regarding oversight and assistance to FBI undercover operations.<sup>271</sup> First, many Undercover Coordinators believe that they are too encumbered by other duties to devote appropriate attention to the undercover program. Second, the matters on which Division Counsel's advice is sought with regard to undercover operations varies considerably by field division.

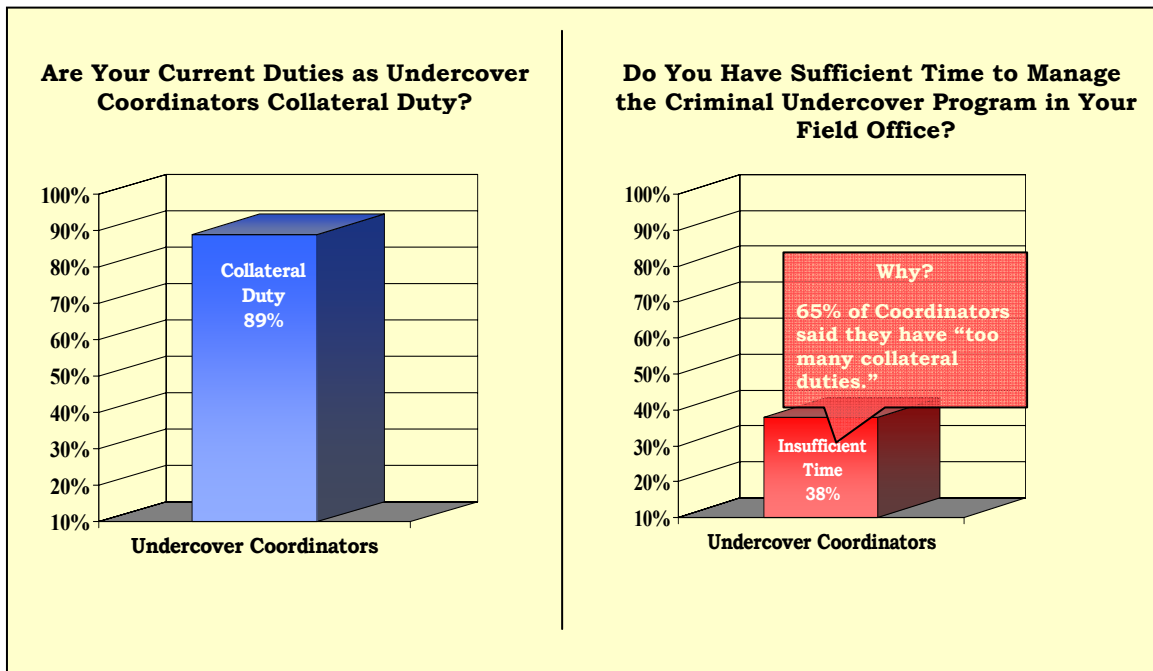
---

<sup>271</sup> We received a 92 percent response rate to our survey. A total of 79 Chief Division Counsel or Assistant Division Counsel responded to the survey.

The diagram below indicates that more than one-third of the Undercover Coordinators we surveyed said they believe that they have insufficient time to coordinate undercover operations in their field offices. Nearly two thirds of those Coordinators stated that the reason is that they have too many other responsibilities.<sup>272</sup>

**DIAGRAM 4.1**

**Undercover Coordinators' Views on Their Duties**

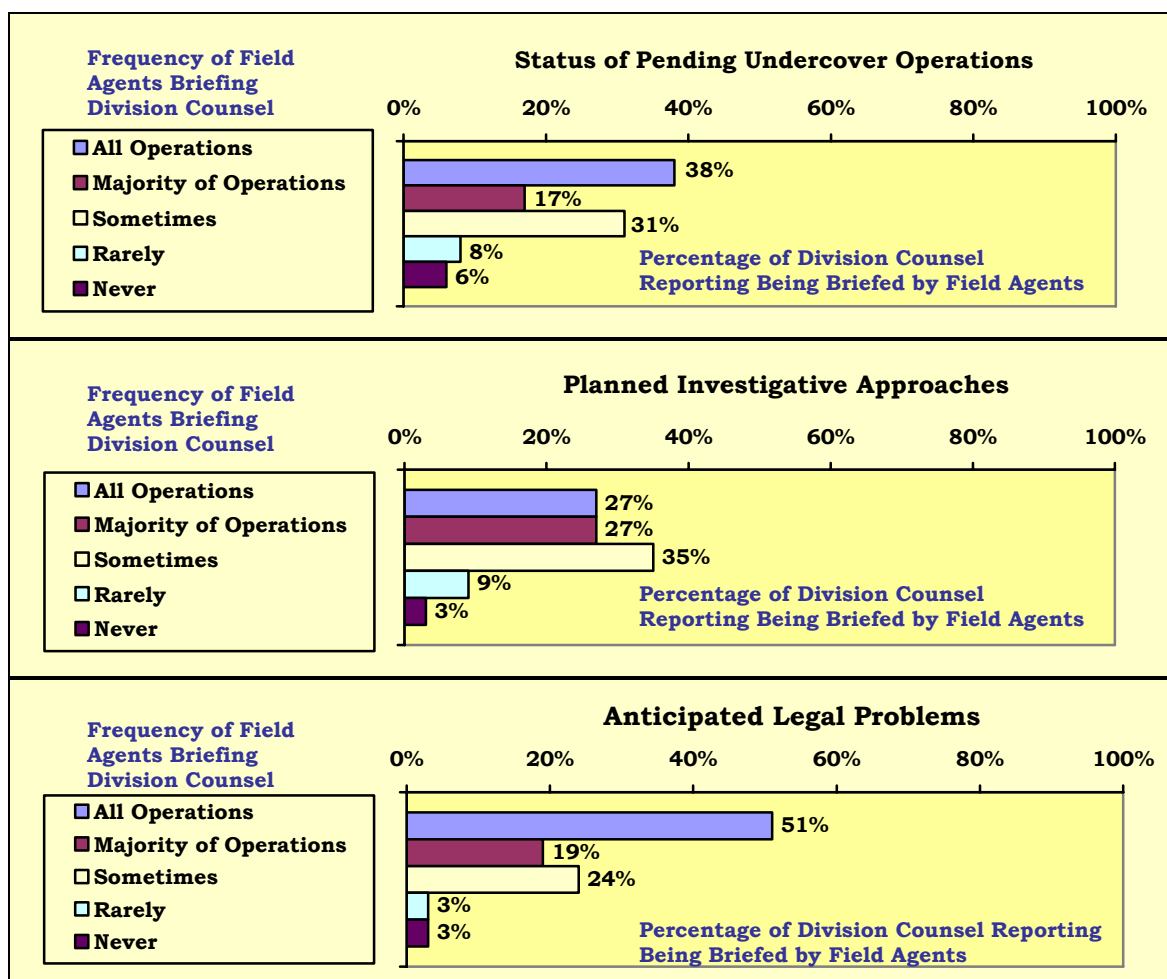


Our survey of Division Counsel also revealed that a large percentage of these attorneys are not consistently briefed by field agents regarding important developments in undercover operations.

<sup>272</sup> In addition, 40 percent of the surveyed Undercover Coordinators said that they have inadequate administrative support.

**DIAGRAM 4.2**

**Division Counsel's Views on Frequency of Field Agents' Consultation on Select Issues Concerning Undercover Operations**



In addition, we found significant agreement concerning the lack of consultation among Division Counsel assigned to the same field office.<sup>273</sup> We found that 40 percent of the offices to which these attorneys were assigned are not regularly briefed on the status of pending undercover operations, 33 percent are not regularly briefed on planned investigative approaches, and 27 percent are not regularly briefed on anticipated legal problems with the undercover operations. Moreover, Division Counsel in the five field divisions that had at least two cases of authorization-related

<sup>273</sup> Fifteen field offices had more than one Division Counsel reply to our survey.

errors reported that they were not regularly briefed on the status of pending undercover operations.

Our interviews with FBI personnel also indicated that some field divisions need more frequent and consistent interactions by Undercover Coordinators and Division Counsel with undercover teams.<sup>274</sup> The Unit Chief of USOU emphasized this point, stating “the mistakes that I have seen since being the Unit Chief of this Unit, if the Undercover Coordinator would have been involved, it probably wouldn’t have happened.” He also stated that “the CDC is first line of legal defense,” and if agents are not working with legal counsel as part of a team effort both in the formulation and implementation of the undercover operation, “you are asking for problems.” In addition, an electronic communication which USOU issued to all field offices during our review emphasized the importance of the Undercover Coordinator, the need for greater consultation with the Coordinator, and the problems that turnover in the Undercover Coordinator position was having on the undercover program.

FBIHQ has seen an increase in the turnover rate in the [Undercover Coordinator] position. Since January 2001, 29 of 56 UCCs have been replaced. While a UCC may be promoted or transferred thus making a change necessary, efforts should be made to ensure continuity by selecting a candidate who will remain in the position for a period of time. Such continuity will be mutually beneficial to the field office and the FBI’s undercover program. . . . It has also been noticed that [Undercover Coordinators] have not been fully utilized as reflected in the fact that several undercover proposals have been submitted to FBIHQ without the careful review by the [Undercover Coordinator].

We also learned that the SSAs who exercise day-to-day supervision over the agents participating in the undercover operations are not required to receive training on undercover operations or compliance issues.

Our review further revealed that the absence of guidance addressing undercover operations in which task forces participated contributed to some of the Guidelines violations we found. In one case a local law enforcement

---

<sup>274</sup> The General Counsel of the FBI, Valerie Caproni, stated that in those offices where Division Counsel reported that they were not being consulted agents may be seeking advice from Assistant U.S. Attorneys (AUSAs). She stated it would assist her if the Inspection Division surveyed not only CDCs to determine whether they believe that they are being consulted properly, but also agents to determine where they are seeking legal advice and why.

task force member made drug purchases using FBI funds on behalf of an FBI agent who previously had participated in the undercover operation, even though the FBI's authorization for the undercover activity had expired weeks earlier. Although the Field Guide includes a section on joint operations, it does not address many compliance issues that are unique to task forces, such as the need to identify in the FBI proposal documentation all task force officers who will participate in the undercover operation. The USOU Unit Chief explained that the FBI has not developed guidance for undercover operations involving task forces.

We also identified some confusion concerning the scope of "sensitive circumstances" in the Undercover Guidelines. Our survey of FBI Undercover Coordinators revealed that 43 percent of those responding believed that determining whether "sensitive circumstances" are present in a case is one of the three most difficult issues to resolve in the course of initiating and conducting undercover operations.<sup>275</sup> Our field work also noted compliance issues associated with the interpretation of "systemic corruption" in § IV.C.2.b and the "significant risk of violence or physical injury to individuals" in § IV.C.2.m.<sup>276</sup> For example, we identified an undercover operation in which law enforcement officers from two agencies were engaged in illegal conduct, and the target of the investigation had consulted with the head of one of the agencies about some of these activities. After we questioned the field division's application of § IV.C.2.b (systematic corruption) in this case and its decision to treat the undercover operation as a Group II, we conferred with the Chief of the Investigative Law Unit of the FBI Office of the General Counsel who described a framework for analyzing when a governmental function has been systemically corrupted. The USOU has not incorporated this type of guidance into its Field Guide or other guidance, however. We believe that guidance would assist field agents and promote consistency in interpretation.

In addition, we reviewed a number of Group II UCO proposals originating from Violent Crime and Major Offender and Drug Units which contained little information about the risks of violence. Our discussions with FBI personnel revealed a wide range of opinions concerning what

---

<sup>275</sup> The other two issues were: 1) avoiding liability in the course of conducting an undercover operation (55 percent), and 2) satisfying the stipulations placed on undercover operations by the FBI Headquarters CUORC (43 percent).

<sup>276</sup> Sections IV.C.2.b and IV.C.2.m concern, respectively, investigations "of any public official at the Federal, state, or local level in any matter involving systemic corruption of any governmental function," and investigations that involve "a significant risk of violence or physical injury to individuals." (emphasis in original).

qualifies as a “significant risk of violence or physical injury to individuals” within the meaning of § IV.C.2.m.<sup>277</sup>

With respect to compliance violations regarding the documentation concerning reviews required under Part VI of the Undercover Guidelines, descriptions of OIA, and the contents of DOJ authorization letters for Group I UCOs, our discussions with FBI personnel indicated that a lack of awareness of the need for the documentation or for greater specificity in such material appeared to be the primary cause of the deficiencies. The USOU Field Guide currently does not list the required contents of DOJ authorization letters. With regard to oversight of undercover employees, § VI.B of the Undercover Guidelines requires the SAC to review “from time to time” the conduct of undercover employees.<sup>278</sup> According to the Unit Chief of USOU, the case agents and their supervisors have the responsibility to document meetings with the SAC.

With respect to the lack of specificity found in some OIA authorizations, the USOU Unit Chief stated that “it is a common sense approach. [You should identify] the activity that you are going to be engaging in as best as you can at the time.” According to one USOU Unit Chief, the kind of general descriptions that we found in several of the OIA authorizations, such as “that which will be needed to maintain sufficient leverage on the subjects in order to persuade them to cooperate with law enforcement,” does not provide sufficient guidance or indicate the likely limitations that the SAC intended to impose on the scope of the OIA. Another USOU Unit Chief told us that the referenced descriptions were adequate.

---

<sup>277</sup> As described in Chapter Three, we noted the same issue in the suitability reports for confidential informants.

<sup>278</sup> According to USOU, this responsibility may not be delegated, even in circumstances where the SAC has delegated responsibility for approving undercover operations to ASACs. We believe this interpretation is sound given that § IV.B.3 of the Undercover Guidelines limits delegation authority to the establishment, extension, and renewal of undercover operations. Consistent with the Field Guide, however, both the USOU and Inspection Division undercover operation checklists require verification that “the SAC, or in the SAC’s absence, the ASAC, has met with undercover employee(s) that [sic] do not come into the field office at a location away from the office at least once every period of authorization.” (Emphasis added.) Neither checklist requires verification of meetings with undercover employees who do not work outside the field office. Because the SAC’s responsibility to review the progress of the undercover operation may not be delegated, ASAC review is not a substitute for SAC review under the Guidelines. Moreover, the Guidelines’ requirement of the SAC’s review of undercover employee conduct applies to all such employees, and is not limited to those who work away from the field office.



## **VII.   OIG Recommendations**

Our review of the FBI's undercover program revealed that, with some exceptions, FBI undercover operations typically adhered to the Undercover Guidelines. We believe this generally favorable record is attributable to the availability of information about the requirements, including a field guide, standardized forms, and a user-friendly web site, and the contributions of experienced FBI personnel in ensuring adherence to the Guidelines. Our review nonetheless identified authorization-related deficiencies in 12 percent of the undercover operations that we examined, an outcome that is consistent with the results of USOU's on-site reviews over the last two years. We believe that these violations, while not high in number, are important to rectify, especially because of the risks that undercover operations present for the participating agents, the FBI, and the public.

To ensure that undercover operations are properly authorized and conducted in accordance with the Guidelines, we believe that the FBI should encourage greater utilization of its Undercover Coordinators and Division Counsel. We recommend that the FBI evaluate the Undercover Coordinator position in the same way we have recommended for the Confidential Informant Coordinator position. Given the demands placed on Undercover Coordinators in certain field divisions, it may be appropriate to afford senior field managers the option of elevating the post to the GS-14 supervisory level. We also concur with the view of the USOU Unit Chief that the FBI should assess whether it should "formalize [the position] so that the Coordinator is put in a position where you do have to go through them and do have to consult with them." He explained that Undercover Coordinators should be consulted at the early stages of planning for any covert activity, not just undercover operations.

We also believe that the FBI should encourage Undercover Coordinators to conduct their own progress reviews of the undercover operations within their field division. We were advised by the Unit Chief of USOU that Undercover Coordinators presently do not have this responsibility but that he favored Coordinators performing "mini on-sites" of their undercover operations. We believe this function is especially important for Group II UCOs since they are rarely examined by USOU in its on-site reviews and are not reviewed by the COURC. Our survey of Coordinators also found support for this work. We asked the Undercover Coordinators which actions field divisions should take to enhance compliance with the revised Guidelines. Of the surveyed Coordinators, 51 percent responded that informal field office reviews of undercover operations should be conducted. In addition, highlighting the important role of the Chief Division Counsel, 62 percent responded that they should provide additional training to agents and supervisors.

Our survey of Undercover Coordinators also revealed another consideration that is relevant to oversight of undercover operations: nine percent of the surveyed field divisions reported that they did not have a local CUORC to review undercover operation proposals. Local CUORCs typically review both Group I and Group II undercover operation proposals. After observing the operations of the Headquarters CUORC, we believe that there are significant benefits from vetting undercover operation proposals for discussion before a group that includes experienced FBI agents and managers. Most FBI's field divisions – 90 percent – have a local CUORC. We believe that those field divisions that do not have a CUORC should be required to establish a local CUORC or specify written internal review procedures for both Group I and Group II UCOs that ensure proper consideration of the undercover operation approval standards set forth in § VI.A of the Undercover Guidelines.

Two other factors are also important to ensure full compliance with the Undercover Guidelines: 1) supervising agents and undercover employees should be adequately trained in undercover procedures; and 2) adequate technology should be employed to monitor undercover operation authorizations. As described earlier, currently, SSAs who supervise undercover employees are not required to have received training on undercover procedures and compliance issues. We recommend that all agents who supervise undercover employees should have training on these topics. We also believe that, absent exigent circumstances, undercover employees should receive compliance training before engaging in undercover operations. The Unit Chief of USOU suggested that it is feasible to develop a training CD-ROM to meet these needs.

Technology also can support compliance efforts. According to the USOU Unit Chief, the FBI will soon be able to use a database to monitor undercover operation authorizations and other compliance issues nationwide.<sup>279</sup> This system will automatically send electronic notifications to users and to USOU of upcoming deadlines and requirements. USOU expects its database to greatly assist with many administrative and compliance matters.

In addition, we believe that the likelihood of finding Guidelines violations of the sort we identified during our field work would be reduced if the FBI issued guidance or supplemented the USOU Field Guide with

---

<sup>279</sup> Among other capabilities, the database is expected to track the scheduling of on-site reviews, assist with locating appropriate undercover employees through storage of biographical and skill data, and track and store undercover inventory information (e.g., weapons and computer equipment).

information addressing compliance issues associated with task forces and the interpretation of sensitive circumstances set forth in §§ IV.C.2.b and IV.C.2.m of the Undercover Guidelines. As described earlier, several of the Undercover Guidelines violations we found involved the failure to obtain proper authorization for activities undertaken in undercover operations that were conducted in conjunction with task forces. We also noted compliance issues associated with the interpretation of “systemic corruption” in § IV.C.2.b and the “significant risk of violence or physical injury to individuals” in § IV.C.2.m. We believe that the FBI should adopt a consistent interpretation of “sensitive circumstances” in both ordinary and task force settings and require its undercover operations proposals to identify facts that will allow FBI supervisors to determine whether such circumstances, including the risk of violence, are present and to what degree.

With regard to the § VI meetings and consultations with undercover employees, the Unit Chief of USOU explained that an e-mail documenting the meetings can be included in the FBI’s records and that a formal electronic communication is not necessarily required. Authorization letters from U.S. Attorneys’ Offices approving Group I UCOs should address all the factors set forth in § IV.F.2.b of the Undercover Guidelines, and the descriptions of otherwise illegal activity can be modified in the same fashion as we have recommended in Chapter Three with respect to otherwise illegal activity authorized for confidential informants.

In sum, we recommend that the FBI take the following steps.

#### **Enhance the Role of Undercover Coordinators and Division Counsel**

(10) Evaluate the grade level of Special Agents who serve as Undercover Coordinators and consider allowing Undercover Coordinators to be elevated to a GS-14 supervisory level, particularly in larger field offices where executive management deems it necessary to be a full-time position.

(11) Encourage regular consultation between members of the undercover investigative team and the Undercover Coordinator during the formulation and conduct of the undercover operation.

(12) Evaluate ways for the Undercover Coordinator to perform progress reviews at least every 90 days on undercover operations, a component of which should include an evaluation by senior managers, in consultation with Division Counsel and the Undercover Coordinator, of compliance with the Undercover Guidelines. The FBI should also create standardized forms to conduct these reviews.

(13) Establish policies that promote more consistent Division Counsel involvement in the development and implementation of undercover operations, and ensure that Division Counsel are advised of anticipated legal problems in undercover operations.

### **Improve Guidance and Training**

(14) Because neither the MIOG nor FBI field guides adequately address the issues below, provide guidance on the following:

- the meaning of “sensitive circumstances” relating to “systemic corruption” of governmental functions, and the “significant risk” of violence or physical injury to individuals pursuant to Undercover Guidelines Sections IV.C.2.b and IV.C.2.m, respectively;
- how to limit the scope of authorizations for otherwise illegal activity in undercover operations; and
- special concerns and compliance issues associated with task force participation.

(15) Identify ways to enhance Undercover Guidelines compliance training for field supervisors and undercover employees, including use of instructional CD-ROMs, web-based courses, and joint training with the U.S. Attorneys’ Offices. Absent exigent circumstances, either as part of the certification of undercover employees or otherwise, the FBI should require undercover employees to complete undercover operation compliance training before participating in undercover operations. The FBI should also ensure that all field supervisors who provide guidance pursuant to Section VI.A of the Guidelines regarding preparation of undercover employees are familiar with undercover techniques, compliance requirements, and the Field Guide for Undercover & Sensitive Operations.

### **Improve Internal Controls**

(16) As part of the Undercover Coordinator’s certification currently provided for Group I and II undercover operation proposals, add a certification that the instructions set forth in Section VI.A.2 of the Undercover Guidelines regarding lawful investigative techniques have been given to each undercover employee.

(17) Amend the Group I and Group II undercover operation proposals forms that currently provide information regarding the expected execution of the undercover operation to include a section: “Facts Pertinent to Violence Risk Assessment.”

(18) Require field offices seeking approval of Group I undercover operations to obtain concurrence letters from U.S. Attorneys' Offices that meet the requirements of Section IV.F.2.b of the Undercover Guidelines and amend Section 4.8(5) of the Field Guide for Undercover & Sensitive Operations accordingly.

(19) Ensure that the Undercover and Sensitive Operations Unit has access to the Inspection Division's undercover operation audits.

## **CHAPTER FIVE**

### **ATTORNEY GENERAL'S GUIDELINES ON GENERAL CRIMES, RACKETEERING ENTERPRISE AND TERRORISM ENTERPRISE INVESTIGATIONS**

Of the four Investigative Guidelines, the Guidelines on General Crimes, Racketeering Enterprise and Terrorism Enterprise Investigations (General Crimes or GCI Guidelines) have the broadest scope. They govern the FBI's investigation of general crimes, racketeering enterprises, and terrorism enterprises. Below we describe the various levels of investigative activity permitted under the General Crimes Guidelines, the two types of investigations they authorize: 1) general crimes investigations and criminal intelligence investigations, and 2) the new anti-terrorism authorities that were added after September 11, 2001. We also provide our compliance findings and recommendations for each of these Guidelines activities and provisions.

#### **I. Levels of Investigative Activities**

The General Crimes Guidelines authorize three graduated levels of investigative activity. These activities are the checking of initial leads, preliminary inquiries, and full investigations. With limited exceptions, the General Crimes Guidelines provide that any lawful investigative technique may be used in preliminary inquiries and full investigations. General Crimes Guidelines, Introduction, A.<sup>280</sup>

One level of investigative activity is the checking of initial leads, which can be undertaken after receipt of information indicating that some follow up regarding the possibility of criminal activity is warranted. Following up on such leads often is for the purpose of determining whether further investigation (either a preliminary inquiry or a full investigation) should be conducted.

The next level of investigative activity is a preliminary inquiry. According to the General Crimes Guidelines, a preliminary inquiry is appropriate when information or an allegation indicates the possibility of criminal activity and responsible handling requires further scrutiny beyond checking initial leads. General Crimes Guidelines, Introduction, A. A preliminary inquiry allows the FBI to determine whether a full investigation should be opened.

---

<sup>280</sup> We provide a copy of the General Crimes Guidelines in Appendix B.

The range of investigative techniques in a preliminary inquiry is broad, with the Guidelines prohibiting only mail openings and nonconsensual electronic surveillance. General Crimes Guidelines, Introduction, A. The Guidelines state that the FBI should not hesitate to use any lawful techniques in a preliminary inquiry, even if “intrusive,” where “the intrusiveness is warranted in light of the seriousness of the possible crime or the strength of the information indicating its existence or future commission.” Id. § II.B.4.

The Guidelines define full investigations as either general crimes investigations or criminal intelligence investigations. General crimes investigations may be opened where facts or circumstances reasonably indicate that a federal crime has been, is being, or will be committed. GCI Guidelines, Introduction, B. The standard for initiating a general crimes investigation is “substantially lower than probable cause” and may be satisfied when the objective of the investigation is to prevent future criminal activity, as opposed to investigating a completed criminal act. Id. § II.C.1.

The second type of full investigation defined by the General Crimes Guidelines is a criminal intelligence investigation. There are two types of criminal intelligence investigations: racketeering enterprise investigations (REIs) and terrorism enterprise investigations (TEIs). According to the General Crimes Guidelines, a racketeering enterprise investigation may be initiated when facts or circumstances reasonably indicate that two or more persons are engaged in a pattern of racketeering activity as defined in the Racketeer Influenced and Corrupt Organizations (RICO) statute, 18 U.S.C. § 1961(5). Id. § III.A.2.a. A terrorism enterprise investigation may be initiated when facts or circumstances reasonably indicate that two or more persons are engaged in an enterprise for the purpose of: 1) furthering political or social goals wholly or in part through activities that involve force or violence and a federal crime, 2) engaging in terrorism as defined in 18 U.S.C. §§ 2331(1) or (5) that involves a federal crime, or 3) committing any offense described in 18 U.S.C. 2332b(g)(5)(B). Id. § III.B.1.a.

We describe below the requirements of the General Crimes Guidelines relating to preliminary inquiries, general crimes and criminal intelligence investigations, and the new counterterrorism authorities, followed by our compliance findings and recommendations.

## **II. Preliminary Inquiries**

### **A. Significant Requirements**

The General Crimes Guidelines state that the opening of a preliminary inquiry must be based on an allegation or other information that is recorded in writing and authorized by an FBI supervisor. In “sensitive criminal matters,” the FBI must notify the U.S. Attorney or an appropriate

Department of Justice (DOJ) official of the basis for an inquiry as soon as practicable after its opening, and must create a record of the notification.<sup>281</sup> GCI Guidelines § II.B.2.

Preliminary inquiries may be authorized for up to 180 days. A Special Agent in Charge (SAC) may grant up to two 90-day extensions if the inquiry has failed to yield a “reasonable indication” of criminal activity and further investigative steps are warranted. Additional extensions require approval by FBI Headquarters. *Id.* § II.B.3.

When a preliminary inquiry fails to develop sufficient information to justify a full investigation, the FBI must end the inquiry and record its closing. In sensitive criminal matters, the FBI must notify the U.S. Attorney of the closing and record the fact of the notification in writing. *Id.* § II.B.7.

## **B. Major Revisions to the Guidelines**

The revised General Crimes Guidelines altered authorization procedures and time limits for preliminary inquiries to provide agents with greater flexibility to respond to terrorist and criminal activity. The major revisions to the preliminary inquiry provisions of the Guidelines were:

- extending from 90 to 180 days the period for initial authorizations;
- authorizing SACs to grant the first 2 extensions for preliminary inquiries and lengthening the duration of these extensions from 30 to 90 days;
- permitting the use of mail covers during a preliminary inquiry;<sup>282</sup>
- authorizing initiation of preliminary inquiries to determine whether grounds exist to initiate a racketeering enterprise or terrorism enterprise investigation; and
- emphasizing that the FBI should not hesitate to use any lawful techniques consistent with the Guidelines, even if intrusive, where the intrusiveness is warranted in light of the seriousness of the possible crime or the strength of the information obtained.

---

<sup>281</sup> A “sensitive criminal matter” is “any alleged criminal conduct involving corrupt action by a public official or political candidate, the activities of a foreign government, the activities of a religious organization or a primarily political organization or the related activities of any individual prominent in such an organization, or the activities of the news media; and any other matter which in the judgment of a Special Agent in Charge (SAC) should be brought to the attention of the U.S. Attorney or other appropriate official in the Department of Justice, as well as FBI Headquarters.” GCI Guidelines § II.A.2 at B-70.

<sup>282</sup> A mail cover is the recording of any data appearing on the outside cover of any class of mail. Manual of Investigative Operations and Guidelines (MIOG) II § 10-6.2.



### **C. The OIG Review of Preliminary Inquiries**

The focus of our review was on the Guidelines' requirements for predication to initiate or extend the preliminary inquiry, and notifications to appropriate DOJ officials of the initiation and closing of sensitive criminal matters.

In our visits to 12 FBI field divisions, we reviewed a sample of 46 preliminary inquiries at 9 FBI field office locations. From a list of over 60,000 preliminary inquiries provided to us by the FBI, we requested 6 inquiries from each of 12 field offices.<sup>283</sup> Three offices did not identify any preliminary inquiries in general crimes cases, while others provided fewer than six. We examined key requirements of the preliminary inquiry provisions of the General Crimes Guidelines. We focused on whether the field office had complied with the following notifications and authorizations.

- Did the SAC authorizing the preliminary inquiry ensure that the allegation or other information justifying the inquiry was recorded in writing?
- If the preliminary inquiry remained open longer than 180 days, did the SAC timely authorize extensions?
- Was the U.S. Attorney or appropriate DOJ official notified of the opening and closing of preliminary inquiries involving sensitive criminal matters?

### **D. Compliance Findings**

All but one of the preliminary inquiry files we examined contained the written allegation or information justifying the inquiry. Nineteen of the preliminary inquiries extended past the initial 180-day authorization period, of which 13 continued more than 270 days and required a second extension. Of these 19 preliminary inquiries, 10 (53 percent) did not contain the necessary documentation authorizing the extensions, closings, or conversions to full investigations. Ten of the 13 files (77 percent) for preliminary inquiries that extended over 270 days contained no documentation authorizing a second extension, closing, or conversion. Thus, of the 32 instances when an extension, conversion to full investigation, or closing was appropriate, we found authorization documentation missing in 20 instances or 63 percent. The following table summarizes these findings.

---

<sup>283</sup> We requested a list of preliminary inquiries that were open on or opened after May 30, 2002.

**TABLE 5.1**

<b>OIG Compliance Findings from 46 Preliminary Inquiries in Select FBI Field Offices</b>	
<b>Preliminary inquiries that extended past the initial 180-day authorization period</b>	19
<ul style="list-style-type: none"><li>Preliminary inquiries extending past the initial 180-day authorization period that did not contain necessary documentation of authorization for extensions, closings, or conversions to full investigations</li></ul>	10 (53%)
<b>Preliminary inquiries that extended past the first extension period</b>	13
<ul style="list-style-type: none"><li>Preliminary inquiries extending past the first extension period that did not contain necessary documentation of authorizations for second extensions, closings, or conversions to full investigations</li></ul>	10 (77%)

Our review also identified six preliminary inquiries involving sensitive criminal matters. We found that all appropriate notifications to the U.S. Attorneys were made in each of these cases.

#### **E.     OIG Analysis and Recommendations**

Preliminary inquiries allow FBI agents to investigate information that is ambiguous or incomplete. The limitations on the duration of preliminary inquiries ensure that a determination whether to end the inquiry or continue with a full investigation is made in a reasonable period of time.

As we discuss in Chapter Two, abuses of the FBI's investigative authorities in conducting domestic intelligence investigations led to the first set of Attorney General Guidelines issued in 1976. Among the abuses documented by the Church Committee were the FBI's extensive use of preliminary inquiries to collect information about students, civil rights

groups, and war protestors, among others.<sup>284</sup> The 1976 Guidelines eliminated the use of certain intrusive techniques in preliminary inquiries, including the recruiting of new informants and the use of mail covers. The revisions to the Domestic Security Investigation Guidelines in 1983 eliminated preliminary inquiries in domestic security investigations, permitting them to be used only in the conduct of general crimes investigations.

In light of the extended time periods for preliminary inquiries and the devolution of significant authority to field managers in the May 2002 revisions of the General Crimes Guidelines, we believe our findings regarding the FBI's failure to develop adequate controls to ensure that authorizations for extensions, conversions, and closings of preliminary inquiries are obtained and documented in case files merit corrective action.

We recommend that the FBI take the following step.

(20) Ensure compliance with the General Crimes Guidelines' requirements to obtain and document authorizations for the extension, conversion to full investigation, and closing of preliminary inquiries.

### **III. General Crimes Investigations**

#### **A. Role of General Crimes Investigations**

The FBI has jurisdiction to investigate federal crimes except where such responsibility is specifically assigned by statute or otherwise to another federal investigative agency. General Crimes Guidelines Preamble; see generally 18 U.S.C. § 533 (2002).

The FBI's general crimes investigations address a broad range of criminal conduct and account for the majority of FBI criminal investigations. From May 2002 through March 2004, the FBI had over 62,000 open general crimes investigations. The FBI categorizes these investigations in program classifications such as Domestic Terrorism, Organized Crime, Drug Program, White Collar Crime, Civil Rights, and Violent Crime and Major Offenders. MIOG Introduction, § 2-1.<sup>285</sup>

---

<sup>284</sup> See "Final Report of the Select Committee to Study Governmental Operations with Respect to Intelligence Activities" (hereafter "Church Committee"), Book III, *Supplementary Detailed Staff Reports on Intelligence Activities and the Rights of Americans*, at 527.

<sup>285</sup> Domestic terrorism cases are divided between general crimes (acts of terrorism) and criminal intelligence (enterprises) investigations, which are discussed in the following section.

## **B. Significant Requirements**

The General Crimes Guidelines impose requirements for both the predication needed to open a full investigation and the authorization process that the FBI must follow. Under the Guidelines, “[a] general crimes investigation may be initiated when facts or circumstances reasonably indicate that a federal crime has been, is being, or will be committed.” General Crimes Guidelines § II.C.1. The Guidelines explain that information justifying the opening of an investigation “must [have] an objective factual basis” and that “a mere hunch is insufficient.” *Id.* In making the determination whether to open a general crimes investigation, the FBI “may take into account any facts or circumstances that a prudent investigator would consider.” *Id.*

The approval process to open an investigation under the General Crimes Guidelines is similar to the process for opening a preliminary inquiry. The FBI supervisor authorizing an investigation must ensure that facts or circumstances satisfy the reasonable indication standard described above and that this information is recorded in writing. *Id.* § II.C.3. In “sensitive criminal matters,” written notification must be provided to the U.S. Attorney or an appropriate DOJ official, as well as to FBI Headquarters, as soon as practicable after the investigation commences. *Id.* When that investigation is terminated, the FBI must notify the appropriate federal prosecutor within 30 days. *Id.* § II.C.4.

The Guidelines also contain procedures for disseminating information regarding general crimes. With limited exceptions, in circumstances where the FBI obtains credible information concerning serious criminal activity not within its investigative jurisdiction, the Guidelines require the relevant FBI field office to promptly transmit the information, or to refer the complainant, to the law enforcement agencies having jurisdiction. *Id.* § II.C.6. Where full disclosure is not made to these agencies within 180 days, the FBI field office is required to notify FBI Headquarters in writing of the facts and circumstances concerning the criminal activity. *Id.*

## **C. Major Revisions to the Guidelines**

The May 2002 revisions to the General Crimes Guidelines did not alter the scope of general crimes investigations. As described above, the most significant changes concerning general crimes investigations involved preliminary inquiries, not full investigations. These changes were in addition to revisions that expressly recognized the fundamental shift in the FBI’s focus to the detection and prevention of terrorist attacks.

#### **D. The OIG Review of General Crimes Investigations**

To examine the FBI's compliance with the general crimes provisions of the General Crimes Guidelines, we reviewed 72 general crimes files at 12 field offices. Initially, we requested that each field office provide documentation on six "sensitive criminal matters" within the meaning of § II.A.2 of the Guidelines. However, many of the case files identified by the FBI did not involve circumstances that met this definition, and we were advised that it was not practicable to isolate qualifying cases from the FBI's many general crimes files during our site visits. In total, we examined 32 files involving sensitive criminal matters, which accounted for 44 percent of all the general crimes files we reviewed.

With respect to the Guidelines' requirements in general crimes cases, we focused on the following issues.

- Was the opening basis, including predication, in writing?
- In sensitive criminal matters, did the FBI provide required opening notifications to the U.S. Attorney's Office or DOJ and to FBI Headquarters?
- Did the FBI provide required closing notifications to the U.S. Attorney's Office or DOJ?
- Did the FBI appropriately disseminate investigative information outside DOJ?

#### **E. Compliance Findings**

Of the 72 general crimes files we reviewed, we determined the following.

- 71 of the 72 files identified the predication in the case opening or ancillary documentation.
- Of the 32 sensitive criminal matters we examined, the FBI notified the U.S. Attorney's Office or the DOJ in all investigations for which such notification was required, although 5 of the case files did not contain the written notification mandated by the Guidelines.<sup>286</sup> In one of the sensitive criminal matters, it was not evident that FBI Headquarters was notified of the case opening.
- 22 of the sensitive criminal matters were still pending at the time of our site visits. Of the 10 sensitive criminal matters that had

---

<sup>286</sup> In these five instances, the notifications were evident from other documentation contained in the investigative file.

closed, the FBI notified the U.S. Attorney's Office or DOJ of the case closing within the required time in nine instances.<sup>287</sup>

- When disseminating information regarding these general crimes investigations to other law enforcement agencies, the FBI consistently documented an adequate basis to do so, in conformity with the Guidelines.

### **Predication in Opening Documentation**

We found only one matter where it was not possible to determine the predication in the opening documentation. This case was investigated in concert with another DOJ component. Later entries in the file, however, established that there was reasonable indication that a crime had been committed and that the basis for the investigation was sound.

### **Notifications in Sensitive Criminal Matters**

#### **(i) Opening Notifications**

The General Crimes Guidelines require that in sensitive criminal matters, the predication for investigations be recorded in writing and provided to both DOJ and FBI Headquarters as soon as practicable after commencement of the investigation.<sup>288</sup> Although we found that the U.S. Attorney, or DOJ, was consistently notified of the basis for sensitive criminal matter openings, in 5 of these 32 cases the written notification required by the Guidelines was not included in the case file. We therefore had to find evidence of the notification from other information in the file (such as an FBI internal memorandum indicating field discussions with a prosecutor). In one of these instances, we were unable to locate the written notification to FBI Headquarters and could not determine from other case file documentation that the notification was made.

#### **(ii) Closing Notifications**

Closing notifications were contained in every case file where appropriate.<sup>289</sup>

---

<sup>287</sup> The Guidelines provide that “[i]n every sensitive criminal matter, the FBI shall notify the appropriate federal prosecutor of the termination of an investigation within 30 days of such termination.” GCI Guidelines § II.C.4 at B-73.

<sup>288</sup> GCI Guidelines § II.C.3 at B-72.

<sup>289</sup> However, in one instance DOJ was not notified of the case closing until 40 days after closure – 10 days beyond the required time limit.

## **Dissemination of Information to Other Law Enforcement Agencies**

Our review examined 16 instances where the FBI disseminated information developed in general crimes investigations to other law enforcement agencies pursuant to § II.C.6 of the General Crimes Guidelines. We determined in each case that the FBI adhered to the applicable Guidelines' requirements.

### **F.     OIG Analysis and Recommendations**

Our review found that the FBI generally is complying with the requirements of the General Crimes Guidelines governing general crimes investigations.

## **IV.    Criminal Intelligence Investigations**

### **A.     Role of Criminal Intelligence Investigations**

In contrast to general crimes investigations, which target individuals and specific criminal acts, the focus of criminal intelligence investigations is on a group or enterprise. The purpose of these investigations is to obtain information concerning the nature and structure of an enterprise – including information relating to its membership, finances, geographical dimensions, past and future activities, and goals – with a view toward detecting and preventing the enterprise's criminal activities and prosecuting those responsible for them. There are two types of criminal intelligence investigations: racketeering enterprise investigations (REIs) and terrorism enterprise investigations (TEIs). GCI Guidelines, Introduction, B.

Terrorism enterprise investigations, which can develop intelligence to help prevent terrorist acts, are classified as either domestic or international.<sup>290</sup> Domestic terrorism investigations involve U.S. persons

---

<sup>290</sup> The "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001" (USA PATRIOT ACT) incorporates a new definition of "domestic terrorism," in order to correspond to the existing definition of "international terrorism." *Domestic terrorism* is defined to mean activities occurring primarily within the territorial jurisdiction of the United States involving acts dangerous to human life that are a violation of the criminal laws of the United States or any state and appear to be intended to intimidate or coerce a civilian population, influence the policy of a government by intimidation or coercion, or affect the conduct of a government by mass destruction, assassination, or kidnapping. 18 U.S.C. § 2331(5).

*International terrorism* involves violent acts or acts dangerous to human life that are a violation of the criminal laws of the United States or any state, or that would be a criminal violation if committed within the jurisdiction of the United States or any state. These acts appear to be intended to intimidate or coerce a civilian population, influence the policy of a government by intimidation or coercion, or affect the conduct of a government by (continued)

residing in the United States who are not acting on behalf of a foreign power, and who may be conducting criminal activities in support of terrorist objectives. International terrorism investigations involve U.S. persons or foreign nationals in the United States who are targeting national security interests on behalf of a foreign power.<sup>291</sup> After the issuance of the revised Investigative Guidelines on May 30, 2002, and until a new FBI investigative classification was established effective October 1, 2003, that combined criminal and intelligence international terrorism investigations, the FBI conducted a limited number of international terrorism investigations under the terrorism enterprise investigation Guidelines.<sup>292</sup> Since October 2003, however, the FBI has elected to use the terrorism enterprise provisions of the General Crimes Guidelines solely to investigate domestic terrorism matters, while international terrorism investigations are conducted under the Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection (NSI) Guidelines.<sup>293</sup>

## **B. Significant Requirements**

### **Racketeering Enterprise Investigations**

The General Crimes Guidelines authorize the initiation of racketeering enterprise investigations “when facts or circumstances reasonably indicate that two or more persons are engaged in a pattern of racketeering activity as defined in the RICO statute, 18 U.S.C. § 1961(5).” General Crimes Guidelines § III.A.2.a. The Guidelines state that “[t]he standard of ‘reasonable indication’ is identical to that governing the initiation of a general crimes investigation.” *Id.*

Racketeering enterprise investigations must be approved by the SAC with notification to FBI Headquarters and must be based upon a written

---

mass destruction, assassination, or kidnapping, and occur primarily outside the territorial jurisdiction of the United States or transcend national boundaries in terms of the means by which they are accomplished, the persons they appear intended to intimidate or coerce, or the locale in which their perpetrators operate or seek asylum. 18 U.S.C. § 2331(1).

<sup>291</sup> See FBI Publication #0308, *Terrorism 2000/2001*, at iii.

<sup>292</sup> To formalize the merger of intelligence and criminal operations, the FBI abandoned separate case classifications for criminal international terrorism investigations and intelligence international terrorism investigations, consolidating them into a single classification for international terrorism. This reclassification officially classifies an international terrorism investigation as one that can employ intelligence tools as well as criminal processes and procedures.

<sup>293</sup> As noted in the Introduction to this report, the Attorney General issued the revised NSI Guidelines on October 31, 2003.



recommendation indicating that the standard for opening the investigation is satisfied. Id. § III.A.5.a. The FBI also must notify the Organized Crime and Racketeering Section of DOJ's Criminal Division and any affected U.S. Attorney's Office of the initiation of the investigation. Id. § III.A.5.b. The first authorization period may not exceed one year, and renewals may be obtained for additional periods also not to exceed one year. Renewal authorization is obtained from the SAC, with notification to FBI Headquarters and the Organized Crime and Racketeering Section of DOJ's Criminal Division. Id. § III.A.5.c. The SAC must review the investigations on or before the expiration of the period for which the investigation and each renewal is authorized. Id. § III.A.5.d.

### **Terrorism Enterprise Investigations**

The standard for initiating a terrorism enterprise investigation also incorporates the "reasonable indication" threshold. The General Crimes Guidelines provide:

A terrorism enterprise investigation may be initiated when facts or circumstances reasonably indicate that two or more persons are engaged in an enterprise for the purpose of: (i) furthering political or social goals wholly or in part through activities that involve force or violence and a violation of federal criminal law, (ii) engaging in terrorism as defined in 18 U.S.C. §§ 2331(1) or (5) that involves a violation of federal criminal law, or (iii) committing any offense described in 18 U.S.C. § 2332b(g)(5)(B).

Id. § III.B.1.a. As with racketeering enterprise investigations, the Guidelines provide that terrorism enterprise investigations must be authorized by the SAC with notification to FBI Headquarters, and they must be based upon a written recommendation.<sup>294</sup> The FBI also must notify the Counterterrorism Section of DOJ's Criminal Division, DOJ's Office of Intelligence Policy and Review (OIPR), and any affected U.S. Attorney's Office of the opening of a terrorism enterprise investigation.<sup>295</sup> General Crimes Guidelines § III.B.4.a. Authorization periods and procedures in these investigations are the same as for racketeering enterprise investigations. Id. § III.B.4.b and c. The FBI is required to report to DOJ's Counterterrorism Section and OIPR the

---

<sup>294</sup> The MIOG, however, provides that a full investigation of domestic terrorism may be authorized by a SAC only with concurrence of FBI Headquarters. MIOG § 100-2.3(3). This inconsistency between the Guidelines and the MIOG is discussed in Chapter Eight.

<sup>295</sup> The Terrorism and Violent Crime Section of the DOJ was renamed the Counterterrorism Section.

progress of terrorism enterprise investigations within 180 days of their initiation and the results at the end of each year the investigation continues. Id. § III.B.4.f.

### **C. Major Revisions to the Guidelines**

The revisions to the criminal intelligence provisions of the General Crimes Guidelines emphasized the reduction of administrative requirements by devolving approval authority to FBI field offices, extending authorization periods, and expanding the scope of terrorism enterprise investigations. Major changes to the Guidelines included:

- authorizing the SAC rather than FBI Headquarters to approve the initiation and renewal of criminal intelligence investigations;
- extending from 180 days to 1 year the period for initial authorizations and renewals; and
- expanding the scope of TEIs to include certain kinds of racketeering activity with a terrorism nexus.

### **D. The OIG Review of Criminal Intelligence Investigations**

#### **Racketeering Enterprise Investigations**

To examine the FBI's compliance with key provisions of the racketeering enterprise investigation provisions of the General Crimes Guidelines, we reviewed all REIs at the 12 FBI field offices we visited. Because 4 of the offices had no REIs, we reviewed the 14 available REI investigative files at the remaining 8 offices. The FBI provided the OIG with a list of all REIs that were open on or after May 30, 2002, which listed a total of 37 such investigations nationwide. Our review primarily focused on whether the field offices obtained the necessary authorizations and provided appropriate notifications. Specifically, we examined the following authorization and notification requirements.

- Did the SAC authorize an investigation after finding that the facts or circumstances in the written recommendation reasonably indicated that two or more persons were engaged in a pattern of racketeering activity as defined in the RICO statute, 18 U.S.C. § 1961(5)?
- Did the SAC notify FBI Headquarters of the opening of the investigation?
- If the investigation remained open longer than one year, did the SAC review the investigation on or before the expiration of the period for which the investigation was authorized or renewed?

- Did the SAC notify FBI Headquarters when extensions of the REIs were authorized?

In addition, we determined whether there was evidence that the FBI notified the Organized Crime & Racketeering Section of the DOJ Criminal Division and any affected U.S. Attorney's Office of the opening of the investigation.

### **Terrorism Enterprise Investigations**

We asked the FBI to identify 6 terrorism enterprise investigative files for each of the 12 field offices we visited. Only 4 of the 12 offices had any TEIs, and, together, they had 5 TEIs. Our review focused on the following documentation and notification requirements.

- Did the SAC authorize the terrorism enterprise investigation after finding that the facts and circumstances in the written recommendation reasonably indicated that the standard for opening such an investigation was satisfied?
- Did the SAC notify FBI Headquarters of the opening of the terrorism enterprise investigation?
- Was there evidence that the FBI notified the Counterterrorism Section of the DOJ Criminal Division, OIPR, and any affected U.S. Attorney's Office of the opening of the investigation?
- Did the FBI report to the Counterterrorism Section of the DOJ Criminal Division and OIPR the progress of the investigations not later than 180 days after initiation, and the results at the end of each year that the investigation continued?
- If the investigation remained open longer than one year, did the SAC review the investigation on or before the expiration of the period for which the investigation was authorized or renewed?
- Did the SAC notify FBI Headquarters when extensions of the TEIs were authorized?

## **E. Compliance Findings**

### **Racketeering Enterprise Investigations**

We found that documents in each of the 14 REI case files adequately stated the reasons for opening these investigations and that the authorizations were properly provided by the SAC.

With respect to notifications of case openings, the investigative files contained documentation that the field office notified FBI Headquarters in 12 of the 14 cases, or 86 percent of the time. According to the MIOG, the initiation of a racketeering enterprise must be followed by notification,

including all supporting documentation, to FBI Headquarters within 14 calendar days of receiving authorization by the SAC.<sup>296</sup> The FBI also must notify the Organized Crime & Racketeering Section of the DOJ Criminal Division and any affected U.S. Attorney's Office. We found no evidence of notifications to DOJ in 10 of the files we examined (71 percent), while 12 of the 14 files (86 percent) lacked evidence of notification to a U.S. Attorney's Office. One field office told us that once it notifies FBI Headquarters of the opening of a REI, it relies upon Headquarters to notify the U.S. Attorney's Office and/or the Organized Crime & Racketeering Section of DOJ. This practice may account in at least some instances for the missing documentation of opening notifications.

Notifications of renewals also were problematic. The files associated with four of the five investigations that continued beyond the initial authorization period did not contain documentation of notification to FBI Headquarters or evidence of review by the SAC on or before expiration of the initial authorization period. The table below summarizes our findings with regard to Guidelines-related documentation for racketeering enterprise investigations.

---

<sup>296</sup> MIOG § 92-6(2) (imposing 14-day notification requirement). The General Crimes Guidelines require notification to FBI Headquarters but do not specify a deadline. See GCI Guidelines § III.A.5.a at B-76.

**TABLE 5.2**

**Documentation of Racketeering Enterprise Investigation Predication  
and Field Office Notifications to DOJ, USAOs, and FBIHQ**

<b>Field Office</b>	<b>Number of REIs Reviewed</b>	<b>Sufficient Predication in Opening Document</b>	<b>Field Notified FBIHQ of Opening</b>	<b>Documentation of Opening Notification to DOJ OCRS</b>	<b>Documentation of Opening Notification to USAOs</b>	<b>Number Lasting More Than 1 Year</b>	<b>SAC Reviewed Before Expiration</b>	<b>Field Notified FBIHQ re: Extensions</b>
Field Office 2	2	2	2	2	1	1	0	0
Field Office 3	4	4	4	0	0	1	0	0
Field Office 6	2	2	1	1	0	0	N/A	N/A
Field Office 7	1	1	1	0	0	0	N/A	N/A
Field Office 9	1	1	1	0	0	1	1	1
Field Office 10	2	2	1	0	0	1	0	0
Field Office 11	1	1	1	0	1	0	N/A	N/A
Field Office 12	1	1	1	1	0	1	0	0
<b>TOTAL (8)</b>	<b>14</b>	<b>14</b>	<b>12</b>	<b>4</b>	<b>2</b>	<b>5</b>	<b>1</b>	<b>1</b>

## **Terrorism Enterprise Investigations**

We found that documents in the five FBI case files adequately stated the reasons for opening these investigations and that the authorizations were properly provided by the SAC. However, the files we reviewed did not consistently contain evidence of required notifications and reports.

### **Opening Basis Adequately Meets Guidelines' Criteria**

A SAC may authorize a TEI (subject to FBI Headquarters' concurrence) after assuring that the facts or circumstances contained in a written recommendation reasonably indicate the existence of an enterprise as described in the Guidelines. General Crimes Guidelines § III.B.1.a. We found that all five TEIs satisfied the standard to open a terrorism enterprise investigation.

### **Notifications to FBI Headquarters**

The General Crimes Guidelines require notice to FBI Headquarters after a SAC authorizes a terrorism enterprise investigation. Id. § III.B.4.a. We found that in all five cases we examined FBI Headquarters was appropriately and promptly notified of the case initiations.

### **Notifications to the Department of Justice.**

The General Crimes Guidelines require that the FBI notify the DOJ Criminal Division's Counterterrorism Section, OIPR, and any affected U.S. Attorney's Office of the opening of a terrorism enterprise investigation. Id. We found that evidence of these notifications was not consistently present in the case documentation. Only one office's files contained notification to the U.S. Attorney's office for a case initiation. We did not find evidence of notification to the Counterterrorism Section for three of the five case initiations and to OIPR for four of the five cases. Officials from one field office told us that once it notifies FBI Headquarters of the opening of a TEI, it relies upon Headquarters to notify OIPR. This practice may account – in at least some instances – for the absence of documentation of opening notifications.

### **Progress Reports to the Department of Justice**

The General Crimes Guidelines require that the FBI report to the DOJ Criminal Division's Counterterrorism Section and OIPR the progress of TEIs no later than 180 days after their initiation, and the results at the end of each year the investigation continues. Id. § III.B.4.f. The MIOG states that the results of the investigation must be furnished within 180 days to FBI Headquarters with a cover communication setting forth the status of the investigation, and the memoranda must arrive at FBI Headquarters at least ten days before the due date. MIOG § 100-3.1.1. We did not find documentation of this progress report in three of the four investigations that

continued beyond 180 days, including one TEI that extended beyond one year. Moreover, the single field office that drafted a progress report submitted its report 39 days late.

### **Investigations Extending Beyond One Year**

A TEI may be authorized initially for up to one year and may be continued for additional periods each not to exceed one year. General Crimes Guidelines § III.B.4.b. Of the five cases we reviewed, only one continued for more than one year. The SAC authorized this investigation with FBI Headquarters' concurrence for periods less than one year and had approved seven extensions. In accordance with the General Crimes Guidelines, the SAC reviewed the case prior to the expiration of each extension and submitted all required authorization documentation to FBI Headquarters. However, the file did not contain evidence of either the 180-day progress report or the yearly progress reports to DOJ.

### **F. OIG Analysis and Recommendations**

With respect to compliance with the criminal intelligence provisions of the General Crimes Guidelines, our review found that the FBI has not ensured that:

- all required notifications to U.S. Attorneys, DOJ, and FBI Headquarters were timely made and documented in the case files;
- reviews by SACs were documented; and
- reports to DOJ were timely completed and included in the case files.

Opening notifications to DOJ and U.S. Attorneys' Offices were not evident in many of the files for REIs (71 percent and 86 percent, respectively), and notifications of TEIs to DOJ's Counterterrorism Section did not appear in 60 percent of the files. Notifications for both OIPR and the U.S. Attorneys' Offices did not appear in 80 percent of the files. Although only a few files (14 percent) lacked documentation of opening notifications to FBI Headquarters, we found a general lack of consistency in the FBI's documentation practices and supervisory reviews. The MIOG does not specify what procedures should be followed in providing notifications to DOJ and U.S. Attorneys' Offices, or whether such notifications should be documented.

We also identified compliance deficiencies with respect to renewals and reporting. In REIs, documentation of SAC reviews was missing in 80 percent of the case files we examined, as were renewal notifications to FBI Headquarters. Progress reports to DOJ in terrorism enterprise investigations were missing in 75 percent of the case files.

In addition, our review identified a discrepancy between the requirements of the General Crimes Guidelines and the MIOG. One of the

most significant changes to the criminal intelligence provisions of the General Crimes Guidelines in May 2002 was the devolution of approval authority from FBI Headquarters to SACs to initiate and renew criminal intelligence investigations. With respect to terrorism enterprise investigations, the Guidelines provide:

A terrorism enterprise investigation may be authorized by the Special Agent in Charge, with notification to FBIHQ, upon a written recommendation setting forth the facts or circumstances reasonably indicating the existence of an enterprise. . . .

Renewal authorization [for terrorism enterprise investigations] shall be obtained from the SAC with notification to FBIHQ.

General Crimes Guidelines §§ III.B.4.a and b (emphasis added). When the revised General Crimes Guidelines were issued, the Attorney General described the rationale for the change:

[U]nnecessary procedural red tape must not interfere with the effective detection, investigation, and prevention of terrorist activities. To this end, the revised guidelines allow Special Agents in Charge of FBI field offices to approve and renew terrorism enterprise investigations, rather than having to seek and wait for approval from headquarters. I believe this responds to a number of concerns we have heard from our field agents. . . . These major changes will free field agents to counter potential terrorist threats swiftly and vigorously without waiting for headquarters to act.<sup>297</sup>

The FBI, however, amended the MIOG to require not only notification to FBI Headquarters, but also concurrence by FBI Headquarters. Effective April 30, 2004, the MIOG provides:

With regard to full-field terrorism enterprise investigations of domestic terrorism, it is hereby the policy of the CTD [Counterterrorism Division] that, consistent with the revised [Attorney General Guidelines] on General Crimes, Racketeering Enterprise and Terrorism Enterprise Investigations, a full-field terrorism enterprise investigation may be authorized by an SAC only with concurrence of the Domestic Terrorism Operations Section in CTD, FBIHQ.

MIOG § 100-2.3(3) (emphasis added). In light of the Attorney General's stated reasons for the revision of §§ III.B.4.a and b of the General Crimes

---

<sup>297</sup> Prepared Remarks of Attorney General Ashcroft Regarding the Attorney General Guidelines (May 30, 2002).



Guidelines, the current MIOG provision regarding authorization of terrorism enterprise investigations appears to be inconsistent with the requirements of those Guidelines and, in practice, may undercut the rationale underlying this Guidelines revision.

Therefore, we recommend that the FBI take the following steps.

(21) Institute measures to ensure consistency in meeting and documenting the notification and reporting requirements provided in §§ III.A.5 and III.B.4 of the General Crimes Guidelines, including requiring FBI field offices to maintain in the relevant investigative file documentation of the notice of the opening of criminal intelligence investigations to DOJ's Counterterrorism, Organized Crime and Racketeering Sections, Office of Intelligence Policy and Review (OIPR), and the relevant U.S. Attorneys' Offices as required in racketeering enterprise investigations and terrorism enterprise investigations. The FBI should also ensure that progress reports required by the Guidelines in terrorism enterprise investigations are provided to OIPR, DOJ's Counterterrorism Section, and FBI Headquarters.

(22) Discuss with DOJ how to reconcile § 100-2.3(3) of the MIOG, requiring Headquarters' concurrence with the initiation and renewal of terrorism enterprise investigations, with §§ III.B.4.a and b of the General Crimes Guidelines, which authorize field level initiation and renewal of these investigations.

## **V. Part VI of the General Crimes Guidelines: Counterterrorism Activities and Other Authorizations**

### **A. Rationale for the New Part VI Authorities**

As we discussed earlier in this report, following the September 11 terrorist attacks the Attorney General ordered a comprehensive review of the Attorney General Guidelines. In remarks accompanying the announcement of the revised Guidelines, the Attorney General explained that the Investigative Guidelines "bar[red] FBI field agents from taking the initiative to detect and prevent future terrorist acts unless the FBI learns of possible criminal activity from external sources." His remarks focused on the absence of clear authority to be proactive in preventing terrorist attacks:

Under the current guidelines, FBI investigators cannot surf the web the way you or I can. Nor can they simply walk into a public event or a public place to observe ongoing activities. They have no clear authority to use commercial data services that any business in America can use. These restrictions are a competitive advantage for terrorists who skillfully utilize sophisticated techniques and modern computer systems to

compile information for targeting and attacking innocent Americans.<sup>298</sup>

These restrictions led the Attorney General to conduct a reevaluation of the Investigative Guidelines and the Guidelines governing foreign intelligence and foreign counterintelligence investigations.<sup>299</sup> Two of the four guiding principles for the Guidelines revisions identified by Attorney General Ashcroft focused on measures to enhance the FBI's authority to proactively investigate terrorist threats by, among other means, visiting public places, attending public events, and "surfing" the Internet. Specifically, the Attorney General stressed that "even absent specific investigative predicates," FBI agents were now "empowered to scour public sources for information on future terrorist threats." In addition, he noted that the FBI "will also be able to enter and observe public places and forums just as any member of the public might."<sup>300</sup>

FBI Director Mueller also addressed the need for proactive authority to access public information in his July 2002 testimony before Congress:

---

<sup>298</sup> Prepared Remarks of Attorney General Ashcroft Regarding the Attorney General Guidelines (May 30, 2002).

A staff statement issued by the National Commission on Terrorist Attacks Upon the United States also stated that the pre-September 11 Guidelines were understood by some in the FBI as restricting their ability to access public places and public resources:

The guidelines limited the investigative methods and techniques available to agents conducting preliminary investigations of potential terrorist activities or connections. They prohibited the use of publicly available source information, such as that found on the Internet, unless specified criteria were present.

These restrictions may have had the unintended consequence of causing agents to even avoid legitimate investigative activity that might conceivably be viewed as infringing on religious liberties or lawful political protest.

Agents we interviewed believed these limitations were too restrictive and adversely affected their intelligence investigations.

National Commission on Terrorist Attacks Upon the United States, *Staff Statement No. 9: Law Enforcement, Counterterrorism, and Intelligence Collection in the United States Prior to 9/11*, at 8 (April 13, 2004).

<sup>299</sup> The FCI Guidelines governing foreign intelligence and foreign intelligence investigations were revised effective October 31, 2003, and were renamed the Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection.

<sup>300</sup> Prepared Remarks of Attorney General Ashcroft Regarding the Attorney General Guidelines (May 30, 2002). See also Statement of The Honorable John Ashcroft Attorney General United States Department of Justice before the Senate Judiciary Committee, July 25, 2002, available at: <http://www.usdoj.gov/ag/testimony/2002/072502agtestimony.htm>.

The changes in the Attorney General Guidelines . . . are designed to increase the ability of our field agents to gather the intelligence we need to prevent terrorist attacks. To that end, they reduce some of the bureaucratic hurdles requiring Headquarters' approval for certain steps, and in the provision that has gotten a great deal of attention, they permit FBI agents to go to public places where anyone else, except FBI agents, including state and local police and non-Justice Department law enforcement agents, were always free to go.

Remember, though, that they may do so solely for the purpose of detecting and preventing terrorist activities, and there are strict limits on record-keeping in such instances.

Now [sic] information obtained from such visits may be retained unless it relates to potential criminal or terrorist activity, and I must say and emphasize, as an institution we are and must be and continue to be deeply committed to the protection of individuals' constitutional and statutory rights. Nothing in the amended guidelines changes that.<sup>301</sup>

Our review examined the steps the FBI took to implement the new and expanded authorities in Part VI of the General Crimes Guidelines, particularly as they relate to the FBI's authority to visit public places and attend public events for the purpose of detecting and preventing terrorist activities. We describe our findings on the FBI's use of these authorities and the internal controls in place to ensure that predication standards and record retention constraints are observed, and conclude with our recommendations. In Chapter Eight, we analyze and evaluate the FBI's steps for implementing these measures, along with other authorities contained in the revised Investigative Guidelines.

## **B. New Authorities Added to the General Crimes Guidelines**

Part VI of the General Crimes Guidelines, entitled "Counterterrorism Activities and Other Authorizations," states that the FBI needs to be proactive in preventing terrorist acts against the United States by authorizing a number of activities "which can be carried out even in the absence of a checking of leads, preliminary inquiry, or full investigation." The new authorizations include activities specifically focused on terrorism (Subpart A) and other tools that are available to obtain information about both terrorism and non-terrorism-related crimes (Subpart B).

---

<sup>301</sup> *Oversight Hearing on Counterterrorism*: Hearing Before the Senate Committee on the Judiciary, 107<sup>th</sup> Cong. 11 (2002) (Statement of Robert S. Mueller, III, Director, Federal Bureau of Investigation).

Subpart A of Part VI authorizes the FBI to engage in two types of “counterterrorism activities”: 1) utilizing information systems, which the FBI may operate or participate in, to identify and locate terrorists and alien supporters of terrorist activity; and 2) visiting public places and events on the same terms and conditions as members of the public “for the purpose of detecting or preventing terrorist activities.”

In Subpart B, the FBI is authorized to conduct topical research, use online resources, and prepare reports and assessments “for purposes of strategic planning or in support of investigative activities.”<sup>302</sup>

### **C. The OIG Review of the FBI’s Use of Part VI Authorities**

As with other Investigative Guidelines, we first identified significant requirements of Part VI of the General Crimes Guidelines that could be tested. We focused on the following questions.

- How frequently has the FBI utilized the authority to visit public places and attend public events for the purpose of detecting or preventing terrorist activities?
- What internal controls are in place in the field or at FBI Headquarters to ensure that minimum predication standards and record retention guidance are followed?

Neither the General Crimes Guidelines themselves nor the MIOG require that agents obtain supervisory approval of or document activities carried out pursuant to Part VI. In advance of our visits to 12 FBI field offices from May to August 2004, we sought to determine what data is collected about the FBI’s utilization of Part VI authorities. We therefore asked the 12 field offices to provide us with documentation reflecting field office policies and procedures regarding the use of these authorities and their document retention policies pertaining to information derived from use of the authorities.

In addition, we collected relevant guidance issued from FBI Headquarters, chiefly from the Office of the General Counsel, the Criminal Investigative Division, and the Counterterrorism Division; surveyed Division Counsel; reviewed a sample of communications between the OGC’s newly established point of contact on constitutional and privacy issues and Division Counsel; examined relevant FBI and DOJ congressional testimony; conducted interviews of Headquarters officials and relevant field personnel

---

<sup>302</sup> An OGC guidance memorandum dated October 7, 2002, suggests that the FBI may have had certain of these authorities prior to the May 2002 revisions. For example, the guidance states that the Part VI authorities “*enhance* the FBI’s ability to visit public places and attend public events . . .”; “*expand*” its ability to gather investigative information from the Internet; and that the provision addressing the FBI’s ability to conduct general topical research “serves to *clarify* pre-existing policy” (emphasis added).

during our visits to 12 FBI field offices; and, in March 2005, conducted interviews of the 12 SACs of those field offices.

#### **D. Compliance Findings**

##### **1. The FBI's Use of Part VI Authorities Since May 30, 2002, and the FBI's Implementing Guidance**

Our effort to collect data from investigative files comparable to those we reviewed in connection with the Confidential Informant Guidelines, the Undercover Guidelines, the Consensual Monitoring Guidelines, and the General Crimes Guidelines was unsuccessful. Apart from the various guidance memoranda issued by FBI Headquarters that we discuss below, none of the 12 field offices we visited provided information in response to our request for documentation reflecting established procedures governing visits to public places and events. We found no forms generated by FBI Headquarters or any of the 12 field offices we visited for recording the fact of a visit to a public place or attendance at a public event pursuant to this new authority. The FBI may not retain information derived from such activities “unless it relates to potential criminal or terrorist activity.”<sup>303</sup> If the information does not relate to criminal or terrorist activities, the only information that can be retained is documentation of the fact of the visit, which, according to OGC guidance, should be maintained in a non-investigative or “zero” file.

However, FBI policy on the maintenance and review of zero files is different from the highly regimented rules pertaining to investigative files. Zero files are created for each FBI classification number to enable the FBI to maintain information relating to that classification that does not, at the time, meet the requirements for initiating an investigation or that does not relate to an ongoing investigation.<sup>304</sup> However, zero files must be reviewed by a supervisor at 120-day intervals, rather than every 90 days in the case of investigative files, or more frequently if deemed appropriate by the SAC.<sup>305</sup>

---

<sup>303</sup> GCI Guidelines § VI.A.2. See also FBI Office of the General Counsel, *Guidance to the Field: New Attorney General Guidelines on General Crimes, Racketeering Enterprise and Terrorism Enterprise Investigations*, at 5 (October 7, 2002).

<sup>304</sup> See MAOP 2-4.1(2). For example, if the FBI were to receive information on a possible criminal civil rights violation (classification 44), but the required threshold to open an investigation were not present, the information would be placed in a 44-0 file and indexed for future retrieval. All information related to possible civil rights violations in that field office would be entered in this file, the hard copy of which contains cumulative information, filed chronologically, on all possible civil rights violations. In conducting a file review of the 44-0 file, it is more difficult for supervisors to evaluate at one time the related bits of information scattered in many separate files than when reviewing a discrete investigative file.

<sup>305</sup> See MAOP § 1-1.4(2).

We were told that program coordinators are also supposed to review zero files. In addition, during the Inspection process every three years, the Inspection Division reviews zero files to ensure they do not contain work of a higher priority than other matters being addressed by the field office.

The number of times that the FBI has used the Part VI authorities is difficult to determine. The Department of Justice advised the House Judiciary Committee in May 2003, that the FBI does not maintain centralized statistics on how many times agents attend public meetings.<sup>306</sup> The Department further stated that fewer than 10 of the 45 field offices the FBI had informally surveyed reported that they had conducted investigative activities at mosques since September 11, 2001, and only one of the investigative activities was conducted pursuant to Part VI authorities of the General Crimes Guidelines.<sup>307</sup>

We asked the FBI Director whether he knew how frequently these authorities are utilized. He reiterated that the FBI does not require agents to obtain supervisory approval or send a form to Headquarters, and therefore it is difficult to determine to what extent these authorities have been used.

In addition, before our visits to 12 FBI field offices, we surveyed the FBI's Division Counsel on a variety of topics related to the Investigative Guidelines, including the subjects about which they have been consulted on Part VI authorities.<sup>308</sup> Our survey showed that 65 percent of surveyed Division Counsel had been consulted regarding the authority to visit or attend public events. Of these inquiries, 96 percent said they were consulted about whether it is permissible to conduct surveillance of or attend such events and 86 percent also stated that they had been consulted about record retention issues.

Our survey also revealed a need for more guidance on the appropriate use of the new authorities. For example, when we asked whether Division Counsel encountered ambiguities or interpretive questions about the General Crimes Guidelines, 23 percent of surveyed Division Counsel responded "yes." Of that number, 83 percent stated that the authority to

---

<sup>306</sup> Letter from Jamie E. Brown, Acting Assistant Attorney General, Office of Legislative Affairs, Department of Justice, to F. James Sensenbrenner, Jr., Chairman, House Committee on the Judiciary (May 13, 2003) (Responses to Committee's Questions on U.S. PATRIOT ACT Implementation and Related Matters) (hereafter *May 13, 2003 DOJ Written Responses to House Judiciary Committee Questions*).

<sup>307</sup> The Department of Justice stated that the remaining visits were conducted pursuant either to preliminary inquiries or full investigations. *May 13, 2003, Department of Justice Written Responses to House Judiciary Committee Questions*.

<sup>308</sup> The role of Division Counsel in the FBI's 56 field offices is discussed in Chapter Three.

visit public places or attend public events generated questions, while 72 percent stated that the permissibility of disseminating the information to law enforcement agencies and others generated questions.

The responses of Division Counsel to our survey questions regarding Part VI authorities are presented below.

**TABLE 5.3**

**Division Counsel's Views on Consultation  
Regarding Part VI Authorities of the General Crimes Guidelines**

<b>Question</b>	<b>Response</b>		
17. Since May 30, 2002, have you been consulted regarding the authority to visit or attend any events for the purpose of detecting or preventing terrorist activities in the absence of leads, a preliminary inquiry, or a full investigation? [AGG Section VI.A.2.]	Yes	51	65%
	No	28	35%
a. Were you consulted as to whether it was permissible to conduct surveillance of, or attend, public events?	Yes	50	96%
	No	1	2%
b. Have you been consulted regarding the propriety of retaining information derived from surveillance of, or attendance at, public events?	Yes	44	86%
	No	7	14%
b-1. Describe the subject matter of the consultation you had regarding the propriety of retaining information derived from the surveillance of or attendance at public events. (Check all that apply.)	Retaining the information	43	98%
	Placing the information in a file	40	91%
	Indexing the information	32	73%
	Uploading the information into ACS	26	59%
19. An EC dated 03/27/03 from FBIHQ OGC notified all field offices of the designation of one attorney at FBIHQ OGC as the point of contact to coordinate OGC guidance and assistance on investigative, operational and policy matters that may have an impact on, or be perceived as having an impact on, individual rights and liberties (e.g., First Amendment or privacy issues).	a. What is your role in advising the Special Agents and supervisors in your field office on individual rights and liberties? (Check all that apply.)		
	I have provided advice regarding visits to any place and the attendance at any event open to the public for the purpose of detecting or preventing terrorist activities.	71	90%
	I have provided advice on issues involving the intrusiveness of various investigative techniques.	67	85%
	I have provided advice regarding online search activity and	51	65%

Question	Response		
	accessing online sites and forums.		
	I have provided advice regarding general topical research.	48	61%
	I have provided advice regarding the operation and participation in identification, tracking, and information systems regarding terrorist activities.	34	43%
	I have provided advice regarding the preparation of general reports and assessments concerning terrorism or other criminal activities for purposes of strategic planning.	25	32%
	Other	6	8%
	b. In light of the 03/27/03 EC from FBIHQ OGC, how would you characterize the adequacy of available guidance on privacy and other civil liberties issues that arise in your field office as they relate to the revised Guidelines?		
	Fully satisfactory	29	37%
	Somewhat satisfactory	27	34%
	Have not encountered	9	11%
	Neither satisfactory nor unsatisfactory	7	9%
	Somewhat unsatisfactory	4	5%
	Not satisfactory	3	4%
	c. Have you consulted the FBIHQ OGC attorney designated in the 03/27/03 EC on privacy and civil liberties issues?		
	Yes	40	51%
	No	39	49%
28. Have you encountered any ambiguities or interpretative questions involving the Attorney General's Guidelines on General Crimes, Racketeering Enterprise and Terrorism Enterprise Investigations?	Yes	18	23%
	No	61	77%
a. With respect to ambiguities or interpretative issues arising under the Attorney General's Guidelines on General Crimes, Racketeering Enterprise and Terrorism Enterprise Investigations, what aspect of the revised Guidelines generated the question? (Check all that apply.)	Visits to any place and attendance at any event open to the public to detect or prevent terrorist activities and retention of information obtained (AGG Section VI.A.2.)	15	83%
	Permissibility of disseminating information to law enforcement agencies and others (AGG Section V.)	13	72%
	Circumstances related to public demonstrations under which a	8	44%



Question	Response		
	terrorism enterprise investigation may be initiated (AGG Section III.B.1.c.)		
	Circumstances under which operation or participation in identification, tracking, and information systems are permitted (AGG Section VI.A.1.)	6	33%
	Performing general topical research (AGG Section VI.B.1.)	5	28%
	Conducting online search activity and access to online sites and forums (AGG Section VI.B.2.)	5	28%
	Other	2	11%
	The choice of investigative techniques in preliminary inquiries (AGG Section II.B.4.)	1	6%

The Division Counsel survey indicates that 21 months after the effective date of the revised Guidelines, field personnel continued to struggle with questions about the use of these authorities. Only 37 percent of the survey respondents stated that they found fully satisfactory the guidance regarding privacy and other civil liberties issues that arose in their field offices in connection with use of the new Guidelines.

## **2. Internal Controls Regarding Predication for the Exercise of Part VI.A.2 Authorities**

Under the General Crimes Guidelines, the FBI must have particularized information to justify the checking of leads or initiating a preliminary inquiry or a full investigation. By contrast, the Part VI.A.2 authorities permit the FBI to visit public places or attend public events “on the same terms and conditions as members of the public” and only “for the purpose of detecting and preventing terrorist activities.” General Crimes Guidelines § VI.A.2.

The FBI relied upon OGC and its Headquarters operating divisions to develop guidance on the Investigative Guidelines. We therefore reviewed the guidance memoranda sent to the field from FBI Headquarters. The following memoranda, which we describe in more detail below, address the predication required for using these authorities.

- October 7, 2002, guidance summarizing the revised General Crimes Guidelines (OGC – “Guidance to the Field: New Attorney General Guidelines on General Crimes, Racketeering Enterprise and Terrorism Enterprise Investigations”).
- March 27, 2003, guidance establishing a Headquarters Point of Contact (OGC – “Point of Contact for Guidance on Constitutional

Rights and Privacy Issues Arising in FBI Investigations/Operations”).

- March 19, 2004, guidance emphasizing FBI policy regarding the protection of civil liberties in connection with use of authorities under both the Investigative Guidelines and the NSI Guidelines (OGC - “Protection of Civil Liberties”).
- April 26, 2004, guidance clarifying the standards for collecting, retaining, and disseminating information in connection with the FBI’s “Special Events” responsibilities (CTD – “Guidance to Atlanta, Boston and New York Divisions Concerning Information Collection, Maintenance, and Dissemination for G-8, DNC and RNC Special Events, 2004”).
- September 1, 2004, guidance emphasizing the limitations on the Part VI authorities and specifying how to collect, maintain, and disseminate the information collected in connection with protest activity (CTD – “Law Enforcement Monitoring of Protest Groups for Indications of Criminal or Terrorist Activity”).

While discussing recurring questions about predication, the guidance memoranda encourage, but do not require, supervisory approval for FBI agents to attend a public event. For example, the October 7, 2002, OGC memorandum states:

If time permits, an agent should obtain his or her supervisor’s approval before visiting a public place or attending a public event to detect or prevent terrorist activity. This policy will help to ensure that the attendance is for a law enforcement purpose authorized by this section, and reflects the appropriate balance between law enforcement and First Amendment concerns. In assessing the use of this law enforcement technique, a supervisor may want to consider, for example, factors such as the potential to detect or prevent terrorist activity, and the potential chilling effect on First Amendment protected activity. Good judgment and discretion are essential to ensure that this investigative technique is in fact effective while at the same time protecting constitutional rights.

In the March 27, 2003, guidance memorandum, the OGC designated an Assistant General Counsel as the point of contact at Headquarters to “coordinate guidance and assistance to FBI Headquarters and Field Offices on investigative, operational and policy matters that may have an impact on, or be perceived as having an impact on, constitutional and privacy

rights and interests.”<sup>309</sup> Among the topics about which field agents were encouraged to consult the point of contact was “attendance at meetings and public gatherings of religious, political or other groups/organizations.”<sup>310</sup>

The Counterterrorism Division’s September 1, 2004, guidance addressed the use of Part VI authorities in the context of attending and surveilling protest events. With respect to predication, it stated:

**Attendance and Surveillance at Public Events.** – Agents may not conduct surveillance of individuals or groups solely for the purpose of monitoring the exercise of rights protected by the First Amendment. . . . The second broad investigative basis for attendance and surveillance is found under Part VI of the General Crimes Guidelines. Under this section, agents may attend a public event or visit a public place on the same terms as the general public. **Under this authority, however, such attendance may be undertaken for the purpose of detecting or preventing terrorism, or assessing a threat to national security.** Further, although the revised Guidelines permit such attendance even if neither a preliminary inquiry nor a full investigation is open, agents are reminded that this authority is limited to matters observable and obtainable in a public forum. Undercover activity, surreptitious entry into a private gathering at these events, and certain other investigative techniques (e.g., consensual recording of conversations) are not permitted under this authority. (Emphasis in original).

We also examined a sampling of the communications between OGC’s point of contact and the field divisions. We noted that OGC has urged caution with respect to use of Part VI authorities and suggested that the FBI is on firmer footing if it obtains “individualized justification” prior to visiting public places. The OGC guidance also reiterated the Privacy Act prohibitions against including names in the FBI’s records systems based solely on the exercise of First Amendment rights.

In a response to Congress, the Department also articulated the considerations the FBI weighed in evaluating whether to require supervisory approval prior to permitting agents to visit public places or attend public events pursuant to Part VI.A.2:

**Question.** The GAO Report reflects that “FBI headquarter [sic] officials are currently considering whether to require mandatory supervisory approval prior to allowing an agent to enter a public

---

<sup>309</sup> Office of the General Counsel, *Point of Contact for Guidance on Constitutional Rights and Privacy Issues Arising in FBI Investigations/Operations* (March 27, 2003).

<sup>310</sup> *Id.* at 3.

place or attend a public meeting.” Have you made any final decisions on this matter? What is the possible downside of requiring supervisory approval of this easily abused investigative technique?

**Response:** In implementing this provision of the Guidelines, existing FBI policy states that, unless time does not permit seeking such approval, an agent should obtain his or her supervisor’s approval before visiting a public place or attending a public event to detect or prevent terrorist activity. No final decisions have been made as to whether such prior approval should be mandatory. In considering whether such a requirement would be appropriate, the FBI does not want to discourage the effective use of this provision in the primary mission of detecting and preventing terrorism. The Guidelines are intended to “enable Agents of the FBI to perform their duties with greater certainty, confidence and effectiveness,” while providing the American people with “a firm assurance that the FBI is acting properly under the law.” (Guidelines, Preamble.) Any policies or procedures that are adopted must conform to this intent.<sup>311</sup>

In our April 2005 interview of Director Mueller, he emphasized that he balanced the need to encourage use of the proactive Part VI authorities with the desire to be able to measure and evaluate their use. He said he had expected the Virtual Case File System would have been implemented and would have had features that facilitated notification to FBI Headquarters of the use of Part VI authorities. The Director stated that had that capability been available, he was prepared to require the “relatively modest imposition” on field agents of sending notice to Headquarters. However, in light of the problems in implementing the Virtual Case File, the Director said he would have to revisit the question whether to require supervisory approval and some form of documentation beyond the entries in zero files.

Finally, it is important to remember that the FBI has multiple sources of authority to enter public places pursuant to the Investigative Guidelines, the NSI Guidelines, and other authorities.

---

<sup>311</sup> Letter from William E. Moschella, Assistant Attorney General, Department of Justice, to Orrin G. Hatch, Chairman, Senate Committee on the Judiciary (March 4, 2004) (Responses to Questions Posed to Robert S. Mueller, III, Director of the FBI, Before the Committee on July 23, 2003) (hereafter *March 4, 2004, FBI Director Mueller’s Responses to House Judiciary Committee Questions*). The General Accountability Office report referenced in the question is *FBI Reorganization: Progress Made in Efforts to Transform but Major Challenges Continue* (hereafter “GAO Report on FBI Reorganization”), June 18, 2003, GAO-03-759T, at 29, available at: <http://www.gao.gov/new.items/d03759t.pdf>.

### **3. Internal Controls for Record Retention Relating to the Exercise of Part VI.A.2 Authorities**

Part VI contains strict limitations on the FBI's authority to retain information derived from its visits to public places and events, stating, "No information obtained from such visits shall be retained unless it relates to potential criminal or terrorist activity." General Crimes Guidelines VI.A.2. In addition to the OGC memorandum dated October 7, 2002, noted above, we identified several guidance memoranda distributed by the FBI that restate the prohibition against improperly retaining information derived from these authorities.

However, due to the manner in which FBI field offices record and maintain information regarding the exercise of Part VI.A.2 authorities and the absence of centrally retrievable data, we were unable to determine whether the FBI is retaining information derived from these activities in conformity with the General Crimes Guidelines and implementing guidance.

OGC guidance has noted the distinction between what the FBI may retain in full investigations and what it may retain from the exercise of Part VI authorities. On March 19, 2004, OGC guidance entitled "Protection of Civil Liberties" stated that information derived from the surveillance of subjects in the course of an open investigation "should be collected, maintained in FBI records, and disseminated in compliance with the Privacy Act and departmental policy."<sup>312</sup> On the other hand, personal identifying information may only be retained from the surveillance of persons under Part VI authorities if the information is "relevant to an existing investigation or preliminary inquiry; by itself or in combination with other known information, justifies a new inquiry or investigation; or relates to another law enforcement activity the FBI is authorized by law or regulation to conduct."<sup>313</sup>

---

<sup>312</sup> The guidance stated that information retained from such surveillance should be maintained in an appropriate control file but may not contain "identifying information about individuals or groups in attendance, absent a valid law enforcement basis." An OGC official told the OIG that the guidance memorandum should have referred to a "zero file" rather than a "control file." Control files are different from "zero files" in that information contained in control files is captured in the FBI's Automated Case Support (ACS) system, and leads may be assigned from control files. See MAOP § 2-4.1.5.

<sup>313</sup> The distinction between what the FBI is permitted to retain in the course of routine investigative activities and what it is permitted to retain when utilizing the Part VI authorities was reiterated in the Counterterrorism Division's September 1, 2004, guidance, *Law Enforcement Monitoring of Protest Groups for Indications of Criminal or Terrorist Activity*. Similar guidance was issued by the Counterterrorism Division on April 26, 2004, *Guidance to Atlanta, Boston and New York Division Concerning Information Collection, Maintenance, and Dissemination for G-8, DNC and RNC Special Events, 2004*. This guidance stated that information "which does not rise to the level of predication for a preliminary inquiry or full investigation" should be placed in a special control file, as distinguished from an (continued)

Similarly, in responding to congressional concerns about record retention issues related to Part VI authorities, Director Mueller stated that “if information obtained during the visit rises to the level of a lead, such information should be properly documented, including a statement describing how the information is related to potential criminal or terrorist activity, and then filed accordingly.”<sup>314</sup>

The following diagram provides FBI Division Counsel’s views regarding Part VI consultations and the clarity of guidance issued by FBI Headquarters concerning retention of information derived from use of Part VI.A.2 authorities during the period May 2002 to February 2004.<sup>315</sup> Our survey indicated that 65 percent of Division Counsel were consulted about the FBI’s authority to visit or attend public events under Part VI authority. Of that number, 96 percent said they were consulted about the permissibility of surveilling or attending public events, 86 percent said they were consulted about the propriety of retaining information derived from these visits, and 63 percent stated that they did not believe FBI guidance on information retention was clear when the revised Guidelines were issued.

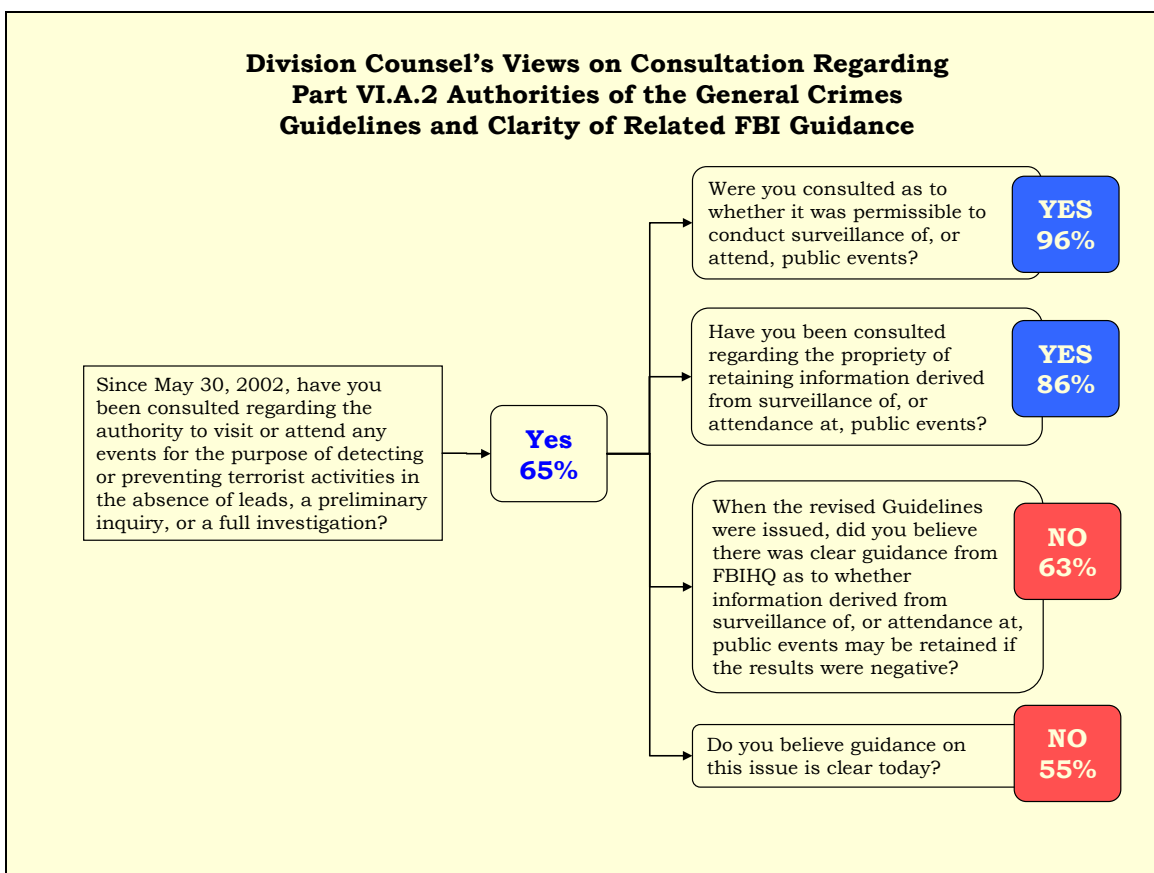
---

investigative file, created specifically for information relating to the special event. At the end of the special events, agents were instructed to close the administrative file for the event but could distribute information collected in it “to the extent that it is pertinent to that office’s special event responsibilities.”

<sup>314</sup> March 4, 2004, Responses to House Judiciary Committee Questions.

<sup>315</sup> As noted above, FBI Headquarters issued additional guidance since this survey was conducted which addresses some recurring issues arising in the exercise of Part VI authorities.

**DIAGRAM 5.1**



### **E. OIG Analysis and Recommendations**

The FBI has provided significant guidance to the field about the highly sensitive Part VI authorities. The FBI does not require advance supervisory approval or documentation of the use of the authority to visit public places or attend public events, and agents do not open a discrete investigative or administrative file in the absence of a preliminary or full investigation. Some SACs we interviewed in the 12 field offices said they require approval by or notification of a first line supervisor of an agent's use of the authority to visit public places or attend public events. However, because of the limited amount of information we were able to obtain from FBI Headquarters or field offices about their utilization of the Part VI authorities, it is unclear, even with respect to the 12 field offices we visited, how often these authorities have been used or whether the FBI is using these authorities in conformity with the Guidelines. That said, we did not find indications that these authorities are used extensively. Field agents, their supervisors, and Headquarters personnel repeatedly told us that given the many leads, inquiries, and active investigations that they must pursue, visiting public places and events absent an indication of unlawful conduct or threat potential is not a priority.

As discussed above and in Chapter Eight, over the last three years since the revised Guidelines were issued, the Office of the General Counsel and the Counterterrorism Division have generated guidance addressing the distinctions between record retention in preliminary inquiries or full investigations, on the one hand, and the stricter limitations imposed on retaining information collected in the course of monitoring protest activities or in connection with the FBI's "special event" responsibilities, on the other.

In our interviews of FBI Headquarters managers, our surveys of Chief Division Counsel, and our field interviews, FBI employees expressed recognition of the FBI's obligation to protect civil liberties. The FBI personnel we questioned about the Part VI authorities – from new agents through the Director – exhibited awareness of the FBI's past lapses in the area of domestic political investigations and surveillance of protesters. Specifically with respect to the authority to visit public places and attend public events, field and Headquarters personnel we interviewed said they are acutely sensitive to the need to exercise these authorities carefully and responsibly.

What is missing, however, in the FBI's implementation of the Part VI authorities is the capability to retrieve and analyze information about when and how these authorities are used; whether information derived from visiting public places and attending public events is being inappropriately retained, indexed, or disseminated; and, for at least the first two years since the Guidelines were in effect, clear, easily accessible guidance on these authorities. Nearly two-thirds of Division Counsel who responded to our survey said they believed the guidance was unclear when the Guidelines were issued, and more than half believed the guidance was still unclear 21 months later when they responded to our survey. In our view, in light of the minimal predication standards and the potential for abuse, the FBI should reconsider whether advance supervisory approval and easily retrievable documentation should be required when Part VI authority is used.

In evaluating the sufficiency of the Guidelines' provisions and related FBI guidance on Part VI.A authorities, we compared the internal controls for predication in the FBI's use of Part VI authorities with the FBI's parallel authorities under the NSI Guidelines. Effective October 31, 2003, the NSI Guidelines introduced a new investigative activity called "threat assessments." The NSI guidelines permit the FBI to visit public places and attend public events for the:

proactive collection of information concerning threats to the national security, including information on individuals, groups, and organizations of possible investigative interest, and information on possible targets of international terrorist activities or other national security threats. . . . This is comparable to the authorization under Part VI of the Attorney General's Guidelines on General Crimes, Racketeering



Enterprise and Terrorism Enterprise Investigations to engage in information collection for counterterrorism or other law enforcement purposes without any more specific investigative predication . . . .

NSI Guidelines, Introduction, § A.1.<sup>316</sup> While the FBI's specific requirements for approval of threat assessments and documentation of information derived from the exercise of this authority are classified, we believe that the FBI should require at least equivalent measures for supervisory approval and documentation as are required for threat assessments under the NSI Guidelines.

Particularly with respect to our analysis of the Part VI authorities and throughout this review, we have been mindful of the leading priority of the FBI: to “develop intelligence about terrorist activity and use that intelligence to disrupt their plans.”<sup>317</sup> We agree with the sentiments expressed by Director Mueller that a careful balance must be struck between the objectives of encouraging proactive use of the Part VI authorities and having the assurance that at least a field supervisor has approved their use. However, we believe that the FBI should reevaluate – now and in conjunction with its ongoing plans for technology improvements and contemplated revisions of the Attorney General Guidelines – its guidance with respect to the authority to visit public places and attend public events, and for retaining, indexing and disseminating information derived from those activities.

First, the FBI's other authorities in the NSI, and investigative portion of the General Crimes Guidelines to visit public places such as religious sites are subject to layers of supervisory approval and documentation requirements. For example, a preliminary inquiry or full investigation of a religious site or its leadership under the NSI Guidelines' counterterrorism classification requires SAC approval with notice to FBI Headquarters and the DOJ. Comparable investigative activity under the General Crimes Guidelines is a “sensitive criminal matter” requiring approval by the SAC with notice to FBI Headquarters and either the U.S. Attorney's Office or the DOJ. These approvals would have to be obtained before an agent entered the religious site. A covert entry of a religious site by an undercover agent would also be classified as a sensitive circumstance under both the NSI Guidelines and the General Crimes Guidelines, requiring in either case FBI Headquarters approval. Likewise, before a source operating at the express

---

<sup>316</sup> The unclassified portions of the NSI Guidelines are available at: <http://www.usdoj.gov/olp/nsiguideelines.pdf>.

<sup>317</sup> Testimony of Robert S. Mueller, III, Director, Federal Bureau of Investigation, Before the Senate Judiciary Committee, May 20, 2004, available at: <http://www.fbi.gov/congress/congress04/mueller052004.htm>.

direction of the FBI could enter a religious site, and before the FBI could open a source who is already a member of a religious organization, the SAC would have to approve the activity, as it would be classified a “sensitive circumstance” under both the Confidential Informant Guidelines and the NSI Guidelines.

We appreciate that the new authorities to visit public places and attend public events for the purpose of detecting or preventing terrorist activities are designed to be used proactively and should not be encumbered with layers of supervisory approval. We therefore are not recommending that supervisory approval and notification for Part VI authorities be the same as that required for preliminary and full investigations. In the absence of exigent circumstances, however, we believe a field supervisor’s judgment should be brought to bear on the exercise of these new authorities. In addition, we believe the FBI’s use of these authorities should be documented in an easily retrievable fashion.

Second, the FBI has already acknowledged in guidance distributed by OGC and in its response to congressional inquiries that when time permits agents should obtain supervisory approval before exercising Part VI.A.2 authorities and that documentation should be maintained in some retrievable fashion. The FBI recognizes the value of this and encourages its agents to do so. However, we believe a uniform requirement to obtain such approval, absent exigent circumstances, should be implemented.

Third, we believe that the FBI’s practice of retaining information derived from visiting public places or events in zero files does not provide the FBI with centrally retrievable information about the use of these authorities and does not facilitate compliance with the Guidelines’ constraints on record retention and dissemination. A simple, standardized form or an e-mail template could be used to capture when and why these authorities are used. Such a record would serve several purposes: 1) it would enable field supervisors to conduct meaningful “file reviews” every 120 days, even in the absence of an investigative “file”; 2) it would assist the Inspection Division in performing the audit we recommend in Chapter Seven; and 3) it would also allow checks on whether the authorities are used appropriately. Since OGC has already issued guidance recommending that agents should document their attendance at public events pursuant to Part VI authorities, we believe the incremental burden of requiring standardized and easily retrievable documentation is reasonable and not significantly burdensome.

Fourth, the added burden on case agents is not likely to be substantial. We were told in many field offices we visited that agents do not have time to visit public places or attend public events other than in connection with checking a lead, a preliminary investigation, or a full investigation. Consequently, requiring supervisory approval and easily

retrievable documentation when these authorities are used should not be onerous.

Fifth, the FBI's information architecture is under a period of fundamental transformation.<sup>318</sup> The FBI has the opportunity now to build into its technology systems the ability to identify the source of all information it collects, stores, and disseminates. Incorporating documentation requirements for the Part VI authorities should be considered now, as the FBI upgrades its information technology systems. Whether the information is collected as evidence for a criminal trial or as part of the FBI's intelligence base, the FBI needs to be able to identify the source of information it collects and retains and be certain that field agents follow appropriate guidance with respect to the intended uses of the information.

We therefore recommend that the FBI take the following steps.

(23) Require field level supervisory approval prior to the exercise of Part VI.A.2 authorities to visit public places or attend public events for the purpose of detecting or preventing terrorist activities, absent exigent circumstances.

(24) Develop a standardized form or a short e-mail template to be completed by case agents to document their use of the Part VI.A.2 authorities.

(25) In light of the survey responses of Division Counsel, consider whether (a) field office practices since May 30, 2002, regarding predication, collection, record retention, indexing, and dissemination of Part VI.A information, and the practices regarding utilization of "zero files" or other files to capture Part VI.A information, are in conformity with the Guidelines and FBI guidance; (b) there is a need for further guidance on predication, collection, record retention, indexing, dissemination, or other issues; and (c) FBI Headquarters managers should have access to data reflecting use of Part VI.A.2 authorities in order to be satisfied that these authorities are used in conformity with the Guidelines.

---

<sup>318</sup> See Office of the Inspector General of the Department of Justice, Audit Report No. 05-07, *The Federal Bureau of Investigation's Management of the Trilogy Information Technology Modernization Project*, Feb. 2005, available at: <http://www.usdoj.gov/oig/audit/FBI/0507/final.pdf>.

## **CHAPTER SIX**

### **PROCEDURES FOR LAWFUL, WARRANTLESS MONITORING OF VERBAL COMMUNICATIONS (CONSENSUAL MONITORING)**

In this chapter we discuss the role of consensual monitoring in FBI investigations, the requirements of the Consensual Monitoring Guidelines, the May 2002 revisions to the Guidelines, and the results of our compliance review of consensual monitoring files in FBI field offices. We then provide our analysis and recommendations based on those findings and on our surveys and interviews of Headquarters and field personnel.

#### **I. Role of Consensual Monitoring**

Consensual monitoring is the interception by an electronic device of any wire, oral, or electronic communication where one of the parties to the communication has given prior consent to the monitoring or recording. A warrant is not required to conduct consensual monitoring, and the party providing consent may be a government agent. See 18 U.S.C. § 2511, (2) (c) – (e) (2002).

The Attorney General Guidelines governing consensual monitoring cover only non-telephonic consensual monitoring.<sup>319</sup> The types of monitorings addressed by these Guidelines include the use of body recorders and transmitting devices. To supplement the Guidelines, the FBI imposes detailed administrative and management controls on the use of both non-telephonic and telephonic consensual monitoring. MIOG II § 10-10.

Non-telephonic consensual monitoring is one of many electronic surveillance techniques available to investigators. Other techniques include dialed number recorders, “trap and trace” devices, and wiretaps. Dialed number recorders, sometimes called “pen registers,” capture electronic impulses generated by a telephone line. The data includes call information such as the telephone numbers dialed, date and time of the activity, and other special services subscribed to by the target through the telephone company, such as caller-ID, call forwarding, conference calls, and call waiting. A “trap and trace” device records the originating phone numbers of all incoming calls on a particular phone line. A wiretap is the interception of oral, wire, and electronic communications.<sup>320</sup> While all of these

---

<sup>319</sup> We provide a copy of the CM Guidelines in Appendix B.

<sup>320</sup> Title III of the Omnibus Crime Control and Safe Streets Act, 18 USC §§ 2510-2522, enacted in 1968, established the basic law for federal and state law enforcement interceptions performed for the purpose of criminal investigations. A wiretap is commonly referred to as a “Title III.”

techniques require a warrant or court order, only wiretaps provide investigators with the record of the conversation. The advantage of consensual monitoring over the methods described above is that no warrant is required and the investigator can obtain a record of the conversation.

## **II. Significant Requirements**

In this section we summarize the requirements of the Consensual Monitoring Guidelines, including those relating to authorizations, application requirements, and recordkeeping.

The Consensual Monitoring Guidelines establish separate authorization procedures for consensual monitorings that require written approval from the DOJ, those that may be authorized by an FBI Special Agent in Charge (SAC) or Assistant Special Agent in Charge (ASAC), and those that may be authorized in emergency situations.

Section II.A of the Consensual Monitoring Guidelines requires DOJ approval for monitorings that concern certain categories of public officials and others, such as members of Congress and state Governors.<sup>321</sup> When an investigation relates to such persons, requests for authorization must be approved in writing by the Director or Associate Director of the Office of Enforcement Operations of the Criminal Division of DOJ.<sup>322</sup> In addition, the FBI requires that a SAC or ASAC must approve requests to conduct non-telephonic consensual monitoring in both sensitive and non-sensitive matters, as described below. MIOG II §§ 10-10.3(1) and (3).

The Guidelines specify that the application to conduct consensual monitoring must address eight factors: 1) the reasons for the monitoring; 2) if the monitoring is for investigative purposes, a citation to the principal criminal statute involved; 3) the nature of any danger to the consenting party if the monitoring is designed for protection; 4) the location of the monitoring device; 5) the location and primary judicial district where the monitoring will take place; 6) the length of time needed for the monitoring,

---

<sup>321</sup> “Sensitive” individuals are listed in Part II.A of the Guidelines and include members of Congress, federal judges, and the Governor, Lieutenant Governor, or Attorney General of any state. See CM Guidelines § II.A at B-90. For certain categories of individuals, DOJ approval is required when the monitoring relates to an investigation in which the sensitive person is a target of the investigation (e.g., a Governor). Section II.A of the Guidelines also identifies persons for whom the monitoring request must be approved by DOJ only when they are a party to the monitored communication (e.g., a member of the diplomatic corps).

<sup>322</sup> Authority to engage in consensual monitoring where written DOJ approval is required may also be given by the Attorney General, the Deputy Attorney General, the Associate Attorney General, the Assistant Attorney General or Acting Assistant Attorney General in charge of the Criminal Division, or a Deputy Assistant Attorney General in the Criminal Division. CM Guidelines III.C at B-93.

but in no event more than 90 days from the day the monitoring is scheduled to begin; 7) the names of the persons, if known, who will be monitored; and 8) whether the facts of the surveillance have been discussed with the U.S. Attorney, Assistant U.S. Attorney, or DOJ attorney responsible for a particular investigation, and that the attorney advises that the consensual monitoring is appropriate under the Guidelines. Requests for renewal of such authorizations must contain all the information required for the original application and must explain why the additional monitoring is needed. Consensual Monitoring Guidelines § III.A(1)-(9).

The authorization procedures for consensual monitorings that do not require DOJ approval (non-sensitive monitorings) are set forth in Section V of the Guidelines. That section states that permission for such monitorings must come from the head of the agency or his or her designee. In the case of the FBI, this may be a SAC or ASAC. As with sensitive monitorings, the FBI must obtain advice from a U.S. Attorney, Assistant U.S. Attorney, or DOJ attorney responsible for the investigation that the proposed monitoring is legal and appropriate. Consensual Monitoring Guidelines § V.

The Guidelines further require that agencies maintain records for all consensual monitorings that they have conducted. *Id.* The FBI has developed Form FD-759, captioned “Notification of SAC/ASAC Authority Granted for Use of Telephonic and/or Nontelephonic Consensual Monitoring Equipment in Criminal Matters Only,” to document approval by a SAC or ASAC for the use of consensual monitoring equipment in both sensitive and non-sensitive matters. Form FD-759 addresses the eight factors listed above. In addition, for sensitive monitorings, this form must be accompanied by a letterhead memorandum that addresses the same eight factors. MIOG II § 10-10.3(9).

The Guidelines do not identify the requirements necessary to obtain approval for non-sensitive monitorings. Part V does, however, require that records for non-sensitive monitorings must be maintained that contain all the information required for sensitive monitorings, including the time needed for the monitoring and documentation of the required attorney advice.<sup>323</sup>

---

<sup>323</sup> MIOG II § 10-10.3(1). Section 10-10.1(4) addresses the maintenance of monitoring records:

Separate control files – one for telephonic consensual monitoring and another for nontelephonic consensual monitoring (body recorders and/or transmitting devices) should be established in each field office. Documents relative to the authorization and utilization of these techniques should be retained in the appropriate control file. These control files will be for the purpose of the SAC’s administrative control and for use during the inspection.

(continued)

The Guidelines also provide authorization procedures for monitoring requests in emergency situations. Emergency requests in cases in which DOJ approval is required may be made by telephone to the DOJ Criminal Division and later reduced to writing as soon as practicable after authorization has been obtained. The Guidelines require that oral requests include all the information contained in written requests, and that documentation relating to the oral authorization be maintained in an appropriate filing system. Consensual Monitoring Guidelines § III.B. The MIOG provides that emergency requests for sensitive monitorings may be authorized verbally by DOJ. MIOG Part II, § 10-10.3(1). In addition, the Guidelines state that “each department or agency shall establish procedures for emergency authorizations in cases involving non-sensitive circumstances similar to those that apply with regard to cases that involve . . . sensitive circumstances . . . .” Consensual Monitoring Guidelines § V. The MIOG, however, does not contain provisions that implement this requirement.

The duration of authorizations for sensitive monitorings is addressed in § III.A.6 of the Guidelines, which requires monitoring requests to state the amount of time needed to perform the monitoring and limits monitoring periods to no more than 90 days. Extensions for additional periods of up to 90 days may be obtained provided a demonstration is made of the need for continued monitoring. Consensual Monitoring Guidelines § III.A.6. Section V of the Guidelines requires records for non-sensitive monitorings to contain all the information required for sensitive monitorings, including the time needed for the monitoring.

The MIOG restates the Guidelines’ language regarding authorization periods for sensitive monitorings. MIOG II §10-10.3(9)(f). For non-sensitive monitorings, the MIOG provides that non-telephonic consensual monitoring (NTCM) in criminal matters may be approved by the SAC for the duration of the investigation. *Id.* §§ 10-10.3(1) and (3).

### **III. Major Revisions to the Consensual Monitoring Guidelines**

The May 2002 revisions to the Consensual Monitoring Guidelines relaxed administrative requirements associated with the authorization of consensual monitoring. The most significant revisions included the following.

---

The MIOG further provides that:

SAC approval for nonsensitive NTCM [nontelephonic consensual monitoring] usage is to be documented on Form FD-759. . . . [and] is to be typewritten, completed in its entirety and forwarded to the appropriate FBIHQ entities within seven workdays of the date authority is granted as indicated on Item 5 of the form.

MIOG II § 10-10.3(1).

- Removing the requirement to obtain concurrence or authorization from a federal prosecutor for consensual monitorings. Instead, the prosecutor must advise that the proposed monitoring is legal and appropriate.<sup>324</sup> When the attorney cannot provide this advice for reasons unrelated to the legality or propriety of the monitoring, the required advice may be obtained from a designated attorney in the DOJ's Criminal Division.
- Allowing delegations of authority to approve monitorings to ASACs in certain circumstances, such as monitorings that do involve sensitive persons or circumstances.

At the time the Guidelines were revised, trial attorneys were sometimes constrained by state ethics rules from providing advice regarding monitorings that were legally appropriate.<sup>325</sup> An additional concern was that the existing requirement of obtaining approval by a SAC for consensual monitorings could “result in a loss of investigative opportunities because of an overly long approval process,” and hence it was necessary to delegate authority to ASACs to “facilitate FBI investigative operations.”<sup>326</sup>

#### **IV. The OIG Review of the FBI's Compliance with the Consensual Monitoring Guidelines**

To assess the FBI's compliance with the Consensual Monitoring Guidelines, we reviewed the documentation supporting 103 consensual monitoring “overhears” (i.e., the recorded verbal communication captured by the monitoring device) in 11 field offices. For each monitoring we examined the following key requirements of the Guidelines.

- Was the monitoring approved before the recording began?
- Did the FBI obtain written approval from the DOJ when the monitoring involved “sensitive” individuals identified in the Consensual Monitoring Guidelines?

---

<sup>324</sup> Memorandum from FBI Office of the General Counsel, *Revised Department of Justice Procedures for Lawful Warrantless Monitoring of Verbal Communications*, July 5, 2002.

<sup>325</sup> *Id.* This change was prompted by the so-called “McDade Amendment,” which subjects federal attorneys to state laws and rules governing the practice of law. 28 U.S.C. § 530B (1999). Because many state ethics rules prohibit attorney contact with represented parties, prosecutors risked violation of these rules when authorizing consensual monitorings.

<sup>326</sup> Memorandum from Attorney General John Ashcroft, *Procedures for Lawful, Warrantless Monitoring of Verbal Communications*, May 30, 2002, at 2.



- Did the FBI document that the facts of the surveillance were discussed with the responsible prosecutor and that the prosecutor advised that the consensual monitoring was legal and appropriate?
- Did the FBI renew the monitoring when appropriate?

## **V. Compliance Findings**

As noted above, the MIOG requires that FBI Special Agents request authorization to conduct non-telephonic consensual monitorings on Form FD-759. Because this Form collects information on all of the Guidelines issues we examined, including required written approval from SACs or ASACs, our review concentrated on the information provided on the Form. We found the following.

- Overhear recordings were made in 9 of the 103 monitorings prior to the authorization date on Form FD-759.
- 2 of the 103 monitorings required written DOJ approval because they involved the monitoring of “sensitive” individuals. The file relating to one of these monitorings did not contain documentation indicating that DOJ had been contacted for approval.
- Agents recorded that an Assistant U.S. Attorney had advised that the monitorings were legal and appropriate in each of the 103 monitorings.<sup>327</sup>
- One of the 103 overhear recordings, which related to the investigation of a “sensitive” individual, occurred over 90 days after approval by the SAC or ASAC, but no documentation was included in the file indicating that an extension was requested.<sup>328</sup>

### **Recording Overhears Prior to SAC or ASAC Approvals**

The Guidelines require that a SAC or ASAC authorize monitoring requests in circumstances where the Guidelines do not require written DOJ approval (i.e., when monitoring non-sensitive persons). In addition, the

---

<sup>327</sup> The most recent version of Form FD-759 states that the Assistant U.S. Attorney has *advised* that the monitoring is legal and appropriate, consistent with the May 2002 Guidelines changes. The earlier version of Form FD-759 stated that the Assistant U.S. Attorney *concurred* in the use of the technique.

<sup>328</sup> We also found that 27 non-sensitive monitorings, or 26 percent of the 103 overhear recordings, occurred over 90 days after approval by the SAC or ASAC and lacked documentation in the file indicating that extensions were requested. However, as we explain below, we believe that the Guidelines are ambiguous with respect to the permissible duration of authorizations for non-sensitive monitorings.

MIOG requires SAC or ASAC approval in addition to DOJ authorization in sensitive monitorings.

Ten of the FD-759s we reviewed recorded approval dates by the SAC or ASAC after the first overhear was recorded. This number does not include those instances when the Form FD-759 contained a notation that approval was granted verbally prior to the first recording. The recording of overhears occurred from between 1 and 59 days prior to receiving approval by the SAC or ASAC, as shown below.

**TABLE 6.1**

**OIG Compliance Findings on Consensual Monitorings Conducted Without Written Authorization in Select FBI Field Offices**

<b>Number of Violations</b>	<b>Number of Days From First Overhear to First Authorization</b>	<b>Field Office</b>
2	1	Field Offices 5 & 6
1	3	Field Office 3
1	24	Field Office 4
1	25	Field Office 12
1	27	Field Office 12
1	56	Field Office 12
1	58	Field Office 1
1	59	Field Office 1

According to our interviews of field office personnel, when recordings were made within a few days of the approvals by the SAC or ASAC, the case agents received oral approvals from the managers prior to the recordings. However, the oral approvals were not noted on the Form FD-759, and we were provided no other evidence of the approvals in response to our request for documentation.

**Monitorings Requiring DOJ Approval**

Section II.A of the Consensual Monitoring Guidelines requires written authorization by the DOJ Criminal Division's Office of Enforcement Operations for consensual monitoring of "sensitive" persons. To implement this provision, the MIOG requires that, in addition to the submission of the Form FD-759, the field office must provide a memorandum to FBI Headquarters for transmission to DOJ describing the information required

by the Guidelines. Our review found that of two monitorings we reviewed that required DOJ approval, one was supported by documentation indicating that such approval had been received and the other was not.

### **Attorney Advice**

Our review of consensual monitoring files revealed that case agents always recorded information regarding their receipt of advice that the proposed monitoring was legal and appropriate. We did not encounter any instances in which an Assistant U.S. Attorney refused to provide advice based on concerns related to the McDade law.<sup>329</sup>

### **Length of Time Authorized for Monitoring**

Section III.A of the Consensual Monitoring Guidelines lists the information that must be included in any request to monitor an oral communication that requires written DOJ approval. Section III.A.6 provides that the request must state the length of time needed for the monitoring and that an initial authorization may be granted for up to 90 days from the day the monitoring is scheduled to begin. Extensions for additional periods of up to 90 days also may be granted. Section V of the Guidelines, which addresses monitorings that do not require DOJ approval, requires that monitoring records include the information set forth in Section III.A, including the length of time needed for the monitoring.

Our review of consensual monitoring records found that for those monitorings that did not require DOJ approval, the FBI was making blanket authorizations for the duration of its investigations rather than specifying the time needed for the monitoring.<sup>330</sup>

Twenty-eight of the overhears we reviewed occurred over 90 days after approval by the SAC or ASAC. One of these occurred in a sensitive

---

<sup>329</sup> The FBI's Office of the General Counsel (OGC) reports that it continues to receive requests from field offices to help overcome some prosecutors' reluctance to approve FBI requests to consensually record a subject who is represented by counsel. The reluctance is based on the concern that approval may violate the state Bar disciplinary rules that typically prohibit contact with represented parties. Federal prosecutors have been subject to these state rules since 28 U.S.C. § 530B, the McDade law, became effective in 1999. This reluctance continues to arise despite extensive legal research by DOJ's Professional Responsibility Advisory Office (PRAO) and FBI OGC which clarifies that pre-indictment covert approaches by a cooperator or undercover agent to a subject does not violate the "represented party" rule according to the prevailing appellate case law.

FBI OGC typically advises field offices to ask the reluctant prosecutors to discuss with their USAO professional responsibility advisor, their criminal chief, and, if need, be the DOJ PRAO.

<sup>330</sup> Form FD-759 includes a check box under the "Duration of proposed use" that provides: "For the duration of investigation."

monitoring. The last overhear date in this matter was 101 days after the initial approval by the SAC or ASAC and 93 days after the first overhear. Representatives from the field office that conducted this monitoring explained that they had inadvertently missed the 90-day deadline, and, in any event, the operational rule they follow is that consensual monitoring authority for sensitive matters begins with the first monitoring. The overhears in the other 27 monitorings were in non-sensitive matters. The last overhears in these matters, which were approved by a SAC or ASAC, occurred from 98 to 764 days after approval.

## **VI. OIG Analysis and Recommendations**

Our review of the FBI's compliance with the Consensual Monitoring Guidelines found that the FBI was generally in compliance with the Guidelines, although we identified notable deficiencies, particularly with regard to the Guidelines' requirements for authorization. Although the MIOG's implementing provisions for the Guidelines require written authorization for all non-telephonic consensual monitorings that are not conducted in emergency situations, in 10 percent of the recorded overhears we examined, supervisory approval post-dated the first overhear, in most cases by more than 3 weeks. The FBI did not provide any documentation from case agents, technicians, or managers demonstrating that the approval was granted prior to recording overhears in these cases. Thus, it appears that, contrary to FBI requirements, agents were not following proper approval procedures in these cases. Our review of FD-759 Forms and ensuing discussions with FBI personnel, including electronic surveillance technicians, established that the Guidelines' requirements for obtaining necessary approvals were not followed in these instances.

We also found that in monitorings that do not involve the "sensitive" persons identified in Section II.A of the Consensual Monitoring Guidelines, the FBI is construing the Guidelines to permit a single approval to authorize consensual monitoring for the duration of its investigations. After consulting with the Office of Enforcement Operations in the DOJ Criminal Division, we believe that the FBI's interpretation of the Guidelines may be in error. Section V of the Guidelines requires that monitoring records include the information set forth in Section III.A.6, which provides that the request must "state the length of time needed for the monitoring" and establishes a 90-day authorization period (emphasis added). The MIOG provides, however, that in non-sensitive consensual monitorings, the SAC or ASAC may approve the monitoring "for the duration of the investigation." MIOG Part II, §10-10.3. This has become a routine practice at the FBI and is incorporated in the standardized FD-759 Forms used to secure approvals. We believe that the FBI and DOJ should discuss the proper interpretation of Section V of the Consensual Monitoring Guidelines and that the FBI should issue clarifying guidance.

In sum, we recommend that the FBI take the following steps.

(26) Ensure that required authorizations for consensual monitoring are obtained in advance and are appropriately documented.

(27) For monitorings that do not require DOJ approval, consult with DOJ to resolve whether the Consensual Monitoring Guidelines should be interpreted to authorize monitoring for more than 90 days (including up to “the duration of the investigation” as currently provided on Form FD-759), or whether the authorization is limited to 90 days. The resulting interpretation should be incorporated in the FBI’s MIOG and communicated to the field.

## **CHAPTER SEVEN**

### **FBI AND DOJ COMPLIANCE OVERSIGHT AND ENFORCEMENT MECHANISMS**

The FBI relies upon various oversight and enforcement mechanisms to ensure compliance with the Attorney General Guidelines. These include two joint FBI-DOJ review committees that approve certain undercover operations and confidential informants, the FBI's Inspection Division, and the employee disciplinary process. In addition, certain FBI program offices conduct field evaluations to gauge the performance of FBI operations. The evaluative criteria employed in such reviews often include requirements that are based on the Attorney General Guidelines. Below we describe how each of these oversight and enforcement mechanisms functions and their respective roles in promoting the FBI's adherence to the investigative standards and authorities set forth in the Guidelines.

#### **I. FBI-DOJ Committees that Approve and Monitor Certain Undercover Operations and Confidential Informants**

We discuss below the committee with authority to approve, fund, modify, extend, or expand the focus of Group I undercover operations, and the committee with authority to approve certain categories of confidential informants.

##### **A. Criminal Undercover Operations Review Committee (CUORC)**

When the first Attorney General Guidelines on FBI undercover operations were issued in 1981, FBI field offices or Headquarters Divisions proposing to initiate certain types of high-risk undercover operations were required to secure the approval of FBI Headquarters and the FBI Director. Since 1978, Headquarters approval has included both the operational unit overseeing the operation (e.g., violent crimes, public corruption) and the Criminal Undercover Operations Review Committee (CUORC). The CUORC is one of the key internal controls employed by the FBI and DOJ to review, approve, modify, and monitor Group I undercover operations involving "sensitive circumstances." In 1979, three voting members from the DOJ were added to the Committee.<sup>331</sup>

---

<sup>331</sup> Initially called the Undercover Operation Review Committee when it was established in September 1978, the Committee consisted of seven voting members from FBI Headquarters. Three DOJ voting representatives were added in 1979 when DOJ attorneys voiced concerns about certain undercover operations and suggested forming a separate review committee from which the FBI's Undercover Operation Review Committee would need to secure approval. The DOJ members added to the CUORC at that time were the Chief of the DOJ Criminal Division's Public Integrity Section and the Assistant Chiefs of the (continued)

Under the May 2002 Guidelines, the CUORC is composed of FBI employees, designated by the FBI Director, and DOJ attorneys designated by the Assistant Attorney General in charge of the Criminal Division.<sup>332</sup> The CUORC chair is a designee of the FBI Director.

The CUORC's members are:

1. the FBI's Deputy Assistant Director of the Criminal Investigative Division (Chairman);
2. FBI Section Chiefs of the Technology Operations Section, Violent Crimes and Major Offenders Section, Counterterrorism Division, Operational Support Section, Cyber Division; Financial Crimes Section, Transnational Criminal Enterprise Section, Integrity in Government/Civil Rights Section, International Terrorism Operations Section 1, Americas Criminal Enterprise Section, and the Domestic Terrorism/Counterterrorism Planning Section;
3. FBI Unit Chiefs of the National Backstopping/Safeguard Unit, Asset/Informant Unit, Confidential Services Unit, Undercover & Sensitive Operations Unit, Civil Litigation Unit, and the Investigative Law Unit, and the Assistant General Counsel, Civil Litigation Unit II;
4. DOJ's Director of the Office of International Affairs; and
5. DOJ Criminal Division Chiefs of the Narcotic and Dangerous Drug Section, Counter Espionage Section, Public Integrity Section, Fraud Section, Domestic Security Section, Organized Crime and Racketeering Section, Child Exploitation and Obscenity Section, Asset Forfeiture and Money Laundering Section, Counterterrorism Section, and Computer Crime and Intellectual Property Section.

The CUORC meets bi-monthly. Its charge is to review, approve, and provide continuing oversight of certain criminal undercover operations conducted in the course of general crimes and criminal intelligence investigations. In particular, upon receipt of a field office's or Headquarters' recommendation, the Committee is responsible for assessing the risks and benefits of proposed criminal undercover operations involving "sensitive

---

Criminal Division's Organized Crime and Fraud Sections. A history of the early versions of the Undercover Guidelines and the Undercover Operation Review Committee can be found in the *Final Report of the Select Committee to Study Undercover Activities of Components of the Department of Justice*, 97<sup>th</sup> Cong. 49-55 (1982).

<sup>332</sup> Undercover Guidelines § IV.D.1 at B-46.

circumstances.”<sup>333</sup> These include investigations of public corruption or other criminal conduct by elected or appointed officials; operations with a substantial risk of violence, physical injury, or financial loss; activities having a significant effect on or constituting significant intrusion into the legitimate operation of a governmental entity; participation in communications between an individual and his or her lawyer, physician, or clergyman; and undercover operations in which undercover agents may participate in felonious activities.<sup>334</sup> Such operations are referred to as “Group I Undercover Operations” or “Group 1 UCOs.”<sup>335</sup>

The following table illustrates the type of Group I UCOs approved by the CUORC:

**TABLE 7.1**

**Group I Undercover Operations Approved  
During FY 2003**

<b>Program</b>	<b>Total</b>
Cyber	[SENSITIVE INFORMATION REDACTED]
Organized Crime/Drug	[SENSITIVE INFORMATION REDACTED]
Violent Crimes & Major Offenders	[SENSITIVE INFORMATION REDACTED]
White Collar Crime	[SENSITIVE INFORMATION REDACTED]
Domestic Terrorism	[SENSITIVE INFORMATION REDACTED]
International Terrorism	[SENSITIVE INFORMATION REDACTED]

**1. The CUORC Review Process**

When an FBI field office or Headquarters Division seeks to initiate, extend, change the focus of, or request additional funding for a Group I UCO, the SAC of the field office must first submit a proposal to the FBI

---

<sup>333</sup> FBI Headquarters must approve a second category of special circumstances in undercover operation proposals. These undercover operations involve “fiscal circumstances,” defined in § IV.C.1 of the Undercover Guidelines, at B-43.

<sup>334</sup> Undercover Guidelines § IV.C.2 at B-44.

<sup>335</sup> Undercover operations that do not involve either sensitive or fiscal circumstances are called “Group II UCOs” and do not initially require FBI Headquarters approval. Undercover Guidelines § IV.B at B-41. Group II UCOs may be initiated and, within certain limitations, extended under the authority of the Special Agent in Charge (SAC). See Field Guide for Undercover and Sensitive Operations (FGUSO) § 2.1(1) (July 25, 2003). We learned that most field offices establish a field office-level review committee to evaluate all Group II proposals, although they are not required to do so.



Headquarters' section handling the investigation.<sup>336</sup> The proposal sets forth the specific details regarding the background, objectives, scenario, and justification of the investigation, the subjects of the undercover operation, the proposed use of informants, and the sensitive or fiscal circumstances involved. The application also contains information on the requested budget for the operation, the investigative team, and any requests for exemptions from the Guidelines (e.g., to lease space or establish a proprietary business). The application must be accompanied by a signed statement from the SAC, the office's Undercover Coordinator, and its Chief Division Counsel acknowledging that they have reviewed and support the proposal. The U.S. Attorney in the District where the operation will be conducted or a Section Chief in the Criminal Division of the DOJ must also submit a letter of support.

FBI Headquarters has a specialized unit within the Operational Support Section of the Criminal Investigative Division (CID) that, among other duties, works with field offices and FBI Headquarters operational units on Group I proposals that are to be submitted to the CUORC for approval. The Undercover and Sensitive Operations Unit (USOU) addresses problems with the proposals and anticipates questions the CUORC may ask at its periodic meetings. It also publishes the Field Guide for Undercover and Sensitive Operations (Field Guide), which contains a step-by-step explanation of the documentation that must accompany applications for undercover operations, including the paperwork needed to administer and to close down an operation. The Field Guide was revised twice since the May 2002 Guidelines were issued, most recently in July 2003.

We learned from our interviews of its managers that USOU has from time to time discovered and corrected Guidelines violations. These included, for example, an instance where a field division was operating an undercover operation as a Group II UCO, when it clearly should have been classified as a Group I UCO. In another instance, USOU identified a Guidelines violation when it reviewed an undercover operation that was targeting a terrorist group, a subject requiring CUORC approval as a Group I UCO.

After approvals by the pertinent Headquarters' operational managers (Section Chief and Deputy Assistant Director) and the Section Chief of the Operational Support Section (which includes USOU), the application is sent to the CUORC for consideration. A representative from the FBI Headquarters' operational section typically presents the proposed

---

<sup>336</sup> Undercover operations proposed as part of the programs supervised by CID must be approved by its Assistant Director. Undercover operations proposed as part of other programs must be approved by both the Executive Assistant Director of the particular program and the Assistant Director of CID. FGUSO § 4.3 (July 25, 2003).

undercover operation to the CUORC and answers questions posed by the Committee's members. The CUORC members may also consult with U.S. Attorneys, SACs, and other personnel when necessary. When the CUORC approves the proposal, the application is sent to the FBI Director or designated Assistant Director for final approval. Upon final approval, the USOU sends a letter to the field office informing it of the decision. If the CUORC is not satisfied with the proposal or is unwilling to approve it in the form originally submitted, stipulations may be attached to the application that will constrain various aspects of the undercover operation, including stipulations to reduce the risk of harm to persons or property and to minimize the risk of entrapment or other legal defenses in the event of a prosecution. Support personnel from USOU record the stipulations and minutes of all CUORC meetings.

The DOJ CUORC members stated that since the May 2002 revisions, FBI Headquarters is doing a better and more proactive job in answering their questions both before and during the meetings. The DOJ members of the Committee told us they are not aware of any problems with the CUORC's operation and did not suggest any changes to the scope of the Committee's activities or the information provided to members prior to their meetings.

## **2. The CUORC's Activities from October 2003 to March 2005**

We attended 18 CUORC meetings during the period October 2003 to March 2005. We observed that by the time the CUORC met on a particular undercover operation – whether in the context of a new proposal or a proposal to extend, expand, or change the focus or increase the budget of an existing undercover operation – the proposal usually had been well vetted. Members of the CUORC had already reviewed the paperwork and had discussed in advance any major issues concerning the proposal. The presenters from FBI Headquarters typically were very well prepared and knowledgeable about the details of the undercover operation and responded effectively to questions posed by committee members.

We also reviewed the official minutes of CUORC meetings from May 2002 to March 2005. Issues and topics that frequently were discussed at CUORC meetings include:

1. whether appropriate measures were being taken to ensure the safety of confidential informants and cooperating witnesses during undercover operations;
2. whether appropriate steps had been taken to ensure that privileged informants [e.g., lawyers or clergy] used in the undercover operation were cognizant of the nature of the information gathered and would avoid the acquisition of privileged information;

3. whether steps were being taken to reduce the likelihood of third party liability, including the addition of stipulations to operations that involved the purchase of property, the operation of a proprietary business, the targeting of products or substances that are subject to federal regulation for health and safety reasons, or the transfer of property in which members of the public could be affected;
4. whether the procedures used to limit the possibility of violence in connection with an undercover operation were sufficient;
5. whether the elements of the federal crimes being investigated were likely to be established by the undercover operation and encouraging close coordination with the pertinent U.S. Attorney's Office; and
6. ensuring that operations that touch on First Amendment-protected activity were carefully vetted (such as operations involving legislation or other governmental processes).

We also reviewed the CUORC's Annual Reports to the Attorney General and its reports to the Congress since 2002. The Reports reflect the variety of sensitive undercover operation matters the Committee reviewed. Cases reviewed by the CUORC during this period included:

- a white collar crime investigation targeting health care fraud in which the CUORC strongly urged the SAC of the field office investigating the case to consult with the U.S. Attorney to ensure that anticipated criminal charges would merit prosecution. In the same matter, the CUORC was assured that the undercover employees would not be submitting false testimony or affidavits in court proceedings because all claims would be settled prior to that stage in the proceedings;
- a Computer Crime-Intellectual Property Rights Program undercover operation targeting the purchase and sale of "gray" market computers in which the FBI instituted procedures at the suggestion of the CUORC to identify the manufacturer of stolen property. These steps were taken to allay concerns regarding potential third-party liability if the stolen property was passed through the undercover operation to subjects intending to sell the items to the general public (as opposed to being purchased by the undercover operation and held as evidence);
- an Organized Crime undercover operation targeting operations in a large U.S. city in which the FBI addressed the CUORC's concerns about the undercover employee's expected involvement in a conspiracy to violate bribery, gambling, and prostitution laws. The CUORC ultimately concluded that the undercover employee's

participation was necessary to obtain evidence to prosecute more serious crimes, and that the undercover employee had not and would not initiate any criminal activity, but would only monitor the criminal acts of others; and

- a White Collar Crime-Health Care Fraud operation which was modified so that the undercover employee would not have access to confidential patient records and would not interview patients and physicians.

We found in our review of CUORC records that nearly all undercover operations brought to the CUORC were approved, some with modifications. However, the CUORC rejected or tabled several proposals for undercover operations during fiscal years 2002 and 2003. These included a proposed undercover operation targeting illegal gambling that was turned down because of the Committee's concerns about the relationship of a cooperating witness with the FBI, the cooperating witness's intent to solicit others to commit criminal acts, and potential civil liability issues. The Committee also rejected a proposed undercover operation targeting a paramilitary operation due to questions relating to the predication of the subjects, the safety of the operation, potential liability issues, and an inadequate plan for the arrest of the subjects.

### **3. FBI Undercover Coordinator Survey Responses**

We surveyed Undercover Coordinators regarding perceptions of the CUORC.<sup>337</sup> Undercover Coordinators are well positioned to provide insights on the CUORC's effectiveness, at least with respect to the Group I UCOs that it sees. We received survey responses from 54 of the FBI's 56 Undercover Coordinators.

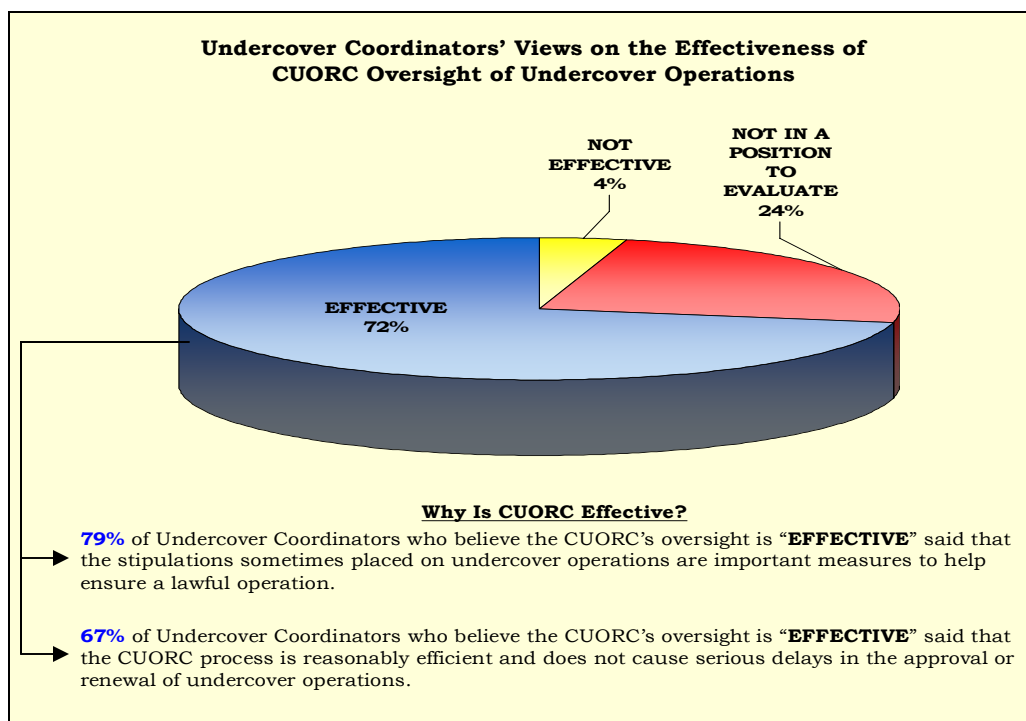
Seventy-two percent of the Undercover Coordinators who responded to our survey said they believe that the CUORC is providing effective oversight of the approval and administration of undercover operations in their field offices.<sup>338</sup> Only two Undercover Coordinators said they did not believe the CUORC provided effective oversight. The reasons Undercover Coordinators cited as to why the CUORC has provided effective oversight, or has not done so, are summarized in Diagram 7.1.

---

<sup>337</sup> As we discuss in Chapter Four, Undercover Coordinators are the FBI Field Divisions' on-site experts concerning undercover matters.

<sup>338</sup> Twenty four percent said they were not in a position to answer the question. As we discuss later in this chapter, by comparison, only 46 percent of Confidential Informant Coordinators said they believe that the FBI-DOJ Confidential Informant Review Committee (CIRC) is providing effective oversight of the Criminal Informant Program.

**DIAGRAM 7.1**



#### **4. OIG Analysis and Recommendations**

We found that during the period of our review, the CUORC played a vital role in reviewing, approving, and monitoring the most sensitive FBI undercover operations. Its members fulfilled their responsibilities both through informal exchanges before undercover proposals were submitted for approval and in formal discussions at the Committee's bi-monthly meetings. Both the FBI and DOJ members of the Committee appeared to work well together, often collegially and by consensus, and we observed a full exchange of information when undercover proposals were presented for initial approval, extensions, budget enhancements, or changes in targeting or scope. When questions were asked about proposed or ongoing operations, FBI personnel provided responses at the CUORC meeting or promptly thereafter.

From our observations of its meetings over an 18-month period, we believe that the CUORC is operating effectively in accordance with its mission to ensure undercover proposals adhere to the Undercover Guidelines, other legal mandates, and internal FBI mandates, and that those supervising the operations from Headquarters and in the field are promptly made aware of the Committee's concerns. It is also clear that the Committee has strong support in the field, as evidenced by the positive observations in response to our surveys of FBI Undercover Coordinators. We believe the CUORC's impact is attributable in part to the critical

supporting role played by the Undercover and Sensitive Operations Unit at FBI Headquarters.

However, we believe that CUORC members would be better informed and provide more effective oversight of undercover operations if they received additional pertinent information. As we discuss later in this chapter, the Inspection Division generates triennial Inspection reports that document the nature and extent of certain Guidelines violations. In addition, USOU conducts periodic on-site reviews of ongoing undercover operations that generate valuable information about the operational and administrative aspects of the operations. We believe the facts and insights contained in these reports concerning undercover operations and in the after-action reports for UCOs approved by the CUORC should be provided to members of the CUORC as they become available.

We also believe the FBI could make more effective use of the extensive experience of the CUORC's members by periodically aggregating the "lessons learned" from CUORC reviews and making them available in training and in USOU's periodic publications.

We therefore recommend that the FBI take the following steps.

(28) Provide CUORC members, upon request, with access to copies of Inspection reports concerning undercover operations, the Undercover and Sensitive Operations Unit on-site reviews, and after-action reports of undercover operations.

(29) Consider ways for the Undercover and Sensitive Operations Unit to develop more complete information for the CUORC and other FBI components, such as conducting a periodic analysis of the patterns and trends found in its on-site reports, informing the CUORC members of any persistent Guidelines violations, and providing copies of its semi-annual report to all FBI Headquarters' operating Divisions, the Office of the General Counsel, and the Training Division.

## **B. Confidential Informant Review Committee (CIRC)**

One of the major changes introduced by the January 2001 revisions of the Confidential Informant Guidelines was the requirement that the FBI and other Department of Justice Law Enforcement Agencies (JLEAs) establish within 30 days a Confidential Informant Review Committee (CIRC).<sup>339</sup> The CIRC was directed to review three major types of confidential informants:

---

<sup>339</sup> CI Guidelines § I.I.2 at B-13. There were no changes to the jurisdiction or membership of the CIRC when the Confidential Informant Guidelines were revised in May 2002. Prior to the January 2001 revisions, DOJ had no role in the initial approval of confidential informants.

- *Long Term Confidential Informants*, defined as those who are registered with the JLEA for more than six consecutive years;
- *High-level Confidential Informants*, defined as those who are part of the “senior partnership of an enterprise that (a) has (i) a national or international sphere of activities, or (ii) high significance to the JLEA’s national objectives, even if the enterprise’s sphere of activities is local or regional; and (b) engages in, or uses others to commit” certain enumerated acts including acts of violence, corrupt conduct, and drug trafficking; and
- *Privileged Confidential Informants*, defined as those who are under the obligation of a legal privilege of confidentiality or are affiliated with the media. Individuals who are under the obligation of a legal privilege of confidentiality include attorneys, licensed physicians, and members of the clergy.

The Confidential Informant Guidelines define the CIRC as “a committee, created for . . . purposes of reviewing certain decisions relating to the registration and utilization of CIs.” The Guidelines specify that the chair of the CIRC should be a person at or above the level of an FBI Deputy Assistant Director. The Guidelines also provide that the CIRC’s membership should include two representatives designated by the Assistant Attorney General in charge of the Criminal Division: a Deputy Assistant Attorney General for the Criminal Division and an Assistant U.S. Attorney.<sup>340</sup>

The FBI Director designated the Deputy Assistant Director for the CID to serve as chair of the Committee. Other FBI members of the CIRC are the Unit Chief and a Supervisory Special Agent in the CID’s Asset/Informant Unit (A/IU) (whose functions were transferred to the Human Intelligence Unit (HIU) as of November 2004), the Chief and Assistant Chief of the CID’s Criminal Intelligence Section, and a representative from the Office of the General Counsel.

The DOJ Criminal Division members of the CIRC are the Principal Deputy Assistant Attorney General, a Senior Litigation Counsel, and the Chief of the Organized Crime & Racketeering Section. In addition, a U.S. Attorney and an Assistant U.S. Attorney serve on the Committee.

The three categories of confidential informants reviewed by the CIRC constitute only a small percentage of informants operated by the FBI. However, under the Guidelines these informants require scrutiny by the CIRC because they present greater risks of potential liability, intrusion into governmental processes, and other adverse consequences.

---

<sup>340</sup> CI Guidelines § I.B.13 at B-11.

## **1. The CIRC Review Process**

The CIRC generally meets monthly. From its inception in 2001 through September 2004, it has approved 391 confidential informants.<sup>341</sup> Of this total, 333 were long term confidential informants; 48 were confidential informants under the obligation of a legal privilege of confidentiality; 3 were confidential informants affiliated with the news media; and 7 were high-level confidential informants.

As soon as the CIRC was established, its charge to review all “long term” confidential informants created an immediate backlog. To deal with the backlog, beginning in 2003 the CIRC reviewed approximately 40 informants per meeting. Once the CIRC completed its review of the backlogged long term confidential informants, it reviewed an average of 10 – 20 informants per meeting.

To evaluate whether to approve or disapprove a long term, high-level, privileged, or media-affiliated confidential informant, the CIRC uses a 6-page form called Initial (or Continuing) Confidential Informant Suitability Report and Recommendation (SR&R).<sup>342</sup> Pursuant to Section II.A.1 of the Confidential Informant Guidelines, the field office or Headquarters’ Division proposing use of such a confidential informant completes the Initial Suitability Report & Recommendation (ISR&R) form.<sup>343</sup> If the CIRC authorizes use of the informant, the office or division handling the informant must complete a Continuing Suitability Report & Recommendation (CSR&R) form, usually annually or when changed circumstances warrant.<sup>344</sup> By the time the CSR&R gets to the CIRC, the information contained in it has already been evaluated and approved by FBI field office management. The CIRC then reviews the information contained in the suitability reports to decide whether, and under what conditions, the person should be utilized as a confidential informant.

---

<sup>341</sup> FBI Asset/Informant Unit Statistics (Sept. 28, 2004).

<sup>342</sup> Suitability Reports and Recommendations are also used for field office approval of lower-level confidential informants who are not required to be approved by the CIRC. We discuss in Chapter Three our findings regarding the FBI’s compliance with the key provisions of the Confidential Informant Guidelines.

<sup>343</sup> The Guidelines require the confidential informant’s contact agent to address in the ISR&R such factors as the person’s reliability and truthfulness; the investigative relevance of the information to be provided; the person’s motivation for providing information; and complete information on the person’s age, alien status, and criminal history, if any. A complete list of the suitability factors is provided in Chapter Three.

<sup>344</sup> CI Guidelines, § II.A.2 at B-15. As we discuss in Chapter Three, in the 12 FBI field offices we visited during this review, we found that 59 percent of the confidential informant files did not contain one or more of the required CSR&Rs.



If the source has been opened as a confidential informant for over a year, the case agent must complete and sign a CSR&R. In addition to the factors addressed in the ISR&R, the report must specify the length of time the person has been registered as a confidential informant and the length of time the person has been handled by the same agent or agents.<sup>345</sup>

Approximately two weeks prior to each scheduled CIRC meeting, the A/IU sends a binder to each CIRC member. The binder includes the suitability report and a 6-page analysis of the confidential informant's suitability based on the sponsoring field office's responses to 26 questions asked by the A/IU.<sup>346</sup> We found a considerable amount of communication about the proposed confidential informants prior to the CIRC meeting. Both the A/IU and DOJ members of the CIRC sometimes raise questions about the proposed informant based on information contained in the suitability reports. The Committee members' questions are forwarded by A/IU to the originating field office, and the answers are discussed at the CIRC meeting. After the Committee makes a decision, the A/IU sends a communication to the field advising the sponsoring agents that the requested action was approved, disapproved, or in some instances tabled until the next CIRC meeting because more information was needed about the proposed or already-registered informant.

## **2. The CIRC's Activities from August 2003 to April 2005**

We attended 12 CIRC meetings from August 2003 to April 2005. Our review found that members of the CIRC invest a considerable amount of time and effort evaluating the benefits and risks of each confidential informant. The questions asked by the FBI and DOJ members addressed virtually all the factors in the Initial and Continuing Suitability Reports and Recommendations form. Some of the most frequently asked questions are below.

1. How is the person in a position to obtain relevant information (Factors 4 and 9)?
2. Have there been allegations that the person was engaged in any act of violence or crimes (Factor 13)?
3. What type of crimes has the person committed and when (Factor 12)?

---

<sup>345</sup> CI Guidelines § II.A.2.a at B-15.

<sup>346</sup> In October 2004, A/IU modified the suitability report to include two additional questions frequently posed by CIRC members regarding the relevance of the person's information and how the person is in a position to obtain relevant information.

4. How can a confidential informant associated with organized crime for the past 20 to 30 years not be involved with any illegal activity (Factor 12)?
5. Has the information the person provided led to indictments or convictions (Factor 5)?
6. What special reporting or control measures can be employed to minimize the risk of violent or serious crimes committed (Factor 16)?
7. What is the specific nature of the person's assistance to the FBI (Factor 6)?

As described below, the CIRC members also frequently inquired about informants' participation in otherwise illegal activity, the length of time agents have handled informants, and other topics relevant to the Guidelines. During our attendance at CIRC meetings, we observed that the DOJ CIRC members were very active in posing questions on a variety of topics.

### **Otherwise Illegal Activity**

An important issue the CIRC members address in preparation for and during meetings is the subject of "otherwise illegal activity" (OIA). As we discussed in Chapter Three, authorization for OIA permits registered confidential informants to commit acts which would otherwise be considered prosecutable crimes.<sup>347</sup> Authorization for OIA is broken down into two categories. *Tier 1 OIA* entails the most serious criminal activity, defined as any activity that 1) would constitute a misdemeanor or felony under federal, state, or local law if engaged by a person acting without authorization; and 2) involves the commission, or the significant risk of the commission, of certain specified conduct, including acts of violence or public corruption. *Tier 2 OIA* is any other activity that would constitute a misdemeanor or felony under federal, state, or local law if engaged in by a person acting without authorization.

---

<sup>347</sup> Under the Confidential Informant Guidelines, authority to engage in OIA is closely supervised by FBI field office and FBI Headquarters managers and U.S. Attorneys' Offices, in addition to the oversight provided by the CIRC for certain defined categories of confidential informants. Confidential informants who operate outside the limits imposed on their OIA are subject to prosecution.

Otherwise illegal activity is distinguished from *unauthorized* illegal activity. The Guidelines impose special notice requirements on FBI personnel who have reason to believe that confidential informants have engaged in unauthorized illegal activity. See CI Guidelines § IV.B at B-31.

During the meetings we attended, the CIRC members often asked for additional information pertaining to the confidential informant's involvement in OIA. Their requests on this topic included inquiries about the period of authorization for OIA, the specific nature of the authorized illegal activities, and whether Tier 1 OIA was authorized by the U.S. Attorney.<sup>348</sup> They also requested information necessary to distinguish Tier 1 from Tier 2 OIA and resolve apparent inconsistencies in an SR&R as to the informant's authorization to engage in otherwise illegal activity.

### **Informant Handled by the Same Case Agent for Extensive Period**

The CIRC closely examines long term informants because this category of informants historically has generated problems during investigations and prosecutions. During some CIRC meetings we attended, questions focused on whether it was prudent to have the same FBI agent handle an informant for five years or more. At the suggestion of a DOJ CIRC member, the CIRC ultimately required the SACs in such cases to provide a written finding that in his or her judgment the agent should continue to handle the informant.

### **Other Questions Raised at CIRC Meetings**

During meetings we observed, CIRC members also raised questions not specifically addressed in the suitability reports but which are nonetheless directly related to the Guidelines. Some of the common questions are below.

- How much has the person been paid?
- What is the person's legitimate source of income?
- When the person testified, was the Assistant U.S. Attorney notified of the person's status as a confidential informant?
- In cases where the confidential informant had recently been arrested, how did the field office reach its conclusion that the arrest does not adversely affect the confidential informant's suitability? Did any law enforcement official intercede on the confidential informant's behalf following the arrest?

In addition to observing meetings of the CIRC, we interviewed 10 current or former members of the CIRC. All of the CIRC members we interviewed said that the scope, quality, and tenor of interaction within the Committee has evolved since its inception. According to the CIRC members we interviewed, in the first year of the CIRC the relationship between the FBI employees and DOJ members was contentious. The DOJ Committee

---

<sup>348</sup> Only Tier 1 OIA must be approved by the U.S. Attorney.

members we interviewed attributed the early difficulties to three factors: a general wariness within the FBI about sharing highly sensitive information regarding confidential informants with non-FBI personnel; a belief that the January 2001 Attorney General Guidelines were an overreaction to the Bulger-Flemmi informant episode and other instances of errant informants; and, to some degree, the personalities of several of the initial CIRC members from both the FBI and DOJ. By all accounts, the level of confidence and interaction between A/IU and FBI field offices, on the one hand, and between the FBI and the DOJ members of the CIRC, on the other, has steadily improved since that first year.

All of the FBI and DOJ members of the CIRC we interviewed said they believe that while field office supervisors are the critical personnel to enforce the Confidential Informant Guidelines, the CIRC serves as an important mechanism to promote adherence to the Guidelines. They also told us that the vast majority of the proposals presented to the Committee do not provoke special concerns or questions.

Several DOJ members of the CIRC, however, voiced two major concerns. First, they said that although the information flow has improved since the CIRC began in 2001, the suitability reports provided in advance to the Committee members are still inadequate. For example, these members said that the standard question on the suitability report, “Is there any negative information about the CI?” has not produced a single affirmative response, even in circumstances where confidential informants have been arrested. The DOJ committee members also said they have repeatedly asked for the suitability evaluation that is required upon the occurrence of unauthorized illegal activity, such as an arrest or illegal activity unrelated to the investigation, yet they have received only oral responses instead of hard copies of the required evaluations.<sup>349</sup> They also said that responses to other routine questions on the suitability reports tend to be unhelpful, rote answers that are used in every suitability form and are not tailored to the particular informant.

Second, these DOJ members said that the FBI CIRC members and particularly the A/IU have been increasingly responsive and cooperative in answering questions that arise during CIRC meetings. They stated,

---

<sup>349</sup> CIRC members also told us that when the CIRC was formed, DOJ members did not always have clear and concise copies of the informants’ criminal history checks when reviewing their SR&Rs. As a result, questions arose about the dates an informant committed crimes, the types of crimes, and the disposition of the charges. CIRC members said that in the last year, the FBI has distributed copies of the informants’ criminal records in advance of CIRC meetings. CIRC members told us that this advance distribution has improved the situation but that some DOJ members of the Committee – all of whom are experienced prosecutors – sometimes have difficulty deciphering the federal or state or local law enforcement codes used to detail the informants’ criminal histories.

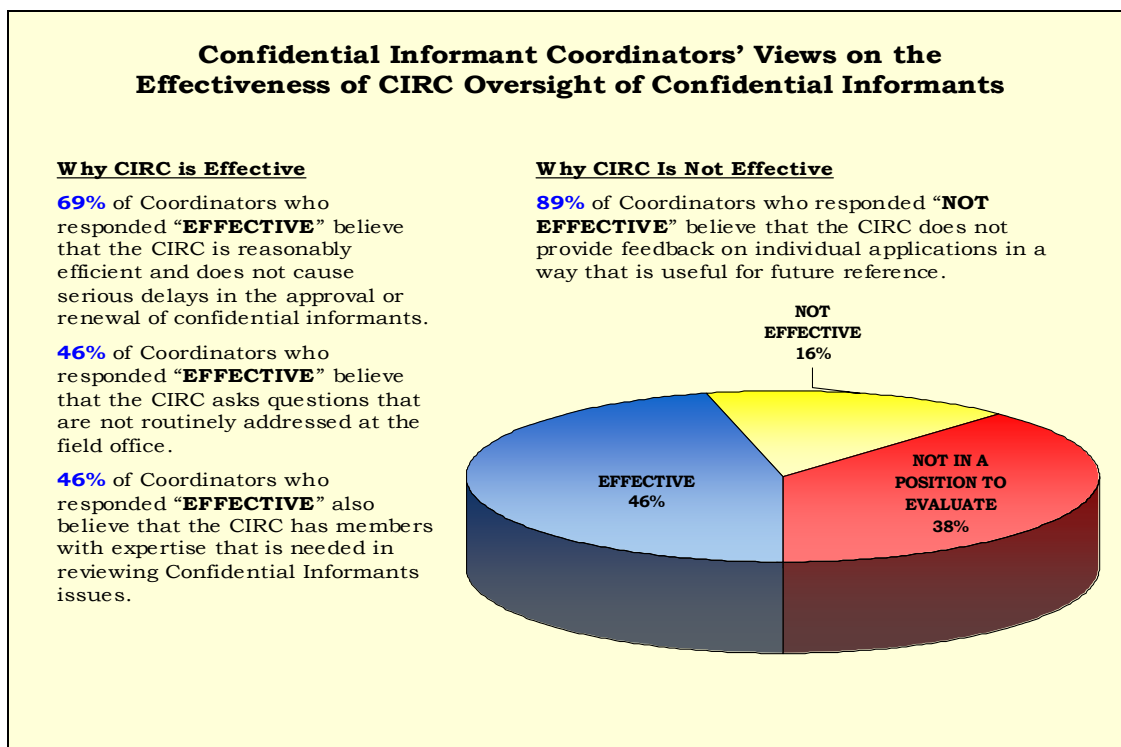
however, that the need to ask the same types of routine but important questions about confidential informants at each meeting, such as those highlighted above concerning suitability, has slowed the process down. They commented that spending time on routine questions has prevented the committee members from focusing on more subtle and complex but potentially more important issues at its monthly meetings.

### 3. **OIG Survey of Confidential Informant Coordinators Regarding the CIRC**

As part of this review, we conducted a survey of Confidential Informant Coordinators in the FBI's 56 field offices. The survey asked a wide range of questions concerning training on the Attorney General Guidelines, evaluation of internal controls, recordkeeping and information technology issues, frequently asked questions regarding the Guidelines, impediments to compliance with the Guidelines, measures to promote compliance with the Guidelines, and special issues arising under the Guidelines. We obtained a 100 percent response rate to the survey.

Several survey questions focused specifically on the operation of the CIRC. Informant Coordinators told us that 86 percent of FBI field offices have sought CIRC authority for long term confidential informants, and 52 percent have sought CIRC approval for high-level, privileged, or media-affiliated confidential informants. The key survey findings regarding the CIRC are illustrated in the following diagram.

**DIAGRAM 7.2**



As Diagram 7.2 depicts, almost half of the Informant Coordinators responded that they believe the CIRC has provided effective oversight over the administration of confidential informants in their field office.<sup>350</sup> Sixteen percent of the respondents said they do not believe the CIRC provides effective oversight, while 38 percent said they were not in a position to evaluate the CIRC's effectiveness because either they had had little or no contact with the CIRC or had not served as Informant Coordinator long enough to make a judgment.

Of the survey respondents who said they believe the CIRC's oversight is effective, 69 percent said they believe the CIRC process is reasonably efficient and does not cause serious delays in the approval or renewal of confidential informants. In addition, 46 percent said they believe the CIRC members have expertise that is needed in reviewing confidential informant issues, and that CIRC members ask questions that are not routinely addressed at the field office.

Our survey also found that the most frequently asked questions of Informant Coordinators (or the agents they work with) by CIRC members include questions regarding the informant's suitability (57 percent), how the proposed CI will be in a position to provide relevant information (66 percent), and questions pertaining to notification or approval issues involving the USAOs (20 percent).

Of the 16 percent of the survey respondents who said they believe the CIRC does not provide effective oversight of the Criminal Informant Program, 89 percent said that the CIRC does not provide feedback on individual applications in a way that is useful for future applications to the CIRC. Seventy-eight percent of these respondents commented that the questions raised by the CIRC were routinely addressed in the field and that the CIRC process is too slow and cumbersome.

### **C.     OIG Analysis and Recommendations**

Based on our review, we believe that although there has been some reluctance within the FBI to share information about its informants with anyone outside the FBI, the persistence of CIRC members, backed by support from senior management of the FBI and the DOJ, and effective supervisory personnel in A/IU, has made the CIRC a vital tool for promoting adherence to the Confidential Informant Guidelines. Over the last four years, the CIRC has provided meaningful oversight of many of the confidential informants who present the greatest risks and potential

---

<sup>350</sup> The 46 percent effective assessment for the CIRC compares to the Undercover Coordinators' 79 percent effective assessment of the CUORC, discussed earlier in this chapter.

rewards for the FBI's top priorities, including counterterrorism, national and transnational criminal enterprises, public corruption, health care and other types of fraud, and white collar crime.

However, we believe the effectiveness of the CIRC can be improved. As described above, some CIRC members expressed concerns regarding missing or incomplete information in the suitability reports, ranging from rote and unhelpful answers on some suitability forms to the failure to provide continuing suitability reports when an informant commits unauthorized illegal activities. These members stated that the need to pursue answers before or during CIRC meetings to questions that the proposing agents should already have provided slows down the functioning of the committee and prevents it from focusing on potentially more important issues. Similarly, our survey revealed that Informant Coordinators who are unsatisfied with the CIRC have criticized the process as being too slow.

In addition, the principal complaint of Informant Coordinators who stated the CIRC is ineffective was that the CIRC does not provide feedback on individual applications in a way that is useful for future reference. We believe this is a valid observation. We found that the questions asked at CIRC meetings fall into familiar patterns based on the experience of the members in spotting circumstances that have proven over the years to be predictors of confidential informant problems. However, the insights from the CIRC's decisions are neither memorialized nor communicated to field personnel at FBI Headquarters or the DOJ.

The purpose of the following recommendations is two-fold: 1) to make critical information about the confidential informants reviewed by the CIRC available to all members prior to their meetings, thereby reducing the need for time-consuming interaction between the field and the CIRC's members; and 2) to use the lessons learned from the CIRC to educate field personnel on a regular basis and to provide more focus to the training of case agents and supervisors about the Criminal Informant Program.<sup>351</sup>

We therefore recommend that the FBI take the following steps.

(30) To assist CIRC members in evaluating the confidential informants within its purview and assist field and Headquarters managers in their supervisory responsibilities in overseeing the Criminal Informant Program, require that the Initial and Continuing Suitability Reports and

---

<sup>351</sup> Effective November 15, 2004, the FBI Director moved the function of the Asset/Informant Unit in CID to the new Intelligence Directorate. We believe our recommendations are important no matter where the FBI Headquarters function for supervising confidential informants is located.

Recommendations contain more thorough answers to the suitability questions, such as:

- a description of the confidential informants' legitimate source of income;
- the confidential informants' statistical accomplishments, including the number of indictments, convictions, Title III wiretap applications, and other indicia of informants' contributions;
- details on how confidential informants are in a position to obtain relevant information;
- details on the nature of any unauthorized illegal activity committed by confidential informants, including informants' criminal history records and the continuing suitability reports required to be completed in accordance with Section II.A.2.b of the Confidential Informant Guidelines; and
- the informant records of any confidential informants who have been previously deactivated for cause by the FBI, including the reasons for deactivation and the field division operating the informants.

(31) Consider having the Human Intelligence Unit draft "lessons learned" from the CIRC's decisions, periodically communicate these lessons to field personnel, and incorporate them into training on the Confidential Informant Guidelines.

(32) Make available to CIRC members, upon request, copies of the Inspection Division's audits of the Criminal Informant Program (including any reinspection reports) and evaluations performed by the Human Intelligence Unit of compliance with the Confidential Informant Guidelines.

## **II. Inspection Division**

Of all the oversight and enforcement mechanisms employed by the FBI, the Inspection Division has the broadest mandate to investigate and evaluate Attorney General Guidelines compliance issues. According to the Inspection Division's 2004 Program Plan, "[the Inspection Division] has a vital role within the FBI providing the Director independent and thorough performance assessments of all aspects of FBI operations and ensuring that performance deficiencies are resolved in a timely manner."<sup>352</sup> Our review, including an interview with the Director, confirmed the significance of the Inspection Division's work to the FBI's compliance with the Attorney General Guidelines.

---

<sup>352</sup> Inspection Division Program Plan (2004) at 1.



In this Section of the Report we examine: 1) the functions of the Inspection Division, including its mission, organization, and inspection procedures; 2) what Guidelines' provisions the Inspection Division examines and how this has changed since May 2002; 3) Inspection Division findings regarding the Guidelines' compliance; and 4) the OIG's analysis and recommendations regarding the inspection process.

To conduct our review, we examined numerous Inspection Division documents, including inspection reports and supporting electronic communications for 41 FBI field offices from May 2002 to October 2004. We also interviewed Inspection Division personnel and senior FBI executives about the work of the Division and inspection procedures.

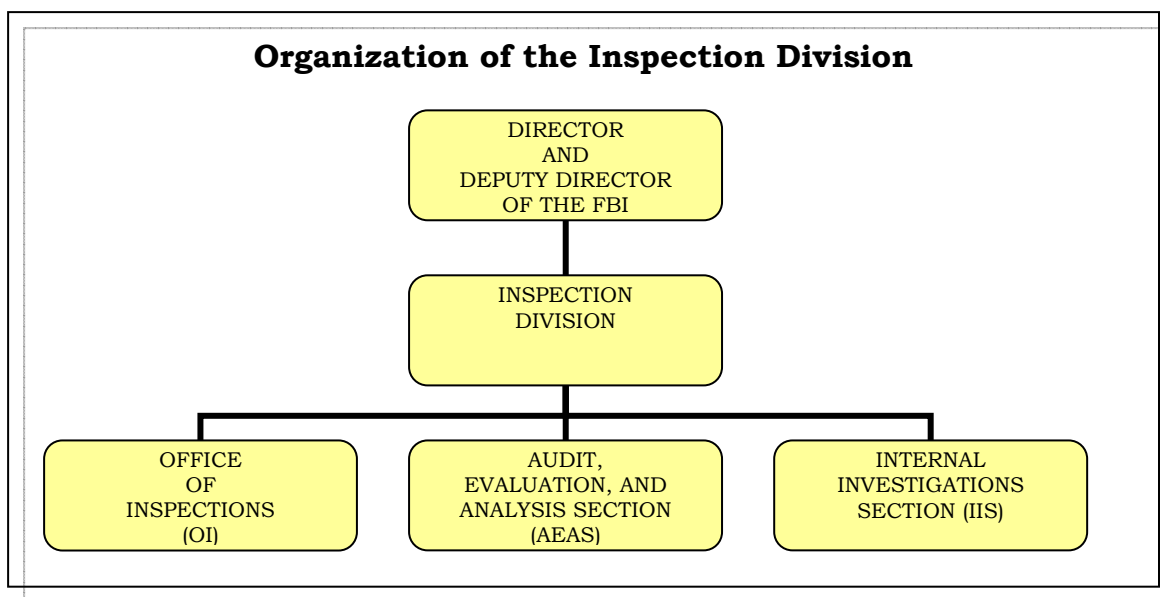
### **A. Background on the Inspection Function**

Below we describe the organization of the Inspection Division, how inspections are performed, and the issues addressed during inspections, including those concerning the Attorney General Guidelines.

#### **1. Organization of the Inspection Division**

The Inspection Division divides its work among three main components: the Office of Inspections; the Audit, Evaluation, and Analysis Section; and the Internal Investigations Section. The Inspection Division reports directly to the Director and Deputy Director of the FBI and is not located within the Bureau's five directorates. The organizational chart below identifies the structure of the Inspection Division.

**DIAGRAM 7.3**



The Office of Inspections, which is the principal focus of this section of the report, is managed by a Chief Inspector and includes an inspection staff comprised of various inspectors, Inspectors-in-Place, Team Leaders, and Assistant Inspectors-in-Place. It has two units: the Inspection Management Unit and the Audit Unit.<sup>353</sup> As of November 2004, the Office of Inspections had 8 Inspectors, 8 Assistant Inspectors, 12 Team Leaders, and approximately 80 Inspectors in Place and 300 Assistant Inspectors in Place, to perform its inspections.<sup>354</sup> The Inspection Management Unit provides logistical assistance, pre-inspection analysis, and post-inspection compliance monitoring. The Audit Unit conducts financial and Information Systems audits.

## **2. How Inspections Are Conducted**

The Inspection Division performs two kinds of evaluations: performance audits and on-site inspections.<sup>355</sup> Performance audits evaluate particular programs across the FBI using audit standards such as the *Government Accountability Office's Government Auditing Standards, 2003 Revision*, and the Office of Management and Budget's *Performance Assessment Rating Tool (PART)*. Inspections are conducted by the Office of Inspections at field offices, Headquarters, and Legal Attaché offices (Legats) on a rotating basis every three years. These inspections evaluate compliance with rules, regulations, policies, and procedures, as well as operational performance. In addition, in conjunction with FBI operational divisions, the Inspection Division has developed program reviews for use by field offices. Field offices conduct program reviews to examine whether field office goals and objectives are consistent with the FBI's national strategy and evaluate how well field offices are implementing the FBI's strategic plan. The results of these reviews are analyzed by program managers at FBI Headquarters.<sup>356</sup>

---

<sup>353</sup> Inspectors in Place and Assistant Inspectors in Place are FBI Agents stationed outside the Inspection Division. Inspectors in Place typically are ASACs, who are assigned to field offices, or Section Chiefs, who are assigned to FBI Headquarters. Assistant Inspectors in Place have either served a minimum of two years as a field supervisor or one year as a field supervisor with at least two years prior service at FBI Headquarters.

<sup>354</sup> Inspections work is important to career advancement in the FBI. To become an Assistant Special Agent in Charge (ASAC), an agent must obtain inspection certification. This requires the agent to participate in at least five inspections and one OPR investigation.

<sup>355</sup> FBI Strategic Plan (2004-2009), App. C at 129, available at: [www.fbi.gov](http://www.fbi.gov) at Reports and Publications.

<sup>356</sup> Program managers administer "substantive" offices (divisions, sections, units) at FBI Headquarters in areas such as cyber, criminal, and counterterrorism.

### **a. The Inspection Process**

The Office of Inspections inspects each FBI field office, Headquarters Division, and Legat Office once every three years. These inspections have three distinct phases: pre-inspection, on-site inspection, and post-inspection.

During the pre-inspection phase, personnel from the Office of Inspections collect data and information about the office to be inspected in preparation for on-site activity. Approximately 120 days prior to the on-site visit, the field office receives interrogatories requesting information on compliance, performance, and related administrative issues. Identification of Guidelines compliance deficiencies is requested in a limited number of program interrogatories, but is not requested in squad interrogatories. The Office of Inspections also solicits information from Headquarters Divisions and other FBI entities that have had contact with the office. After this information is collected, a pre-inspection analysis is prepared that summarizes statistical accomplishments, management data, program strengths and weaknesses, and prior inspections findings, including how those findings were resolved.

The on-site inspection typically is conducted over a period of up to three weeks by a team of Inspectors, Inspectors in Place, and their assistants working under the supervision of an SES-level Inspector in Charge. For example, a recent inspection of the Miami Division involved approximately 75 FBI personnel. While on-site, the inspection team examines hundreds of paper files. Routing slips may be sent to agents requesting an explanation of any deficiencies identified in the files. More than 25 separate FBI programs are subject to “compliance audits” during inspections. These include the Criminal Informant Program, undercover operations, electronic surveillance activities, training matters, and the functioning of executive management.<sup>357</sup> See Table 7.2. The Inspection Division has prepared detailed checklists for each type of audit to ensure consistency in the information that is collected in each office. In addition, the inspection team interviews FBI employees in the field office and representatives of agencies and organizations with which the office interacts, including other law enforcement agencies and the U.S. Attorney’s Office.

At the conclusion of the on-site inspection, the inspection team prepares a draft written report for review by the field office. In circumstances where 1) detailed data and information must be conveyed to

---

<sup>357</sup> According to the Inspections Guidebook, an important component of Inspection Division audits is to determine whether the inspected “entity has complied with significant laws and regulations applicable to the program.” Inspections Guidebook at 20 (2000).

support proposed corrective actions or 2) the findings in question must be disseminated to entities other than the office inspected, the inspection staff prepares a separate electronic communication or memorandum in addition to the findings contained in the written report. The draft report and electronic communication are then discussed at a closing conference held on the last day of the inspection with members of the inspection team and personnel from the field office.

Inspection reports typically contain six substantive sections and two appendices that are presented in the following order: 1) an inspection summary; 2) background information about the office, its staff, and events that affected the office during the inspection period; 3) an evaluation of the performance of executive management; 4) a summary of the various compliance audits conducted; 5) a summary of the performance appraisals for the various investigative programs, squads, and other units evaluated; 6) an analysis of investigative support services; 7) an appendix of the inspection's findings; and 8) an abbreviation appendix. With respect to the third and fifth sections, the report will specify whether the entity inspected was "effective" and "efficient."<sup>358</sup> Any deficiencies noted are followed by recommendations or instructions designed to eliminate the identified compliance deficiencies.

Within 30 days from the close of the on-site inspection, the field office must furnish responses to the Office of Inspections for each finding, instruction, and recommendation contained in the draft report. The Office of Inspections finalizes the report during this period and distributes a summary to senior FBI management, including the Director, who reviews the inspection results with the senior executive manager of the office or division.

After the inspected field office provides its written response to the inspection report, the Office of Inspections evaluates the submission and determines whether appropriate action has been taken to remedy the deficiencies identified in the report. The Inspection Management Unit is responsible for ensuring that the office complies with each instruction contained in the report. When a field office fails to respond adequately to a finding and instruction, the Inspection Management Unit prepares an electronic communication requesting additional information or action. The Office of Inspections considers findings resolved when the office has reported actions necessitated by the findings, which often occurs in the

---

<sup>358</sup> According to the Inspections Guidebook, "effective" means "adequate to accomplish an intended purpose; producing the intended or expected result." "Efficient" means "performing or functioning in the best possible and least wasteful manner; having and using requisite, [sic] knowledge, skill, and industry; competent; capable." Inspections Guidebook at 44-45 (2000).

office's written response to the inspection report. When all findings have been resolved, usually within a few months from completion of the inspection, the Inspection Management Unit notifies the office by electronic communication. The Inspection Management Unit does not attempt to monitor implementation of remedies between on-site inspections. Recurring deficiencies identified in a subsequent inspection may lead to a finding directed to executive management in the office.

In addition to the planned triennial inspections described above, the Office of Inspections has supervised field office "self-inspections" as well as "reinspections," both of which may examine Guidelines compliance issues. During a self-inspection, the Office of Inspections furnishes audit forms that are completed by the field office and then returned for examination by analysts in the Inspection Management Unit. The self-inspection allows the field office to identify and correct problems prior to its triennial inspection. If a self-inspection is completed for a particular audit (e.g., an audit of the Victim Witness Assistance Program), the Office of Inspections staff determines during the triennial on-site inspection if the audit was properly conducted. Prior to June 2004, self-inspections typically occurred at the midpoint of an office's regularly scheduled inspection cycle. Inspection Division management stated, however, that it has halted this practice and that future self-inspections likely will be conducted nationwide by program, not at the midpoint of an office's inspection cycle.

In rare circumstances, the Inspection Division also has participated in "reinspections" of particular field offices or programs if the results of the regular inspection are unsatisfactory or if an event indicates that prompt intervention is necessary. According to the FBI's former Chief Inspector, Robert Grant, a program that receives anything less than an "Effective and Efficient" rating is at risk of being reinspected. The decision to conduct a reinspection is made by the Assistant Director of the Inspection Division in consultation with the Deputy Director and Director of the FBI. Depending on the nature of the deficiency, the reinspection may be conducted with a Headquarters program office working in conjunction with the Inspection Division.

**b. The Inspection Division's Efforts to Improve Inspection Procedures Through Technology and Reengineering Initiatives**

Our interviews with Inspection Division management and review of inspection files revealed that the Division is seeking to upgrade its use of technology and to reengineer many of its current procedures. As explained to the OIG, these initiatives are being undertaken to address weaknesses that hinder the Division's ability to provide timely and comprehensive compliance and performance information to FBI management, including Guidelines compliance issues.

Our review found that the Inspection Division's use of information technology tools currently is quite limited. Much of the data collection, analysis, and reporting performed by the Office of Inspections is not collected or recorded electronically. For example, we learned during our review that when offices responded to inspection reports, the Office of Inspections collected the paper copy of the response to each finding, collated them with a paper copy of the inspection finding, and retained the information in a cardboard file. According to one former senior Inspection Division official, the Division is "nowhere near where we should be or need to be to make [the inspection process] efficient."

The Inspection Division has identified the following problems resulting from the inadequate state of its technology:

- delays in incorporating new performance measures and policies into the FBI's information systems;
- long delays in the detection of deficiencies as a result of the inspection cycle;
- an inadequate process to evaluate the appropriate operation and management of quality human sources; and
- an inadequate system to identify individual component and nationwide compliance deficiencies between on-site inspections.<sup>359</sup>

### **3. What is Inspected**

The Inspection Division's decisions concerning the extent of its compliance data gathering occur primarily in two ways: 1) by identifying the programs and initiatives that are subject to compliance audits; and 2) by specifying the particular kinds of information that will be collected during the audits.

The Inspection Division's Inspections Guidebook (2000) identifies the various audits that are conducted during on-site inspections. These are set forth in the table below.

---

<sup>359</sup> Inspection Division Program Plan (2004) at 2.

**TABLE 7.2**

**Audits Conducted During Inspection Division  
On-Site Inspections**

Alias/False Identification (AFID)	Intelligence Oversight Board (IOB)
Assets	Merit, Promotion & Placement Plan (MPPP)
Automotive Fleet Management (AA)	National Crime Information Center (NCIC)
Community Outreach Program (COP)	Program Administration and Agent
Criminal Informant Program (CIP)	Complement (PA/A)
Communications Security (COMSEC)	Public Affairs and Media (PM)
Drug Deterrence Program (DDP)	Radio Maintenance (RM)
Electronic Surveillance (ELSUR)	Security Program
Employee Assistance Program (EAP)	Management (SPM)
Equal Employment Opportunity (EEO)	Support Services Section (SSS)
Ethics Program (EPA)	Technically Trained Agents (TTA)
Evaluation of Internal Controls (EC-B)	Training Matters (TM)
Evidence Program (EVP)	Undercover Operations (UCO)
Executive Management (EM)	Utilization of Aircraft (UA)
Financial Management (FM)	Victim Witness Assistance
Foreign Intelligence/Counterintelligence Audit FICA)	Program (VWAP)
Foreign Language Program (FL)	

The types of audits that the Office of Inspections performs change over time. Over the last four years, the Division has added three audits to the list above (Computer Analysis Response Team Field Examiner Program, Information Systems, and Foreign Intelligence/Counterintelligence) and dropped one audit (Foreign Intelligence/Counterintelligence). In addition, the emphasis that the Inspection Division places on particular audits varies over time. For example, according to a former Chief Inspector, the importance of the Security Program audit increased dramatically after the espionage activities of former FBI agent Robert Hanssen were discovered.

With respect to administrative compliance measures, Inspection Division management stated that the electronic surveillance, evidence, and Criminal Informant Programs currently are the most pressing priorities. We were told by a former Chief Inspector that the rationale for this emphasis is that these programs directly affect investigations and the testimony of FBI agents, and affect the reputation of the FBI with the U.S. Attorneys' Offices, the courts, and other law enforcement agencies.

Of the audits identified in Table 7.2, four are pertinent to the Attorney General Guidelines: Criminal Informant Program, Electronic Surveillance, Undercover Operations, and Executive Management. The Inspections Guidebook also identifies procedures to evaluate the performance of investigative programs and squad/resident agencies, both of which are subject to requirements found in the Guidelines. Of the four Investigative Guidelines, we did not find comparable audit coverage of the core activities and authorities authorized pursuant to the General Crimes Guidelines. For example, we did not identify any audits that attempt to gauge the FBI's compliance with the new or expanded authorities of the General Crimes

Guidelines that implicate civil rights and civil liberties concerns, such as how authorities to “surf” the Internet or visit public places and events were utilized, or how information gleaned from those activities is retained or disseminated.<sup>360</sup>

In addition to selecting the kinds of audits it conducts, the Inspection Division defines the scope of its information gathering by identifying the particular data that is collected during audits. The Inspection Division has developed detailed checklists that inspection personnel use during audits to collect compliance data.<sup>361</sup> These are updated by Inspection Management Unit personnel, who consult formally at least annually with FBI divisions concerning revisions. Each division in the FBI is assigned an Inspection Management Unit analyst to monitor policy changes.

Despite this work, our review of the checklists and worksheets that relate to the Guidelines revealed that most are not comprehensive on Guidelines issues.<sup>362</sup> For example, the checklists for investigative programs and squads/Resident Agencies contain little or no compliance information.<sup>363</sup> Although the checklist for informants employed by the FBI during the period of our review (generally May 2002 to May 2004) states that its purpose is “to determine if an informant has been operated in compliance with current policy and instructions.” it does not contain various items that are important to making such a determination, such as the following items required by the Confidential Informant Guidelines:

---

<sup>360</sup> See General Crimes Guidelines § VI at B-83.

<sup>361</sup> The Inspection Division uses interrogatories and worksheets to collect information concerning investigative programs and squads/Resident Agencies.

<sup>362</sup> The exceptions to this finding are the checklists for undercover operations and electronic surveillance. We note, however, the checklist for undercover operations does not address whether the undercover operation complies with all applicable CUORC stipulations. We recommend that the Inspection Division consider adding this question to its undercover operation checklist. We also suggest that the Inspection Division include in its undercover operation checklist language comparable to the following from the Undercover and Sensitive Operation Unit’s undercover operation checklist: “The Group II UCO does not fall into **any** of the sensitive circumstances, requiring FBIHQ approval, as delineated in Paragraphs A and B of the Attorney General Guidelines on FBI undercover operations. [AGG Section IV, Paragraph C] **By my signature, this confirms that no sensitive circumstances exist in this UCO.** \_\_\_\_\_ [Signature of USOU Representative]” (emphasis in original).

<sup>363</sup> For example, although each checklist includes sections on “Program Management,” the squad/RA checklist only seeks compliance information concerning the supervisory file review required by the MIOG. As we noted in Chapter Three, FBI Headquarters and field officials we interviewed stated that first-line supervisors are uniquely positioned to ensure adherence to the Guidelines. Notwithstanding that widespread view, the Inspection Division squad/RA checklists do not currently capture compliance performance data regarding any of the Attorney General Guidelines.



- whether the continuing suitability report and recommendation was completed by the Special Agent;
- whether indices checks were performed as required;
- whether Tier 2 Otherwise Illegal Activity was properly characterized;<sup>364</sup>
- whether proper informant deactivation procedures were followed; and
- whether authorization was obtained for ongoing contacts with informants deactivated for cause.<sup>365</sup>

In addition, our review of the inspection data collection materials revealed that they do not consistently seek information concerning the causes of the deficiencies that are found during the inspections. For example, the Criminal Informant Program checklist states that: “‘No’ answers [entered on the checklist] usually indicate non-compliance and may require further inquiry.” In contrast, the undercover operation checklist provides: “‘No’ answers indicate non-compliance and require an explanation.” Our review of the completed checklists that were used in the field offices with the worst Criminal Informant Program compliance records, for example, showed that inspectors rarely entered information setting forth the field office’s explanation for the deficiencies. Instead, notations typically were made that allowed the inspector to verify the fact of the non-compliance. In some cases, inspectors sent routing slips to agents and others requesting confirmation of the deficiencies identified in the case files. While these generated important information concerning the circumstances surrounding the violation, the questions posed by the inspectors typically were not formulated to solicit information regarding the cause of the deficiency. Director Mueller stated during our interview of him that he believes the Inspection Division should collect information on the causes of identified deficiencies.

---

<sup>364</sup> For example, the Confidential Informant Guidelines include “the commission, or the significant risk of the commission, of any act of violence by a person or persons other than the Confidential Informant” in the definition of Tier I activity. CI Guidelines § I.B.10 at B-9. Our review failed to ascertain any consistent standard by which the FBI was applying this definition, and the Criminal Informant Program checklist does not address this risk assessment.

<sup>365</sup> The Criminal Informant Program checklist was revised in August 2004 to address several issues identified by the OIG, although it was not employed consistently during the remainder of 2004. We found that while the updated checklist was used in an inspection of the Baltimore Field Office in September 2004, the May 2003 version was used in inspections of Sacramento, Boston, and Cincinnati in October and November 2004. We were advised by the Inspection Division that it was not until February 2005 that it began to use the revised checklist in all inspections.

The Inspection Division's written interview procedure does not remedy these shortcomings. Guidance provided to Division personnel does not expressly mention compliance performance as a topic of inquiry. Rather, the Inspections Guidebook recommends, for example, that Supervisory Special Agents (SSAs) be interviewed on "investigative responsibility, specific investigations, initiatives, special projects, investigative techniques, task forces, liaison, prevailing crime problems, goals and objectives, the IB [intelligence base], and accomplishments." Further, the Inspection Division's guidance does not require that interviews be conducted to isolate the causes of compliance deficiencies. We were advised by Inspection Division personnel, however, that information regarding the causes of deficiencies frequently is collected during inspections.

We also noted that Inspection Division reports do not weight or categorize the seriousness of the deficiencies that are identified during inspections. Although a former Chief Inspector confirmed that the Office of Inspections historically has not undertaken this task, he explained that his office recently was attempting to institute changes that would characterize the gravity of any problems that the Inspection Division discovers. The current Assistant Director for the CID also noted this issue in his interview with the OIG. He stated that "[w]e count [the compliance deficiencies] all the same when we go out and do our audits. An error is an error is an error. We see these pretty high error rates when we do our compliance audits. Somehow we have to figure out a way to weight these things so that you get a real sense of where agents are [having problems]. . . . It doesn't stand the test of logic that we weight them all the same."

Our examination of 41 final inspection reports issued between May 1, 2002, and October 31, 2004, found that their content typically reflected the limitations of the data collection practices described above. The reports tended to itemize the various violations with little or no analysis and did not include the views or explanations expressed by supervisors or executive management during the inspection concerning their compliance performance. See Case Study 7.1 below. The reports also did not attempt to compare the results/findings with the performance records of other offices. Moreover, non-compliance in the Criminal Informant Program typically was not explained with reference to supervision deficiencies identified in particular squads or by individual performance lapses.

In contrast, during the recent informant reinspections conducted by the Inspection Division in conjunction with A/IU, the inspection team not only identified noncompliant conduct in their reports, it identified the squads and supervisory agents responsible for the conduct. As the case study below of one FBI Field Division shows, this degree of detail is not common in Inspection Division inspection reports.

### **Case Study 7.1: FBI Inspection Division Audit of a Field Division's Criminal Informant Program**

In January 2004, the Inspection Division conducted an inspection of an FBI Field Division, including an audit of its Criminal Informant Program. The period under review was from September 2000 to January 2004. After completing the inspection, the Inspection Division prepared a separate electronic communication to the office and the Criminal Investigative Division at FBI Headquarters summarizing its findings. The electronic communication explained that the audit "included a review of pertinent documentation, interviews with appropriate management personnel, SAs, support personnel, as well as review of selected pending and closed informant files." According to the electronic communication, Inspection staff examined 29 percent of the Division's source files during the audit and found that 88 percent had errors and 65 percent had multiple errors. Of the 21 categories of errors identified, 9 were recurring deficiencies from the 2000 inspection and included the following: failure to advise the source of the Attorney General Guidelines; failure to obtain proper authorization prior to a source's participation in otherwise illegal activity; failure to notify FBI Headquarters of a source's participation in criminal conduct; and failure to follow special provisions concerning the operation of sensitive sources.

Inspection staff also identified in the electronic communication the managers of the Division's Criminal Informant Program and the duties of certain support staff. With respect to the Criminal Informant Program Coordinator, the electronic communication explained as follows:

Review of confidential informants/cooperative witness/CSs files and records maintained by the Criminal Informant Program Coordinator determined [that he] utilized ticklers and e-mails to remind agents and supervisors of compliance issues. Furthermore, the Criminal Informant Program forms were made available on a shared drive for all agents and supervisors to access. [The Criminal Informant Program Coordinator] provided individual training session [sic] to SAs and regularly disseminated policy communications received from the Asset/Informant Unit.

No information was included in the electronic communication concerning the action or inaction of other members of senior management, such as the ASACs who had supervised the program during the inspection period, or an explanation of their interpretation of why, given the apparent adequacy of the Criminal Informant Program Coordinator's efforts, this Division had one of the highest Criminal Informant Program non-compliance rates in the FBI. The electronic communication concluded without analysis that the Division's Criminal Informant Program was "in substantial non-compliance with Criminal Informant Program rules and procedures" and set forth the following instruction and recommendation: (1) the "SAC should ensure cited deficiencies are corrected, where possible, and administrative controls are strengthened to preclude recurrence of these deficiencies," and (2) the "SAC should ensure all compliance issues brought to the attention of squad/RA supervisors by the Criminal Informant Program Coordinator are promptly handled in an effort to minimize violations of policy and procedure." No explanation was provided concerning how this should be done or why the Inspection Division believed these general recommendations would eliminate the many recurring deficiencies that were subject to similar post-inspection remedies four years earlier.

## **B. Changes in the Inspections Process After the May 2002 Revisions of the Attorney General Guidelines**

According to a former Chief Inspector, one of the major challenges facing the Inspection Division is keeping pace with FBI programmatic and policy changes as they occur. He explained that this task is difficult because of the volume of new policy and guidance that is generated at the FBI. To address this issue, the Inspection Division's 2004 Program Plan identified as an "action item" the establishment of a "system that ensures timely notification of the [Inspection Division] on program and policy changes." The Inspection Division's standard practice is for Inspection Management Unit personnel to consult in mid-summer with the various FBI divisions concerning needed revisions to the Division's inspection documents. We were informed, however, that not all Divisions adequately share information regarding changes to policy and procedures.

Moreover, we found that changes in policies do not always result in timely changes to Inspection Division practices. For example, the modification of the Attorney General Guidelines in May 2002 did not prompt comprehensive revisions to the Inspection Division's checklists or interrogatories.<sup>366</sup> Although written Continuing Suitability Reports and Recommendations have been required since 2001, Inspection Division checklists did not address this important requirement for three and a half years after the Guidelines revisions.<sup>367</sup> According to the FBI's Chief Inspector in May 2002, consistent with its standard practice, during the summer of 2002, the Inspection Division solicited feedback from Headquarters divisions as well as the Criminal Informant Program concerning revisions to the Division's Criminal Informant Program checklists. Although the CID recommended a limited number of alterations to the confidential informant checklist, the one in use in 2003 contained the gaps described in Section I.A above.

## **C. Inspection Division Findings Regarding Attorney General Guidelines Compliance**

Our review of 41 Inspection Division inspection reports and supporting documentation issued between May 1, 2002, and October 31, 2004, revealed that FBI inspectors often discovered Guidelines violations.

---

<sup>366</sup> We are not suggesting that the nature of the Guidelines revisions alone necessitated extensive rewriting of the checklists. Rather, the changes to the Guidelines could have refocused attention on the content of the checklists and resulted in the filling of important information gaps that existed at the time.

<sup>367</sup> In the course of this review, A/IU generated a revised checklist for use by the Inspection Division that addresses the CSR&R requirement. As explained *supra*, it was not used consistently by the Inspection Division until February 2005.

However, the frequency of identification of these violations varied between programs and often was significantly less than what the OIG identified during its field work. While we identified few violations in the Inspection Division reports with regard to the Undercover Operations, General Crimes, and Consensual Monitoring Guidelines, violations in the Criminal Informant Program were commonplace. Although the Inspection Division identified many Guidelines violations in the administration of the Criminal Informant Program, it found violations related to the Confidential Informant Guidelines at less than half the rate identified during our visits to 12 FBI field offices. Below we summarize inspection report findings for each of the four Investigative Guidelines.

### **1. Criminal Informant Program**

Between May 1, 2002, and October 31, 2004, the Inspection Division examined 3,434 Criminal Informant Program files in 41 of the FBI's 56 field divisions. Of the files examined, Inspection Division documentation shows that approximately 34 percent indicated a violation of the Confidential Informant Guidelines during the relevant inspection period. The table below ranks these 41 FBI field divisions according to the percentage of inspected Criminal Informant Program files that contained one or more compliance deficiencies (which include violations of MIOG requirements as well as of the Attorney General Guidelines). As shown below, nearly one in three field divisions identified in Table 7.3 had a file non-compliance rate at or above 40 percent and thus qualified for an additional inspection (a "reinspection") conducted by Inspection Division personnel in conjunction with the Headquarters-based Asset/Informant Unit.

When the rates above are compared with those obtained during inspections before May 2002, we found that over the last two inspection cycles (1999 to present) non-compliance recurred in certain offices. Of the 13 field divisions identified above with a Criminal Informant Program non-compliance rate at 40 percent or more, 6 divisions had a non-compliance rate during the preceding inspection that exceeded 30 percent, along with a high number of recurring deficiencies. Other divisions had a significant worsening of compliance performance as measured by the Inspection Division. For example, the Albany Field Division's non-compliance rate rose from 11 percent in 2001 to 68 percent in 2004. In contrast, a number of field divisions maintained rates below 15 percent for the last two inspections, while others showed marked improvement. Table 7.4 presents these findings for select field divisions.

**TABLE 7.3**

**Percentage of Criminal Informant Program Files with  
Compliance Deficiencies Identified by the Inspection Division  
(May 2002 – October 2004)**

<b>Field Division</b>	<b>Non-compliance Rate</b>	<b>Field Division</b>	<b>Non-compliance Rate</b>
<b>Columbia, SC</b>	88%	Anchorage, AK	27%
<b>Buffalo, NY</b>	85%	Atlanta, GA	26%
<b>Albany, NY</b>	68%	Minneapolis, MN	25%
<b>Norfolk, VA</b>	65%	Denver, CO	25%
<b>Milwaukee, WI</b>	63%	Las Vegas, NV	24%
<b>St. Louis, MO</b>	59%	El Paso, TX	22%
<b>San Diego, CA</b>	58%	Charlotte, NC	21%
<b>Omaha, NE</b>	56%	Chicago, IL	21%
<b>Cleveland, OH</b>	56%	Memphis, TN	20%
<b>San Francisco, CA</b>	56%	Sacramento, CA	20%
<b>Jacksonville, FL</b>	53%	Oklahoma City, OK	19%
<b>Salt Lake City, UT</b>	52%	Springfield, IL	18%
<b>Mobile, AL</b>	43%	Albuquerque, NM	15%
New Orleans, LA	39%	Newark, NJ	14%
Indianapolis, IN	37%	Little Rock, AR	12%
New York, NY	35%	Seattle, WA	13%
Dallas, TX	29%	San Juan, PR	13%
Baltimore, MD	29%	Knoxville, TN	6%
Pittsburgh, PA	28%	Kansas City, MO	4%
Miami, FL	27%	Jackson, MS	0
Louisville, KY	27%		

**Bold** = Exceeds threshold for the Asset/Informant Unit reinspection

**TABLE 7.4**

**Inspection Division Deficiency Data for  
Criminal Informant Program in Select Field Offices**

<b>Field Division</b>	<b>Non-compliance Rates</b>		<b>Number Of Recurring Deficiencies</b>
	<b>Pre-2002 Inspection</b>	<b>Post-2002 Inspection</b>	
	<b>Persistent Non-compliance (consistently above 30%)</b>		
Columbia, SC	47%	88%	9
Milwaukee, WI	47%	63%	8
St. Louis, MO	60%	59%	10
San Francisco, CA	52%	56%	7
Jacksonville, FL	31%	53%	5
Salt Lake City, UT	32%	52%	6
	<b>Worsening Non-compliance Rate (from below 30% to significantly above 30%)</b>		
Buffalo, NY	29%	84%	7
Albany, NY	11%	68%	3
Norfolk, VA	25%	65%	3
San Diego, CA	15%	58%	3
Cleveland, OH	11%	56%	1
Omaha, NE	25%	56%	2
Mobile, AL	15%	43%	3
	<b>Improved or Consistently Low Non-compliance Rate (below 15%)</b>		
Jackson, MS	*	0%	3
Kansas City, MO	31%	4%	3
Knoxville, TN	10%	6%	3
Little Rock, AK	28%	12%	3
San Juan, PR	16%	13%	2
Seattle, WA	Minor*	13%	*
Newark, NJ	10%	14%	2

\*Inspection Division report did not itemize deficiencies or report percentage error rate.

Although each of the above field divisions that experienced persistent non-compliance received an instruction from the Inspection Division during the inspection preceding May 2002 to prevent the recurrence of Criminal Informant Program deficiencies, and each responded to the inspection report in a way that led the Division to close out its findings and terminate its oversight, the Criminal Informant Program compliance problems in these divisions persisted, and in some instances worsened substantially.

When Criminal Informant Program problems are discovered, the Inspection Division typically requires that “internal controls be strengthened,” which, according to a former Chief Inspector, is a directive targeted at the Confidential Informant Coordinator, the ASAC who supervises that person, and the SSAs. The former Chief Inspector explained that after issuing its Criminal Informant Program directives, the Inspection Division frequently finds that field offices adopt remedies that include reminding supervising agents of their responsibilities and providing FBI personnel with enhanced training opportunities. Our review of field division responses to Criminal Informant Program inspection findings confirmed this often occurred, and that generally the divisions responded in a detailed fashion describing their completed and proposed corrective actions. However, as evidenced by the field divisions identified in Table 7.4 with persistent Criminal Informant Program non-compliance, the practice of delivering reminders, creating training opportunities, and issuing directives to enhance administrative supervision was inadequate in some cases. See Case Study 7.2 below.

Because Inspection Division oversight usually terminates shortly after the field division responds to the inspection report, field divisions that require greater supervision historically have been allowed to operate their Criminal Informant Programs in non-compliance until the next inspection three years later. For example, even though the Inspection Division’s inspection of the St. Louis Field Division’s Criminal Informant Program in 2001 identified 23 different types of non-compliance and an overall non-compliance rate of 60 percent, by 2004 the Program had improved its non-compliance rate by only 1 percent – to 59 percent.<sup>368</sup>

The experience of the San Francisco Criminal Informant Program also illustrates the practice of allowing field divisions to operate their Criminal Informant Programs in violation of FBI and DOJ rules and regulations.

---

<sup>368</sup> A self-inspection of the St. Louis Criminal Informant Program in 2003 found a non-compliance rate of 58 percent. The 2004 inspection revealed that during the 2001-04 inspection period, the St. Louis Criminal Informant Program had five different program managers and three different Informant Coordinators, the last of whom reported that he was only able to devote five percent of his time to the Program due to his extensive collateral duties.



### **Case Study 7.2: The San Francisco Criminal Informant Program**

Despite five inspections over the past decade [three triennial, a self-inspection, and a reinspection], the San Francisco Field Division consistently has maintained one of the worst Criminal Informant Program (CIP) compliance rates in the FBI. For the inspection period ending in 1996, the Inspection Division documented compliance errors in 58 percent of the CIP files examined. Compliance was little improved by 2000, with 52 percent of the CIP files failing to comply with FBI mandates. The Inspection Division's inspection in 2003 revealed a non-compliance rate of 56 percent, which followed a field office-initiated self-inspection of the CIP in 2002 that found an error rate of nearly 49 percent. The self-inspection had reported that "the Informant Program was in substantial compliance with regulations and Bureau policy."

In light of its June 2003 findings, the Inspection Division and the Asset/Informant Unit (A/IU) conducted a reinspection in December 2003 of every pending CIP file in the San Francisco Field Division. Despite a recommendation from the Inspection Division that the "SAC, San Francisco ensure all pending confidential informants\CS\CW files are reviewed and brought into compliance prior to the A/IU on-site review," and approximately 6 months prior warning of the upcoming reinspection, the Inspection Division and the A/IU identified compliance errors in 70 files, or 22 percent of those inspected, with 19 of these having multiple errors. The reinspection analyzed compliance performance by squad and specifically noted that a lack of accountability among SSAs contributed to the Division's failings. The report explained:

One contributing factor for a majority of the deficiencies identified during this re-inspection was the failure of the San Francisco SSAs to ensure personnel under their direct supervision were correcting identified CIP deficiencies. For example, the re-inspection determined that many of the errors cited in this report were the result of SSAs failing to follow-up on issues identified by the San Francisco CIC [Informant Coordinator]. This re-inspection reviewed numerous routing slips, e-mails, and reminders from the CIC which were placed in the confidential informant/CW/CS files to assist the SSAs and SAs with management of their files. In many instances these notations were ignored by the SSAs and SAs, resulting in compliance errors documented during this re-inspection. In some instances SSAs noted deficiencies on consecutive file reviews which were ignored by the SA with no follow-up by the SSA.

The A/IU reinspection report also discussed several other factors that contributed to the Division's CIP problems, including lack of consistency in standardized forms and specific topics on which agents required training. The report concluded that the San Francisco CIP is "adequate," though "closer administrative oversight was needed."

Our review also revealed that field divisions that experienced a substantial deterioration in their non-compliance rate often had a lack of continuity in the support provided by the Criminal Informant Program's management. For example, of the field divisions identified in Table 7.4 with worsening non-compliance rates, one had five different Confidential Informant Coordinators during the inspection period, not counting a seven-month period when the Confidential Informant Coordinator position was vacant. A second division had three different Criminal Informant Program managers in two and a half years. In another field division, the Inspection Division found that the Confidential Informant Coordinator had too many collateral duties, and in two other divisions the Confidential Informant Coordinator was found deficient in the performance of his duties, leading to the removal of one Coordinator.

Our review of the written performance appraisals of the SSAs, ASACs, and SACs in divisions with Criminal Informant Programs that had significant compliance problems indicated that the appraisals did not reflect the deficient Criminal Informant Program compliance performance.<sup>369</sup> This was in contrast to what the FBI Director and the Assistant Director for the CID told us should occur. Both of them stated that high rates of non-compliance in the Criminal Informant Program should be taken into account in the performance appraisals of field office managers.

In contrast, our interviews with Confidential Informant Coordinators from field divisions that had consistently good or significantly improved Inspection Division inspection performances revealed that management of the Criminal Informant Program typically had less personnel turnover and employed a number of best practices that, in the opinion of the Coordinators, contributed to their divisions' favorable compliance record. These included the use of standardized forms, computer-generated reminders by the Confidential Informant Coordinators or confidential file room analysts to case agents to meet upcoming deadlines, intensive file reviews, compliance checklists for SSAs to assist them with their file reviews, and adequate training, especially for SSAs.<sup>370</sup> Two Confidential Informant Coordinators we interviewed even developed a Criminal Informant Program handbook for use in educating agents.

---

<sup>369</sup> In response to a draft of this report, the FBI correctly noted that its performance appraisal process for Special Agents, SSAs, and ASACs does not allow for narrative evaluations and, according to the FBI, "[t]herefore, there is little ability by which to distinguish superior compliance performance in an employee's Performance Appraisal Report (PAR). . . . [D]eficient compliance performance would only be reflected if it was sufficiently significant to warrant a rating of 'Does Not Meet Expectations' for the critical element which pertains to compliance performance."

<sup>370</sup> For a description of the role of the confidential file room analyst, see discussion *supra* at n.200.

Moreover, support for the Criminal Informant Program by the Division's executive management in these offices also was described as very important. In one field division, executive management implemented an *ad hoc* "three strike policy" that required the informant file to be closed administratively if an agent received more than three notifications of compliance deficiencies on the same informant.

In addition, our interviews with FBI personnel confirmed the impact that high-performing Criminal Informant Coordinators can have on the functioning of the Criminal Informant Program, an observation that we also found in Inspection Division inspection reports and Criminal Informant Program electronic communications. These described several instances where the performance of an individual, such as the Confidential Informant Coordinator, accounted for the rehabilitation of an otherwise deficient Criminal Informant Program. For example, the most recent inspection report for the Cleveland Field Division described the work of the Confidential Informant Coordinator as substantially improving the Program:

Cleveland's Criminal Informant Program improved substantially during the second half of the inspection period. This coincided with the appointment of SA [name deleted] as the Criminal Informant Coordinator in February 2002. [The Criminal Informant Coordinator] implemented a 90-day compliancy review of the pending files and began reporting findings to the SSA responsible for conducting the file reviews. [The Criminal Informant Coordinator] conducted file reviews for all pending Cleveland Division confidential informants and cooperative witnesses prior to the scheduled SSA file reviews.

Prior to the assignment of [the Criminal Informant Coordinator], the former coordinator had not implemented new policies regarding 137s [i.e., confidential informants] and a large number of files were delinquent regarding SI status and Attorney General Guidelines. [The Criminal Informant Coordinator] implemented most of the 137 procedures and made improvements to address delinquencies. Those improvements were apparent from the Criminal Informant Program Audit, as well as from a review [sic] the tracking systems in place in [the Criminal Informant Coordinator's] office. As of August 4, 2003 the pending files were almost 100 percent compliant in these areas.

The Inspection Division's inspection of the Kansas City Criminal Informant Program also highlighted the positive work of the Criminal Informant Coordinator:

This audit indicated that the management team closely monitored the Criminal Informant Program throughout this

inspection period. They personally reviewed confidential informants/cooperative witness files on a regular basis and met frequently with SSAs and SAs regarding informant matters. . . . [The Criminal Informant Coordinator] was intimately involved in every aspect of the Criminal Informant Program and she personally reviewed all confidential informants/cooperative witness files on a semiannual basis. She coordinated directly and frequently with case agents regarding compliance issues and she operated a weekly tickler system to ensure timely response. [The Criminal Informant Coordinator] implemented an aggressive Criminal Informant Program training program for the division and regularly educated Kansas City personnel regarding policy and program changes in the Criminal Informant Program. Further, she implemented a comprehensive self-inspection program.

The incidence of Criminal Informant Program deficiencies described above is not the only indicator of problems in the program. The nature of the violations that the Inspection Division identified also is highly significant. Table 7.5 summarizes the types of Criminal Informant Program non-compliance most commonly identified by the Inspection Division from May 2002 through October 2004, including the section of the Confidential Informant Guidelines violated, the number of files in which violations were found, and the share that each violation represents in relation to the Confidential Informant Guidelines deficiencies itemized below.<sup>371</sup>

---

<sup>371</sup> The “frequency” of violations described here understates the actual number of violations contained in the files reviewed by the Inspection Division. In some cases, the Inspection Division did not identify in its report or supporting Criminal Informant Program electronic communication the number of files that contained deficiencies. For example, in the Cleveland Criminal Informant Program audit several categories of deficiencies were described as “inveterate,” meaning they appeared in every applicable file reviewed. Such information is not captured in Table 7.5. In addition, the Inspection Division often reports that multiple errors are contained in a single file, which may include multiple errors of the same type. Table 7.5 represents these as a single file violation.

**TABLE 7.5**

**Types of Confidential Informant Guidelines Violations  
Identified by the Inspection Division (May 2002 – October 2004)**

<b>Violations</b>	<b>CI Guidelines Violated</b>	<b>Frequency (Number of Files)</b>	<b>Percentage of all CI Guidelines Deficiencies</b>
Failure to Timely Provide AGG Instructions	CI AGG II.C	229	44%
Failure to Include Photograph of CI in File	CI AGG II.B	80	15%
Failure to Convert CI to Operational Status Prior to Use, or to Extend or Close SI Period	CI AGG II.B	58	11%
Failure to Obtain Authorization of OIA	CI AGG III.C	38	7%
Failure to Document Background Information (e.g., criminal history)	CI AGG II.A	34	7%
Failure to Report Unauthorized Illegal Activity	CI AGG IV.B	18	3%
Failure to Obtain Authorization for Privileged or Sensitive Sources	CI AGG II.D	15	3%
Failure to Maintain Proper Payment Documentation	CI AGG III.B	13	3%
Failure to Follow Special Provisions When Operating Sensitive CIs/CWs	CI AGG II.D	11	2%
Failure to Notify FBI Headquarters of Conversion of Sensitive Source to Operational Status	CI AGG II.D	8	2%
Failure to Have Two Witnesses to Payment of CI	CI AGG III.B	3	1%
Maintaining Ongoing Contact with Closed Source	CI AGG V.C	3	1%
Failure to Prevent the Use of CI to Obtain Privileged Information	CI AGG III.C	1	.2%
Use of Faulty Instructions	CI AGG II.C	occurred	NA
<b>Other Related Violations (non-AGG)</b>			Share of All CIP Deficiencies
Failure to Conduct Timely File Reviews	MIOG 137-4	348	21%
Failure to Document Upon Closing Whether Identity of CI was Revealed Outside the FBI	MIOG 137-15	14	1%
Failure to Obtain Proper Authorization to Disclose the Identity of the CI	MIOG 137-9	13	1%

As explained in Chapter Three of this report, these findings were comparable to the results of the OIG's field work with respect to those Guidelines violations that the Inspection Division evaluated.

## **2. Inspection Division Audits of Undercover Operations and Consensual Monitoring**

In contrast to the high number of deficiencies that the Inspection Division identified with the Criminal Informant Program, its audits of undercover operations and consensual monitoring found few Guidelines violations. Of the four violations that the Inspection Division identified during its audits of undercover operations from May 2002 through October 2004, one involved a Group II UCO that continued for more than a year without Headquarters approval, while in another division, Headquarters was not properly notified after two undercover operations were initiated. The fourth violation involved a failure to present a fiscal circumstance to FBI Headquarters for review.<sup>372</sup> The Inspection Division's inspection reports identified violations of the Consensual Monitoring Guidelines in six field divisions. In each case, proper authorization was not obtained and documented prior to the start of the monitoring, contrary to the Guidelines' requirement. By comparison, we found in our review approximately 10 percent of the undercover operations and consensual monitoring files contained authorization-related errors.

## **3. General Crimes, REIs, and TEIs**

Although the Inspection Division's data collection instruments for the Criminal Informant Program, Undercover Operations, and electronic surveillance (ELSUR) audits address many key provisions of the Attorney General Guidelines, we did not find comparable coverage for the authorities contained in the General Crimes Guidelines. For example, Part VI of the General Crimes Guidelines constrains the expanded authorities to create information systems, "surf" the Internet, visit public places and attend public events, as well as instructions for complying with the Privacy Act. We were advised by the FBI, however, that the Inspection Division does not audit information pertaining to the FBI's attendance or monitoring of public events or its record retention practices relating to those activities. Despite the limited coverage of the authorities contained in the General Crimes Guidelines, our review of inspection reports issued since May 2002 identified a limited number of General Crime Guidelines' violations. These included the continuation of a preliminary inquiry for more than one year without obtaining proper authorization, and several instances of agents

---

<sup>372</sup> Undercover operations that involve any of the "fiscal circumstances" enumerated at § IV.C.1 of the Undercover Guidelines require special approvals.

failing to provide the requisite notifications regarding the opening of investigations into sensitive criminal matters.

#### **D.     OIG Analysis**

Inspection Division management and other FBI officials recognized the importance of the Inspection Division's role in ensuring compliance with the Attorney General Guidelines. For example, a former Inspection Division Assistant Director stated that "[the Director] depends on us to measure those things that matter most," and, "we are required to ensure that all Attorney General Guidelines are complied with. We cannot have an Attorney General Guidelines' violation." A former Chief Inspector also commented on the importance of perceptions regarding the Inspection Division's priorities to actions in the field, observing that the conduct of agents is heavily influenced by what the Division chooses to monitor.

We concluded that the Inspection Division's efforts to assess performance of all investigative and support operations could be improved in three critical respects: 1) increasing the scope of inspections to better assess compliance with the Guidelines; 2) better promoting accountability for adherence to the Guidelines; and 3) shortening the time to detect violations and incorporating information technology tools to make its work more efficient and its findings more useful.<sup>373</sup> With regard to the Inspection Division's substantive inspection findings, we found systemic Criminal Informant Program deficiencies, including widespread violation of certain Attorney General Guidelines' requirements and persistent non-compliance in some field divisions. The seriousness of these violations varies widely, from documentation errors to failing to report unauthorized illegal activities by confidential informants. This conclusion is consistent with the findings of our field work, which we described in Chapter Three.

#### **1.     Scope of On-site Inspections**

Our analysis of the Inspection Division's inspection reports indicates that the Division should increase the scope of its audits to include more information concerning Guidelines compliance and implementation. We believe that both the types of audits performed by the Inspection Division during its on-site inspections as well as the information collected from the current audits should be expanded to provide better oversight of Guidelines issues. The Inspection Division also should focus its audits on areas that are deemed priorities or that have been identified as problems from prior inspections, and make its reporting more comprehensive by collecting reliable information on the causes of deficiencies and categorizing the gravity of deficiencies that are found.

---

<sup>373</sup> Inspection Division Program Plan (2004) at 1.

As explained above, several of the checklists used by the Inspection Division to collect data on topics addressed in the Attorney General Guidelines, including those for the Criminal Informant Program, squads, and programs are not sufficiently comprehensive. For example, we believe the Inspection Division's failure to include Continuing Suitability Report & Recommendations (CSR&R) preparation on the Criminal Informant Program checklist was a significant contributor to the high non-compliance rate we discovered for that requirement. At the time of our visits, two field divisions had not completed any CSR&Rs, even though the requirement to do so has plainly been set forth in the Confidential Informant Guidelines since 2001. As a former Chief Inspector observed, "people do what they are measured by."

We also recommend adding an evaluation of the FBI's compliance with key provisions contained in Part VI of the General Crimes Guidelines. During our review we asked the FBI to provide us with information relating to its exercise of Part VI authorities and were advised by the Inspection Division that it was not practicable to locate the information since it was not separately retained in FBI files. Because we repeatedly have been told by field personnel that agents typically do not have time to visit public places and events due to the press of other business, we believe the burdens associated with the review and analysis of the information should not be great. Moreover, with respect to visiting public places and events, the FBI already has recommended documentation requirements. FBI OGC Guidance explains that "[a]ttendance by an agent under Part VI of the General Crimes Guidelines . . . should be documented in some retrievable fashion."<sup>374</sup> We do not believe that the addition of Inspection Division oversight should add significantly to agent administrative burdens.

Although we believe that the Inspection Division should expand its information collection in some areas, our review also revealed that the Division would benefit by targeting a greater proportion of its on-site inspection resources to priority and problem areas. Division management stated that its priority audits are the Criminal Informant Program, ELSUR, and Evidence. However, the Inspection Division does not identify these programs for more frequent on-site inspections or reinspections. Some programs may warrant inspection every four years of a relatively small sample of files; others may require inspection every year of every file. We believe the Inspection Division should focus its inspection resources on programs that are priorities or are identified with chronic or persistent problems, and should work with Headquarters program divisions to enhance inspection oversight in these areas. The Inspection Division also should continue to supplement its work with field-initiated self-inspections.

---

<sup>374</sup> See Electronic Communication from the FBI General Counsel, March 19, 2004.



Specifically, we believe it should initiate a simultaneous self-inspection or limited reinspection of the Criminal Informant Program for field divisions identified as having significant compliance problems.

The scope of the Inspection Division inspection reports and supporting electronic communications should be expanded to include: 1) collection of data suggesting the causes of the identified compliance deficiencies and an analysis of the explanations provided by field personnel for the inspection results, and 2) an assessment of the gravity of the compliance deficiencies based on information gathered from revised checklists. Currently, the inspection reports itemize violations with little or no supporting analysis, and they do not address the field office's version of events. We believe this creates two problems.

First, itemizing the violations and announcing a non-compliance percentage based on the number of files that contain one or more errors can mask important performance information and lead to the misallocation of reinspection resources. For example, a Criminal Informant Program in which agents failed to include a photograph of the confidential informant in the file due to lack of training might have a 100 percent non-compliance rate, while another Informant Program might have a much lower non-compliance rate but have more significant deficiencies associated with the commission of unauthorized illegal activity by informants whose handlers ignore Guidelines' requirements and the instructions of their SSAs and Confidential Informant Coordinator. Our review of the Inspection Division's inspection reports suggests that the latter circumstance would not receive the greater remedial attention it deserves. The causal factors associated with compliance performance and the field office's explanation of its performance should be more fully described in the reports. This should include providing information comparing an office's performance with other FBI components and specifically identifying deficiencies as Guidelines violations when they are found.

These recommendations are especially relevant to the Criminal Informant Program. Before the suspension of reinspections in November 2004, the standard employed to trigger reinspection of noncompliant Criminal Informant Programs was based on Inspection Division findings concerning the percentage of informant files that contained one or more errors. Criminal Informant Programs with a file error rate that exceeded 40 percent were eligible for a reinspection by personnel from A/IU. However, the gravity of the violations found did not influence whether this percentage threshold was exceeded; it was a purely statistical computation. We believe that there are better ways for the Inspection Division to analyze and compare Criminal Informant Program compliance performance, and that the Inspection Division and HIU should work together to develop new measures that determine when inspection resources should be targeted on problems of special concern in the field. The Inspection Division Assistant Director

agreed that the 40 percent threshold for reinspections should be replaced with a standard that accounts for the frequency and gravity of the violations found during inspections.

Below we provide an example of how the FBI could assess field office compliance with key Informant Guidelines and MIOG requirements. To illustrate such an approach, we utilized a matrix that weights violations of these requirements and accounts for both the frequency and severity of Criminal Informant Program deficiencies identified during inspections. Application of such a matrix could also be used to develop a standard for conducting reinspections. We recommend that the FBI determine what considerations best capture noteworthy performance issues, how to weight various compliance deficiencies, and what should be reported by the Inspection Division.

To demonstrate how use of a matrix can change the evaluation of the Criminal Informant Program, below are comparisons of Inspection Division non-compliance percentages and the scores generated for select field divisions from the matrix which we developed. Using this model, the deficiency score for San Diego is noteworthy because it is significantly lower than scores for divisions with comparable non-compliance percentages. The reason for this is straightforward: more than 80 percent of San Diego's deficiency points were generated from deficiencies such as failing to include a photograph of the CI in the informant file and failing to provide annual instructions to CIs, which are weighted as less severe in the matrix than deficiencies such as failing to obtain authorization for a source's participation in illegal activity and failing to notify FBI Headquarters of a source's participation in unauthorized illegal activity, which accounted for more of the compliance deficiencies found in other field offices.

**TABLE 7.6**

**Comparison of Deficiency Measures for  
Select FBI Field Office Criminal Informant Programs**

<b>Field Division</b>	<b>Inspection Division Non-compliance Percentage</b>	<b>Deficiency Matrix Score</b>
Newark	14%	3.1
Jacksonville	53%	24.0
San Diego	58%	11.8
Albany	68%	37.0
Columbia	88%	46.0

Besides masking important information about compliance performance, a second disadvantage of itemizing violations in the inspection reports with little or no qualitative assessment or supporting analysis concerning causation is that it makes it more difficult to evaluate the sufficiency of the remedies proposed by the field division in response to the report.<sup>375</sup> Ideally, these remedies would address the causes of the deficiencies identified by the Inspection Division. Field divisions should explain in their responses how their remedies will effectively address the causes of the identified deficiencies.

## **2. Promoting Accountability**

Our review indicates that the Inspection Division can and should do more to promote accountability for compliance performance. Too often we found in the inspection reports and their supporting electronic communications instances of recurring non-compliance with insufficient corrective response to the conduct of those who were responsible for it. We believe that if a particular squad or individual is responsible for a disproportionate share of a field division's compliance deficiencies, this fact should be stated explicitly in the inspection report. The reinspection reports generated by the Inspection Division and A/IU for the Columbia, Omaha, and San Francisco Criminal Informant Programs are examples of how accountability can better be reinforced through inspection findings. These reports analyze Criminal Informant Program compliance performance by squad.

We believe that inspection findings should be accounted for in agent performance appraisals, which was not done, for example, in field offices with seriously noncompliant Criminal Informant Programs.<sup>376</sup> The Inspection Division Assistant Director agreed that significant deficiencies noted during inspections should be accounted for in employee performance appraisals.

The Inspection Division also should modify its squad and investigative program checklists to note areas where compliance performance is inadequate. Information collected from these documents can assist

---

<sup>375</sup> It also makes it more difficult to determine whether the remedies should involve referral to the FBI's Internal Investigations Section. Without knowing the cause of a deficiency, it is not possible to evaluate whether it was performed knowingly or recklessly. See e.g., OPR offense codes 1.5 and 1.8 which address the knowing or reckless failure to abide by an FBI or DOJ operational guideline or policy.

<sup>376</sup> The Informant Guidelines require the FBI to establish procedures that ensure "that compliance with these Guidelines is considered in the annual performance appraisal of its agents." Informant Guidelines, § I.I. See also discussion *supra* Chapter Three describing the FBI's failure to account for compliance with the Informant Guidelines in these appraisals.

inspectors to better identify the causes of deficiencies. These checklists should include cross-references to the findings in other data collection instruments. For example, excessive deficiencies in a squad's Criminal Informant Program compliance performance should require examination of the findings from the squad/RA audit worksheet that address "Communication Capacity" and "Personnel Management and Administration," among other topics.

In addition, we believe that the Inspection Division can better promote accountability and Guidelines compliance through more effective follow-up on inspection instructions, recommendations, and findings. At present, even in circumstances where serious deficiencies are found during an inspection, the Inspection Division's involvement rarely continues more than a few months beyond the period during which offices respond to the inspection report. In our view, this practice has allowed the persistent non-compliance identified in Table 7.4. When a program is identified as having a poor compliance record, the Inspection Division should evaluate the feasibility of sending at least one Assistant Inspector in Place back to the office at periodic intervals until the problem is resolved and compliance verified. Comprehensive reinspections by the relevant Headquarters program office can be a substitute for this process, as occurred in a limited number of field offices with deficient Criminal Informant Programs. We also suggest that the Inspection Division provide commentary on the findings and indicate whether further reinspection work is needed.

We also recommend that where egregious non-compliance is discovered, the violation be elevated to a finding directed to executive management in the inspection report and not wait until a recurring deficiency is noted three years later during the next inspection cycle.<sup>377</sup> In our view, the practice of deferring prompt elevation of serious problems has contributed to delays in remedying them.

### **3. The Timing of Inspections and Better Use of Technology**

The amount of time it takes the Inspection Division to detect Guidelines violations is problematic. At present, the Inspection Division's standard practice is to conduct on-site inspections every three years. Reinspections are rare and self-inspections were cancelled as of June 2004, although we understand that the Inspection Division may reinstitute self-inspections in a different form in the future. We believe that investing resources to identify violations that occurred more than two to three years

---

<sup>377</sup> Inspection reports contain a section that describes the inspection's findings concerning the performance of the field division's executive managers, including whether they are "effective" and "efficient."

in the past is of limited utility, especially when technology is available that would allow the Inspection Division to identify violations with greater frequency and to monitor performance trends and indicators. With such a long delay between inspections, by the time inspectors arrive on-site the cause of the deficiencies identified during the inspection may have changed or ceased altogether. Moreover, problems may persist much longer than might be the case with a shorter period between inspections.

Former Assistant Director Steve McCraw, former Chief Inspector Grant, and the former Deputy Assistant Director of the Inspection Division, Michael Clemens, all emphasized to us the importance of changing the focus of the Division from identifying past mistakes to improving future performance. To realize this goal, they, along with current Assistant Director Thornton, told the OIG that a key component in any reform of the inspection process must include automation of the collection of compliance data. A recent Inspection Division program plan identified the limited state of the Division's technology.<sup>378</sup> In our view, shifting the orientation of the Inspection Division, and the associated resources, from compliance detection to compliance enforcement and assistance would enhance support for Guidelines compliance. The current inspection process and technology limitations, however, are obstacles to the implementation of such a shift in orientation.

To more quickly and efficiently identify instances of Guidelines non-compliance, we believe that the FBI should seek to automate that part of the inspection process that involves the manual review of paper case files for compliance errors. We saw from our own experiences in extracting compliance information from the FBI's files that the methods currently available to obtain this information are inadequate. The FBI continues to rely too heavily on paper file reviews to document its compliance performance.

We recognize that the completion of the work above is a long term goal that will take several years to achieve. However, with respect to monitoring of the Criminal Informant Program we believe a technology upgrade is necessary now and that an interim solution should be devised to assist with compliance oversight. Specifically, we believe the FBI should consider developing a standard Criminal Informant Program "tickler system" that can

---

<sup>378</sup> The Program Plan stated:

The Division is sorely lacking advanced automation and information technologies. This has hampered its ability to efficiently perform inspections, audits, and evaluations. . . . Inasmuch as information is the primary product of the Division, automation and information technology is foremost to success.

Inspection Division Program Plan (1999-2003) at 6-7.

be deployed in all field divisions and that will enable A/IU (now the HIU) and the Inspection Division to monitor compliance trends. Depending on the conduct at issue, computer-generated notifications should be set for ASACs, SACs, HIU, and the Inspection Division. We were advised by an FBI supervisory agent with experience in creating computer databases that the software to complete this work is commercially available and can be operational within 12 months.

## **E. Recommendations**

We recommend that the Inspection Division take the following steps.

(33) Revise Inspection Division checklists and interrogatories to increase inspection coverage of Attorney General Guidelines-related issues.

(34) As part of the Inspection Division's triennial inspections of field and Headquarters' divisions, establish an audit examining the collection of information obtained from exercise of counterterrorism authorities pursuant to Section VI.A.2 (Visiting Public Places and Events) of the General Crimes Guidelines.

(35) Provide more thorough and timely reporting of Attorney General Guidelines' violations by identifying in inspection reports the causes and gravity of compliance deficiencies; developing summary statistics to assist in determining when reinspections are appropriate; and automating key components of the inspection process.

(36) Increase inspections for the Criminal Informant Program and other programs that are priorities or experiencing significant problems by performing more frequent inspections at irregular intervals. The Inspection Division should also develop a standard for reinspections that accounts for the frequency and seriousness of the Attorney General Guidelines' deficiencies identified during the regular inspection and develop a standard for determining when reinspections should be conducted that accounts for both the number and gravity of the deficiencies found. The Inspection Division and the Human Intelligence Unit should reinstate its Criminal Informant Program reinspection process.

(37) Address in employee performance appraisals the findings from Inspection Division inspections that identify either superior or deficient Attorney General Guidelines' compliance performance.

(38) Elevate egregious non-compliance with Attorney General Guidelines to an executive management finding in the inspection report rather than deferring that action until the next three-year inspection contingent on the detection of recurring, serious deficiencies.

### **III. On-site Reviews by Program Offices**

In addition to Inspection Division inspections, various program offices at FBI Headquarters participate in field office reviews of activities in their program specialty. In conjunction with the Inspection Division, the Asset/Informant Unit has conducted reinspections of Criminal Informant Programs with high non-compliance rates. Certain undercover operations also are evaluated by USOU with assistance from Headquarters operational program offices. Because the field evaluations performed by A/IU and USOU sometimes address Guidelines compliance issues, we studied these additional efforts to assess their role in promoting adherence to the Guidelines.

#### **A. Undercover & Sensitive Operations Unit On-site Reviews**

From May 2002 through October 2004, USOU conducted on-site reviews of 60 undercover operations, of which 59 were Group I operations. In accordance with procedures set forth in the FBI Field Guide for Undercover Operations, Group I UCOs receive an on-site review from FBI Headquarters during their initial stages, generally within the first year. The Field Guide explains that “[a]n on-site review is not considered an inspection; but, rather an oversight procedure designed to facilitate the implementation of the undercover operation in a minimum amount of time and in compliance with applicable FBI rules and regulations.” Undercover operations that continue for more than one year after the initial USOU on-site may be reviewed periodically by the operational Headquarters section and USOU. According to the Unit Chief of USOU, the need for a second on-site review is rare because most undercover operations terminate before the need arises.

Personnel participating in the on-site review include a supervisor from USOU, a Headquarters supervisor from the substantive program involved in the undercover operation, and an auditor from the Inspection Division. The on-site typically lasts two to three days, during which time the review team examines the following: 1) program and operational issues, such as investigative strategy, accomplishments, and evidence-handling; 2) compliance and safety issues; and 3) financial issues. The USOU supervisor is responsible for conducting the compliance and safety review, which, according to guidance prepared by USOU, includes an examination of the undercover operation’s compliance with the Undercover Guidelines and CUORC stipulations.

Unlike A/IU, USOU does not use Inspection Division checklists during its on-site visits. Instead, it has developed its own checklist which, as of December 2004, was being substantially revised. Our review of both the revised draft and preceding versions of USOU’s checklist revealed that it does not seek information on several important Guideline issues, such as entrapment, OIA, and whether joint undercover operations are carried out

in accordance with the Undercover Guidelines. For example, the checklist evaluates neither the authorization nor implementation of OIA.

According to guidance prepared by USOU, Group II UCOs (which may be initiated without Headquarters approval) also are subject to on-site reviews under the following conditions: 1) the undercover operation has been extended beyond the initial six-month period of authority granted by a designated Assistant Director; 2) the undercover operation has expended more than \$100,000 in operational expenses; or 3) circumstances requiring special attention arise during the conduct of the undercover operation. From May 2002 through October 2004, USOU inspected only a single Group II UCO.

Once the results of the on-site visit are collected, the review team prepares an electronic communication that is formatted into the following sections: 1) synopsis of the undercover operation; 2) investigative achievements to date; 3) objectives of the undercover operation; 4) program and operational issues; 5) compliance and safety issues; and 6) audit and financial matters. The Headquarters operational unit supervisor is responsible for compiling the electronic communication, although both the operational unit and USOU supervisors are responsible for briefing the SAC or ASAC about the review's findings prior to the departure of the on-site team. As with inspection findings, the field division prepares a response to the electronic communication and explains how it will resolve any deficiencies noted during the review. A copy of the response is forwarded to USOU.

Our review of the results of USOU's on-site visits revealed comparatively few violations of the Undercover Guidelines. As explained in Chapter Four, USOU identified the following deficiencies: 1) in seven undercover operations, agents failed to obtain proper authorization for undercover activity; 2) in two undercover operations, division management failed to meet with undercover employees, while in five other undercover operations, documentation of the meetings was lacking; and 3) in one undercover operation a financial transaction was not properly structured.<sup>379</sup> None of the electronic communications identified these actions as Guidelines violations.

## **B. Asset/Informant Unit Reinspections**

A/IU led reinspections of four FBI field office's Criminal Informant Programs during the period June 2003 through November 2004. A/IU's participation in the Criminal Informant Program reinspections was initiated only recently. The former Chief of the Criminal Intelligence Section,

---

<sup>379</sup> These seven undercover operations were in different field divisions.



Criminal Investigative Division, told us that he initiated the practice in June 2003 following the Inspection Division's inspection of the San Francisco Division. The former Section Chief stated that he was the second-ranking Inspector for that inspection and was concerned by the high non-compliance rate for the Criminal Informant Program, a condition that had persisted for more than a decade. See discussion *supra* at Case Study 7.2 (describing San Francisco Criminal Informant Program). He said that after that inspection he advised FBI executive management in San Francisco that A/IU would return in six months to look at every confidential informant and cooperative witness file in the Division.

The new reinspection policy, which was transmitted in an electronic communication to the Inspection Division, provided that if a Criminal Informant Program had a non-compliance rate of 40 percent or more, a reinspection by A/IU would be triggered. The Section Chief stated that his drive to institute reinspections for offices that exceeded a 40 percent non-compliance rate was based on the belief that "if [agents] don't follow the rules with the simple things, and there is not enough oversight, that is where we could have an unhealthy relationship."

During reinspections, A/IU personnel work under the supervision of an Inspector in Place, typically an ASAC. ASACs serve as Inspectors in Place and are not assigned to the Inspection Division. Data is collected using the Inspection Division's Criminal Informant Program compliance checklist, and the findings are presented in a separate electronic communication. The reinspection electronic communications provide recommendations and instructions to the field division and are provided to the Inspection Management Unit for follow-up and resolution.

As of December 2004, A/IU had completed four Criminal Informant Program reinspections. The table below presents the inspection and reinspection non-compliance rates, and the number of recurring deficiencies for these four field divisions.

**TABLE 7.7**

**Inspection and Reinspection Non-compliance Rates  
for Select Criminal Informant Programs**

<b>Field Division</b>	<b>Inspection Non-compliance Rate</b>	<b>Reinspection Non-compliance Rate</b>	<b>Number of Recurring Deficiencies*</b>
Columbia	88%	38%	3
San Diego	58%	51%	6
Omaha	56%	33%	8
San Francisco	56%	22%	12

\*Deficiencies of the same type identified during succeeding inspections.

As shown above, by the time of the reinspection three of the four field divisions improved their non-compliance rates significantly, although the non-compliance rates generally remained high. Moreover, the reinspections revealed that several of the divisions had significant numbers of recurring deficiencies and that only one of the four divisions eliminated deficiencies related to two of the most critical Guidelines' provisions: the conduct of OIA and the handling of sensitive sources.

In addition to identifying overall Criminal Informant Program non-compliance rates, reinspections also can illuminate problems with implementation practices and deficiencies in the remedies instituted by Informant Program management in response to adverse inspection findings. For example, the San Diego Criminal Informant Program reinspection report highlighted the following implementation problems:

SAC [name omitted] took a number of strong steps to provide the necessary attention, emphasis, and support to the Criminal Informant Program since the November 2003 Inspection. . . . However, follow up to ensure the SAC's instructions were followed was not as strong. . . . An internal review of Criminal Informant Program files which was conducted by experienced supervisors failed to correct numerous deficiencies subsequently identified by the re-inspection team. . . . [T]he re-inspection uncovered numerous other deficiencies which were unambiguous by any standard. . . . The re-inspection for this period identified inadequate oversight to ensure the SAC's direction was followed as evidenced by a 51 percent error rate.<sup>380</sup>

As of December 2004 the Inspection Division and A/IU halted all reinspections of Criminal Informant Programs pending completion of discussions over revised reinspection procedures. According to the FBI's Chief Inspector at the time, the Inspection Division and A/IU need to address resource issues and the standards that will guide future reinspection activity. In February 2005, the OIG was told by a representative from the newly formed Human Intelligence Unit that the Inspection Division was changing its Criminal Informant Program inspection procedures and that until that work is complete reinspections would not be conducted.

---

<sup>380</sup> As explained supra at Case Study 7.2, the San Francisco Criminal Informant Program reinspection also noted problems with implementation of corrective action, most notably that the SSAs and agents often were ignoring requests from the Criminal Informant Coordinator.

### **C.     OIG Analysis and Recommendations**

We believe that the reinspections should be an important part of the FBI's compliance enforcement efforts and the former CID Section Chief should be commended for his efforts to institute the program in the Criminal Informant Program. We believe, however, that the FBI should re-examine the criteria that it uses to determine when reinspections should be performed for this program. Under the terms of the reinspection electronic communication issued by A/IU in February 2004, "any field office with a compliance error rate in excess of 40 percent will undergo a comprehensive Criminal Informant Program audit within six months of its inspection." This language sweeps too broadly. In our view, which is shared by the current Assistant Director of the Inspection Division, both the number and seriousness of the violations detected during the regular Criminal Informant Program inspection should be considered when determining reinspection eligibility and priority. See discussion in the preceding section of this chapter regarding Criminal Informant Program deficiency matrix.

In addition, we believe that the FBI should continue intensive monitoring of reinspected programs until satisfactory performance is demonstrated. Even though three of the four Criminal Informant Programs identified in Table 7.7 above showed some improvement in their non-compliance rates, the rates generally remained high, and several of the offices failed to eliminate problems with OIA and the handling of sensitive or privileged sources.

As with A/IU's reinspections, we believe there is significant merit in the on-site reviews of undercover operations supervised by USOU. They highlight important compliance and performance issues that warrant enhanced scrutiny and face-to-face interaction with Headquarters personnel. Our review of USOU's on-site data collection instrument revealed, however, that certain critical compliance provisions, such as the conduct of OIA, were not addressed. Given that the opportunities to perform on-site reviews of individual undercover operations are limited, we believe that when they are conducted they should be as comprehensive as practicable.

We recommend the following.

(39) The Inspection Division and the Human Intelligence Unit should institute procedures that establish follow-up inspection measures to reinspections that indicate ongoing compliance problems, such as assigning a single Assistant Inspector in Place to conduct an additional inspection within the first six months following the reinspection.

(40) Modify the Undercover and Sensitive Operations Unit's on-site review data collection instrument to better address Undercover Guidelines' compliance, including issues such as otherwise illegal activity, potential entrapment issues, and task force participation.

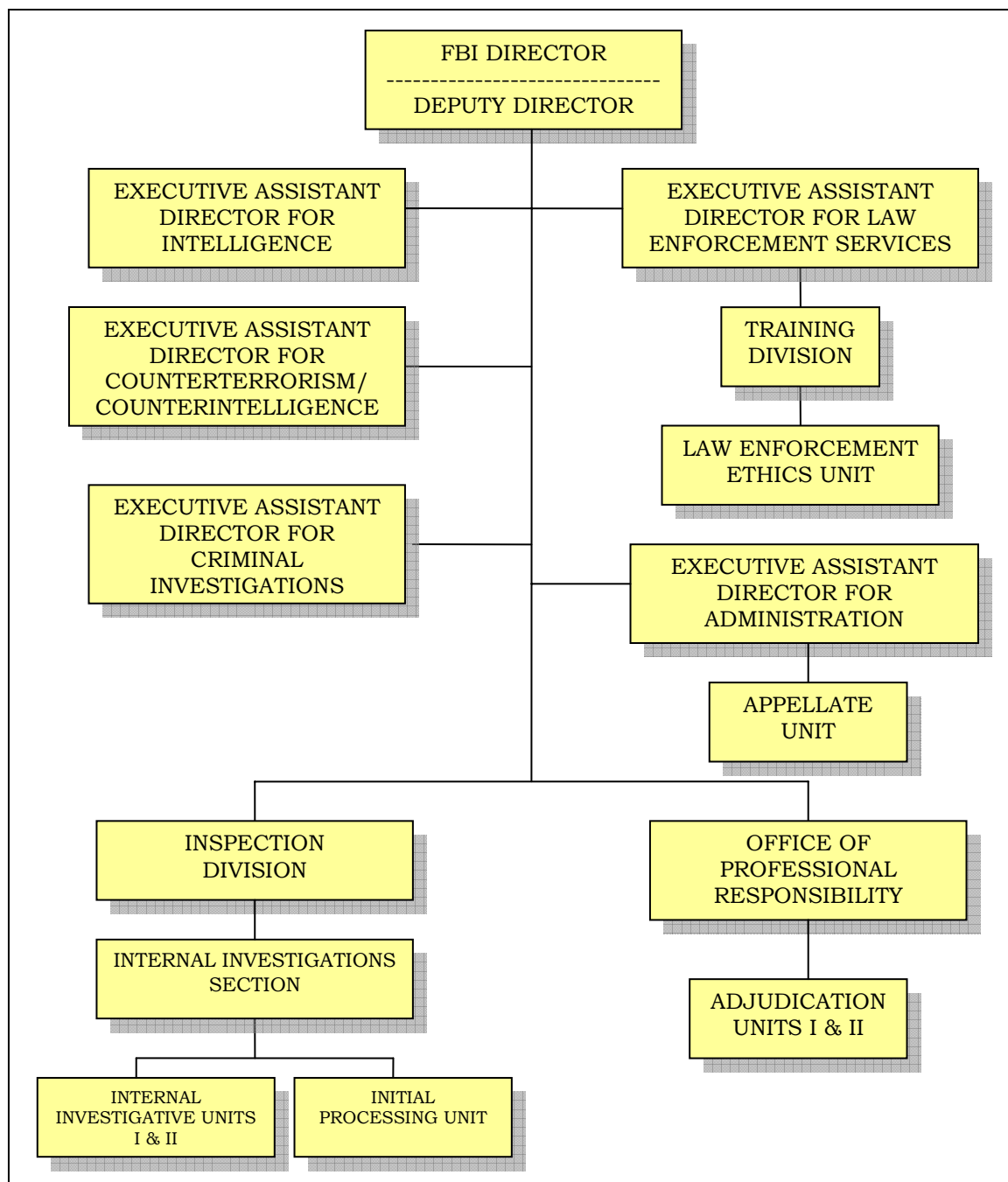
#### **IV. FBI Disciplinary Process**

The FBI's disciplinary process also plays an important role in promoting compliance with the Attorney General Guidelines. Unlike the Inspection Division, A/IU, and USOU, which affirmatively seek out compliance deficiencies through planned inspections or on-site reviews, the FBI's internal investigation caseload is normally generated by referrals of alleged employee misconduct to the Internal Investigations Section (IIS) of the Inspection Division. The IIS maintains the responsibility to investigate the allegation and to refer its findings to the Office of Professional Responsibility (OPR). If the allegations of misconduct are sustained, OPR has authority to impose disciplinary sanctions.

The following diagram shows the current structure of the FBI's disciplinary units.

**DIAGRAM 7.4**

**Organization Chart: FBI Disciplinary Units**



## **A. Investigative Guidelines Issues Addressed by the FBI Disciplinary Process**

Below we describe how the FBI disciplinary process addresses the Attorney General's Investigative Guidelines through its categorization of misconduct offenses. We also summarize the OPR cases that have involved violations of the Guidelines during the last five years.

### **1. Classification of Offenses**

The FBI evaluates allegations of misconduct according to a classification scheme that is based on a list of 63 offenses, known as "offense codes." Neither OPR nor the Units in the Internal Investigations Section (IIS) of the Inspection Division that investigate allegations of misconduct track as a discrete category violations of the Attorney General Guidelines. Two prior offense codes that recently were eliminated referred to the "AG Guidelines" in their titles: 18F – Informant/CW Matter – Violation of AG Guidelines; and 7F – Asset Matter – Violation of Executive Orders/AG Guidelines.<sup>381</sup> However, our review of misconduct cases under these and other offense codes revealed that Attorney General Guidelines' violations concerning informants were not consistently captured by the 18F classification. Officials at OPR (prior to its restructuring in 2004) could not explain why the two codes above contained express references to the Guidelines.

The FBI's new offense codes cover Attorney General Guidelines' violations in two ways: 1) by specifying types of conduct that are subject to the FBI disciplinary process; and 2) by identifying general categories of conduct standards the violation of which can result in disciplinary sanctions. With respect to the latter, three codes refer to operational guidelines such as the Attorney General Guidelines.<sup>382</sup>

---

<sup>381</sup> The 7F offense code addresses assets, or intelligence informants, rather than criminal informants. Assets are governed by another set of Attorney General Guidelines that were not examined in this review.

The FBI revamped its offense codes in the course of implementing recommendations contained in the February 2004 Bell-Cowell Commission report on ways to improve the FBI's disciplinary process. In response to the Bell-Colwell Commission's recommendations, the FBI reengineered OPR's organizational structure and procedures including separating its investigative and adjudicative functions by moving OPR's intake and investigations units to the Inspection Division, relocating the Law Enforcement Ethics Unit in the Training Division, and creating a revised set of offense codes and a consolidated set of penalty guidelines (Penalty Guidelines).

<sup>382</sup> These codes are: 1.5 Asset/CW/ Informant (Source) – Violation of Operational Guidelines and Policies, Other; 1.8 Investigative Deficiency – Violation of Operational Guidelines and Policies, Other; and 5.23 Violation of Miscellaneous Rules/Regulations. (continued)

## **2. Investigative Guidelines Violations Adjudicated by OPR from 1999 to 2004**

We reviewed OPR cases adjudicated from November 1999 to November 2004 to identify violations of Attorney General Guidelines. Out of approximately 1,500 cases in which OPR imposed discipline, we identified 24 cases that involved violations of the Confidential Informant Guidelines, 7 cases where agents initiated unauthorized investigations in violation of the General Crimes Guidelines, and 1 case where authorization was not obtained for a consensual monitoring in violation of the Consensual Monitoring Guidelines. Although several cases discussed misconduct that occurred during undercover operations, none of the infractions cited in those cases was a violation of the Undercover Guidelines.

With regard to violations of the Confidential Informant Guidelines, most of the cases involved multiple violations, including the following: improper personal relationship (10 cases); improper financial transactions (7 cases); wrongful disclosure of information (3 cases); failure to obtain proper authorization for otherwise illegal activity (3 cases); failure to obtain authorization for a privileged or sensitive source (2 cases); failure to witness confidential informant payments (2 cases); failure to conduct required background checks (2 cases); and failure to report unauthorized criminal activity (1 case). As explained in Section III above, the kinds of Guidelines violations adjudicated by OPR often are identified during Inspection Division inspections (and also were found in the OIG's review of FBI case files).

### **B. OIG Analysis**

Our review identified several issues concerning Guidelines-related misconduct that we believe warrant careful evaluation by the FBI: 1) the lack of clear standards regarding what Guidelines-related conduct should be referred to FBI Headquarters for evaluation of possible misconduct; 2) the associated issue concerning the distinction between "performance" and "misconduct;" and 3) the potential for disparate disciplinary treatment of Guidelines violations due to inadequate information retention, information sharing, tracking procedures, and technical support. In addition, we believe that certain violations of the Guidelines involving the operation of human sources merit elevated attention due to the seriousness of the conduct and should therefore be identified as discrete OPR offense codes.

---

The description of Code 1.8, for example, is "[k]nowingly or recklessly failing to enforce or comply with an FBI or Department of Justice (DOJ) operational guideline or policy, not specifically delineated in any other 'Investigative Deficiency' offense codes provided herein, which falls outside the parameters of performance."

## **1. Standards for Referral to the FBI Disciplinary Process**

Both the MIOG and Manual of Administrative Operations and Procedures require that allegations of “criminality or serious misconduct” be reported to FBI Headquarters.<sup>383</sup> While Part 263 of the MIOG lists a number of offenses that are considered serious misconduct, it provides little additional guidance as to when referrals to FBI Headquarters are appropriate. Our review of OPR adjudications over the past five years, Inspection Division inspection findings, and our own field work revealed that some actions that have been treated as misconduct by OPR, such as operating a privileged source without proper authorization, have been viewed by the field and the Inspection Division as not warranting referral for possible discipline. For example, in 2002 OPR disciplined an agent for failing to obtain proper authorization for a confidential informant’s participation in otherwise illegal activity and for failing to conduct proper background checks. However, the Inspection Division’s review in 2004 of five source files during one inspection revealed that the responsible Special Agents failed to obtain approval for the source’s participation in otherwise illegal activity and violated one or more Guidelines’ or MIOG requirements while operating the sources. Unlike the 2002 case, none of these matters was referred to OPR.

FBI managers recognize the need to ensure that the disciplinary process is both transparent and consistent. For example, the Chief of IIS told us that the MIOG and MAOP will be revised to include a reference to the FBI’s forthcoming manual on the disciplinary process and will provide guidance regarding when it is appropriate for field and Headquarters divisions to notify the Initial Processing Unit (IPU) about actual or potential misconduct. An Inspection Division official told us that SACs and other managers will be encouraged to report everything that could be deemed misconduct, and that the IPU will ensure consistency in its determinations regarding what is appropriate for investigation through development of a precedent database. We believe that such actions are warranted and that this FBI initiative could promote greater consistency in how violations of the Guidelines are treated.

### **“Performance” versus “Misconduct”**

An issue which creates uncertainty regarding which violations of the Attorney General Guidelines are subject to discipline is the distinction between “performance” and “misconduct.” Without clear and well-understood principles to guide application of this distinction, the disciplinary process will be less effective in promoting compliance with the

---

<sup>383</sup> See MIOG § 263-2; MAOP I § 13-2.



Attorney General Guidelines, and the FBI's disciplinary investigations and adjudications on this subject could produce inconsistent results.

Several of the FBI's offense codes refer to conduct "which falls outside the parameters of performance." For example, code 5.23 makes eligible for discipline an employee's failure "to enforce or comply with an FBI, DOJ, Office of Personnel Management, or other federal administrative or operational guidelines or policy not specifically delineated in any offense code, which falls outside the parameters of performance." Given the broad reach of this offense code, the distinction between performance and misconduct is critical to determining what behavior, including violations of the Attorney General Guidelines, is subject to discipline at the FBI. We believe that consistency would be enhanced if those codes that include the "which falls outside the parameters of performance" language were supplemented with examples demonstrating the difference between behaviors that are performance-based and others that constitute misconduct. As one FBI electronic communication stated with regard to the offense codes, "[b]y having clearly defined elements, employees and investigators will know what actions constitute misconduct, and will make the entire disciplinary process more transparent."

## **2. Additional Offense Codes**

We also recommend that several offense codes be added to the FBI's offense table to address conduct related to the operation of human sources that merits heightened scrutiny due to its seriousness and the frequency of deficiencies associated with them. These new codes would target misconduct related to informant participation in otherwise illegal activity and the authorization and operation of privileged or sensitive sources.

Our field work and examination of the results of the Inspection Division's inspection findings revealed that the failure by case agents to obtain proper authorization for otherwise illegal activity and for the handling of confidential informants identified in Section II.D of the Confidential Informant Guidelines (sensitive and privileged confidential informants), occurred with significant frequency. For example, Inspection Division inspections covering the last inspection cycle from May 2002 to October 2004 identified 38 case files showing that case agents failed to obtain proper authorization for confidential informants to engage in otherwise illegal activity, and 15 cases where agents operated sensitive or privileged sources without necessary authorizations.<sup>384</sup> We also identified cases where agents

---

<sup>384</sup> Because some Inspection Division inspection reports did not identify the case files where deficiencies were found, it is not possible to specify the total number of deficient files evaluated by the Inspection Division. For example, some inspection reports merely stated that a particular kind of deficiency occurred during the inspection period. In addition, even (continued)

failed to follow special handling procedures related to the operation of privileged or sensitive sources.

The FBI's current list of offense codes includes four conduct-based codes that reference human sources. These codes address the failure to report a source's criminal activity, engaging in improper personal or financial relationships with a source, and improperly intervening on behalf of a source with respect to law enforcement or legal obligations. The list does not include codes addressing the knowing or reckless (i) failure to obtain authorization for a source's participation in otherwise illegal activity; (ii) failure to obtain authorization for the operation of privileged or sensitive sources; and (iii) mishandling of privileged or sensitive sources.<sup>385</sup> While such conduct may be covered by a standard-based offense code, such as 1.5 ("Asset/CW/Informant – Violation of Operational Guidelines and Policies, Other), creating separate conduct-based codes would highlight the importance of avoiding these types of Guidelines violations and make the conduct codes concerning human sources more complete. The Confidential Informant Guidelines devote special attention to otherwise illegal activity and the handling of privileged and sensitive sources (see §§ II.D – Special Approval Requirements, and III.C – Authorization of Otherwise Illegal Activity) because of the seriousness of the conduct, the risks to prosecutions of informants and others, and the risks of liability to the United States. This justifies separate offense codes for misconduct involving authorization to participate in otherwise illegal activity, authorization for the operation of privileged or sensitive sources, and for the mishandling of such sources.

### **3. Technology and Information Dissemination**

We believe that the FBI's disciplinary units should develop electronic information retention, information sharing, and tracking procedures to ensure that disciplinary decisions, including those relating to Guidelines violations, are consistent and based on complete information. We learned that as of December 2004, adequate technology and support that would allow for the development and maintenance of upgraded precedent databases for Headquarters units involved in the FBI's disciplinary process were not in place, and it was unclear how case information was going to be shared and tracked. The FBI's Chief Information Officer (CIO) told us that,

---

in those circumstances where the case files were identified, the report did not indicate the number of violations found in the files.

<sup>385</sup> We believe that the new offense codes relating to privileged or sensitive sources should be limited to circumstances where the source is providing information based upon his/her privileged or sensitive status. Accordingly, we do not believe that a case agent's mishandling of an attorney informant who was providing information unrelated to legal matters should be covered by the new offense codes.

due to the antiquated nature of the computer system in use by OPR and IIS, it is very difficult and time-consuming to execute simple data manipulations, such as adding data fields.<sup>386</sup> FBI Headquarters officials told us that since that time both OPR and IIS have started to use a database that was developed by an SSA in the Inspection Division.

To ensure that information is not “stove-piped” in individual units involved in the FBI’s disciplinary process, resulting in inconsistent treatment of factors such as Attorney General Guidelines violations, we believe that the FBI’s internal discipline components should adopt procedures and shared technology that allow for retrieval of case information, precedents, and trend analyses.

### **C. Recommendations**

To ensure appropriate and consistent treatment of the Attorney General Guidelines in the FBI’s disciplinary process, we recommend the following.

(41) Ensure that alleged Attorney General Guidelines’ violations warranting potential discipline are referred to the FBI’s Internal Investigations Section in a consistent fashion throughout the FBI.

(42) Ensure that the Inspection Division’s standards for referring misconduct involving Attorney General Guidelines’ violations are consistent with practices adopted by the Internal Investigations Section.

(43) Add separate offense codes for: (i) knowingly or recklessly failing to obtain proper authorization for a source’s participation in otherwise illegal activity; (ii) knowingly or recklessly failing to obtain proper authorization to operate long term, high-level, privileged or media-affiliated confidential informants or other informants subject to special approval requirements; and (iii) knowingly or recklessly failing to operate long-term, high-level, privileged or media-affiliated confidential informants, or other informants subject to special approval requirements in accordance with the relevant Confidential Informant Guidelines and MIOG provisions.

---

<sup>386</sup> For example, the Office of the Chief Information Officer stated that it would take approximately two weeks to add a single data field to OPR’s case management system. However, that function was completed in a matter of seconds in a demonstration of IIS’s new database.

## **CHAPTER EIGHT**

### **HOW THE FBI IMPLEMENTED THE MAY 30, 2002, REVISIONS TO THE ATTORNEY GENERAL'S INVESTIGATIVE GUIDELINES**

In this review we assessed the FBI's compliance with the Attorney General Guidelines and the methods by which the FBI enforced compliance with the Guidelines. We also evaluated how the FBI implemented the revised Investigative Guidelines. The importance of the implementation process was highlighted by Attorney General Ashcroft when he issued the new Guidelines. In a memorandum to the heads of all DOJ components dated May 30, 2002, the Attorney General stated:

I hereby direct all affected components to implement these revised guidelines and procedures, and to incorporate them as relevant into their training programs for new and current personnel. The new tools made available by the guidelines will only be effective if our agents and employees know how to use them.

We believe it is important to evaluate how the FBI implemented the revised Guidelines because lessons learned from this process can be useful when future changes to Guidelines are made. As explained below, we found several significant deficiencies in the FBI's process for implementing the revised Guidelines.

#### **I. The FBI's Implementation Process for the Revised Investigative Guidelines**

To assess the procedures the FBI employed to implement the Investigative Guidelines, we interviewed FBI personnel, including representatives of the Office of the General Counsel (OGC), Inspection Division, and Training Division, and reviewed documents describing implementation activities. For example, we examined communications to FBI personnel relating to the May 2002 revisions and documents describing the FBI's plans for implementing the Guidelines. In addition, we reviewed reports, data, and other information provided to the Attorney General and DOJ components concerning the FBI's implementation activities.

Our review focused on four aspects of the FBI's implementation of the revised Guidelines: 1) initial planning; 2) communications and the provision of guidance to agents concerning the revisions; 3) training; and 4) administrative support. We summarize below our findings for each part of the implementation process.

##### **A. Planning for Implementation**

Our review found that components within the FBI did not sufficiently coordinate planning to implement the revised Guidelines. Although

Headquarters personnel told us that discussions occurred within various divisions and offices at FBI Headquarters regarding the need for new guidance and training, FBI officials told us that no office or entity provided coordinated oversight of the Guidelines implementation process.

Of all FBI components, OGC's role in the implementation process for the revised Guidelines was most prominent. It prepared guidance for the field and conducted some training sessions. See discussion in Sections II.B and C below. Without inter-division consultation and coordination, however, the implementation of the Guidelines proceeded in a patchwork fashion. For example, as we describe below, updating of the FBI's Manual of Investigative Operations and Guidelines (MIOG) was significantly delayed, and agent training needs were not timely identified and addressed.

## **B. Communication and Guidance**

OGC assumed responsibility for many of the communication-related tasks associated with notifying the field of the amendments to the Guidelines. On May 31, 2002, the day after the revised Guidelines were issued by the Attorney General and became effective, OGC e-mailed electronic copies of the four Investigative Guidelines to all Chief Division Counsel and announced plans to post the documents on the Investigative Law Unit's (ILU) Intranet website. The e-mail also explained that "ILU will be providing guidance regarding the implementation of the new guidelines in the near future." The FBI provided no other documentation to the OIG concerning its initial notification to its employees, such as a broadcast e-mail or posted Intranet announcement for all FBI agents.

From early June to October 2002, the FBI issued five sets of guidance documents concerning the revised Investigative Guidelines.<sup>387</sup> On June 11, 2002, the Undercover and Sensitive Operations Unit (USOU) in the FBI's Criminal Investigative Division (CID) issued an electronic communication to all field offices and divisions announcing approval of the revised Field Guide for Undercover and Sensitive Operations (Field Guide) that incorporated changes required by modifications to the Undercover Guidelines. The electronic communication provided a 5-page summary outlining 12 important policy changes, including increased monetary limits for Group II UCOs and emergency approval procedures.

---

<sup>387</sup> The electronic communications for consensual monitoring, confidential informants, and undercover operations indicate that the following enclosures were provided: the consensual monitoring electronic communication included a copy of the revised Consensual Monitoring Guidelines; the confidential informant electronic communication included a revised MIOG Part 137; and the undercover operations electronic communication included a copy of the revised Field Guide, which contains a copy of the Undercover Guidelines.

On July 5, 2002, OGC issued a 2-page electronic communication to all Divisions that described changes to the Consensual Monitoring Guidelines. On October 7, 2002, OGC sent a 15-page explanation to all divisions and Legats regarding the revisions to the General Crimes Guidelines. The electronic communication discussed changes to the major sections of the General Crimes Guidelines, including those addressing full investigations, racketeering enterprise investigations (REIs), terrorism enterprise investigations (TEIs), counterterrorism activities, and the dissemination of investigative information. With respect to counterterrorism activities involving visiting public places and events for the purpose of detecting or preventing terrorist activities, the guidance stated that, time permitting, agents should obtain their supervisor's approval for the visit and that no information collected should be retained unless it related to potential criminal or terrorist activity.

On August 6, 2002, the Criminal Intelligence Section issued to all field offices a 3-page explanation about the revisions to the Confidential Informant Guidelines. It described the changes to the Guidelines, including elimination of the requirements to read verbatim instructions to CIs and to obtain the CI's written acknowledgment that the CI had received the instructions.

The FBI's Counterterrorism Division issued an electronic communication to all field offices on August 8, 2002, concerning the initiation and renewal of TEIs. The guidance addressed issues such as predication standards and authorization levels and time periods. The Counterterrorism Division supplemented this guidance with an electronic communication to all field offices on January 2, 2003, describing the proper use of preliminary inquiries in TEIs.

Besides issuing explanatory electronic communications concerning changes to the Investigative Guidelines, the FBI took other steps to assist the field with interpreting the Guidelines and understanding related civil liberties issues. On March 27, 2003, OGC designated an attorney to coordinate guidance and assistance on investigative, operational, and policy matters concerning constitutional and privacy interests. The FBI also issued the following guidance documents (which are described more fully in Chapter Five):

- March 19, 2004, guidance emphasizing FBI policy regarding the protection of civil liberties in connection with use of authorities under both the Investigative Guidelines and the NSI Guidelines (OGC – "Protection of Civil Liberties");
- April 26, 2004, guidance clarifying the standards for collecting, retaining, and disseminating information in connection with the FBI's "Special Events" responsibilities (CTD – "Guidance to Atlanta, Boston and New York Divisions Concerning Information Collection,

Maintenance, and Dissemination for G-8, DNC and RNC Special Events, 2004”); and

- September 1, 2004, guidance emphasizing the limitations on the Part VI authorities and specifying how to collect, maintain, and disseminate the information collected in connection with protest activity (CTD – “Law Enforcement Monitoring of Protest Groups for Indications of Criminal or Terrorist Activity”).

Despite these and other guidance memoranda issued by FBI Headquarters, we found numerous instances where agents were not timely informed of Guidelines’ requirements. Furthermore, we identified problems in communication between FBI Headquarters and the field concerning the requirements of the new Guidelines. For example, our survey of Division Counsel indicated that 55 percent said they believed that guidance is not clear with respect to Section VI.A.2 of the General Crimes Guidelines.<sup>388</sup> Our survey of Confidential Informant Coordinators also revealed that 45 percent reported that communication breakdowns with FBI Headquarters regarding changed procedures resulting from the Guidelines revisions were a significant issue raised by agents in their respective field offices.

### **C. Training**

Our review of the FBI’s training initiatives on the Investigative Guidelines revealed inadequate planning and poor coordination between Headquarters Divisions, with the consequence that nearly two years after the Guidelines were revised, key groups within the FBI reported significant deficiencies in both the sufficiency and effectiveness of the available Guidelines training. Our interviews revealed that no entity in the FBI made a determination regarding which agents or supervisory personnel should receive training, the form it should take (e.g., classroom, training by Division Counsel, or the use of computer-assisted tools such as CD-ROMs), and when it should be completed.

Training for FBI agents is provided by various sources, including OGC, the Training Division, and field and Headquarters operating

---

<sup>388</sup> The comments of two Division Counsel are noteworthy. When asked what measures they believed should be taken to enhance compliance with the revised Investigative Guidelines, they responded:

- “[C]larity is needed from proposed/draft guidelines to the time they are enacted. This information seems to come in piecemeal.”
- “Provide examples and clear answers. For example, the most recent CDC conference in November 2003, someone from OGC regurgitated the brand new AG Guidelines. But when asked a very specific, no-wiggle-room question about visiting a mosque, we got a non-answer as to what to do.”

divisions.<sup>389</sup> The Training Division informed us that it does not maintain records on field or Headquarters training that does not involve Training Division resources. According to the Training Division, new agents receive copies of the Investigative Guidelines as well as instruction on Guidelines issues related to consensual monitoring, the operation of confidential informants, undercover operations, and investigative techniques. Guidelines instruction also is provided during in-service training at the FBI's training facility in Quantico, Virginia, in sessions for agents on domestic and international terrorism.

Chief Division Counsel in each field office also provide mandatory quarterly legal training for each field office. According to OGC, Guidelines issues are covered in this setting. However, OGC could not verify that the May 2002 revisions had been addressed by CDCs in all field offices. Moreover, CDCs did not themselves receive training on the revised Guidelines until a January 2003 CDC conference at FBI Headquarters.

Headquarters program units within the CID also provided training that addressed the Guidelines. For example, USOU provided Undercover Guidelines training on the Confidential Informant Guidelines in several courses that it sponsored as did the Asset/Informant Unit (A/IU).<sup>390</sup> Finally, a limited number of courses that address Guidelines issues are available to FBI personnel through DOJ's Office of Legal Education (e.g., Online Undercover Investigations Seminar).

Yet, despite this training activity, our survey of FBI personnel revealed significant gaps and inconsistencies in the sufficiency and effectiveness of Guidelines training. For example, our survey of Division Counsel in early 2004 showed substantial variation in the percentage of agents in field offices who had received general training on each of the four Investigative

---

<sup>389</sup> For example, by invitation from various FBI Headquarters and field components, OGC conducted more than 20 training sessions addressing Guidelines issues from June 2002 to June 2003.

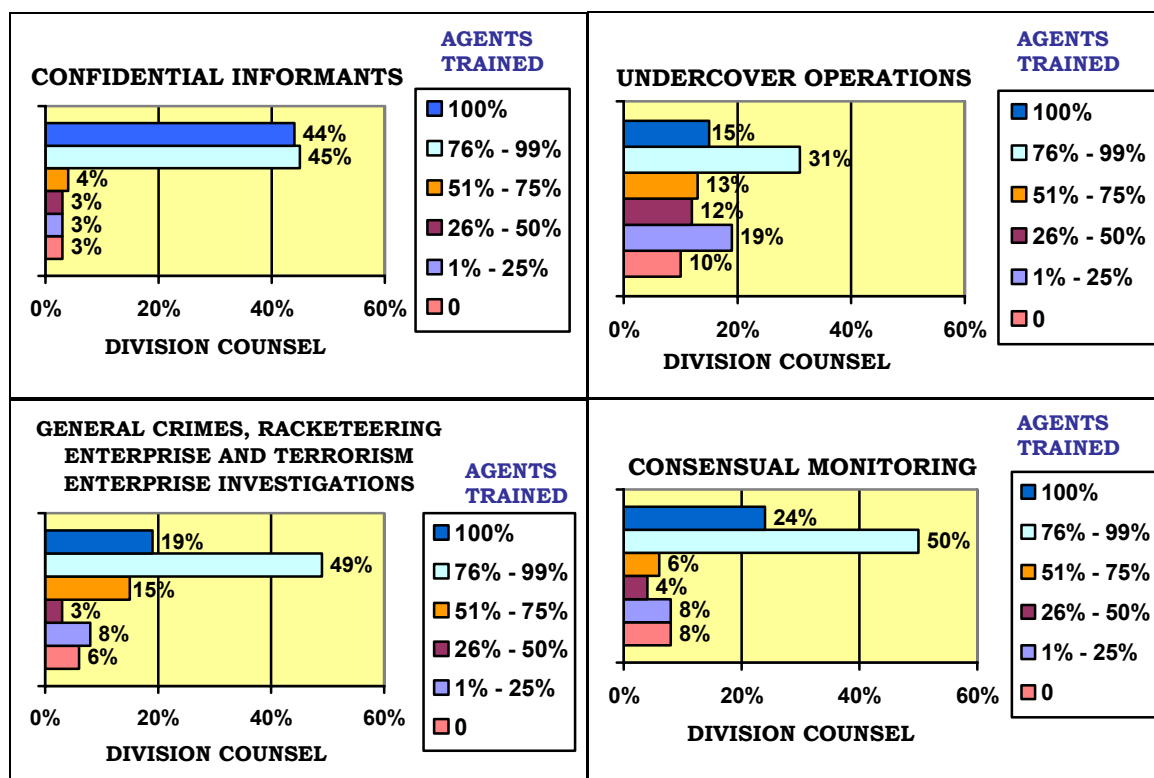
<sup>390</sup> According to the former Chief of the Criminal Intelligence Section (CIS), a project was initiated in November 2003 to provide FBI-wide "Back to Basics" training to all Special Agents, including managers, on the operation of human sources. All Informant Coordinators were provided a standard PowerPoint presentation to deliver to field agents. An instructional CD-ROM also was distributed that included a mandatory test. The former Section Chief explained that all FBI agents were trained the same way in approximately a 45-day period. He also stated that training is provided to the field through dissemination of Weekly Human Source Advisories, which discuss issues that come to the attention of the Informant Coordinators, such as the results of Inspection Division inspections. According to the former Section Chief, agents in the field find the MIOG to be a difficult source for answers and therefore very few agents consult the MIOG on informant issues. Instead, they consult with their Informant Coordinator, especially if they do not regularly operate informants.



Guidelines, apart from guidance provided by Division Counsel on particular cases. As shown below, only 19 percent of surveyed Division Counsel reported that all agents in their field office had received training on the General Crimes Guidelines (which includes the new anti-terrorism measures added with the May 2002 revisions), and 6 percent reported that no agents in their office had received such training. In addition, fewer than half of the respondents said that all agents in their respective field offices had received training on the revised Confidential Informant Guidelines.

**DIAGRAM 8.1**

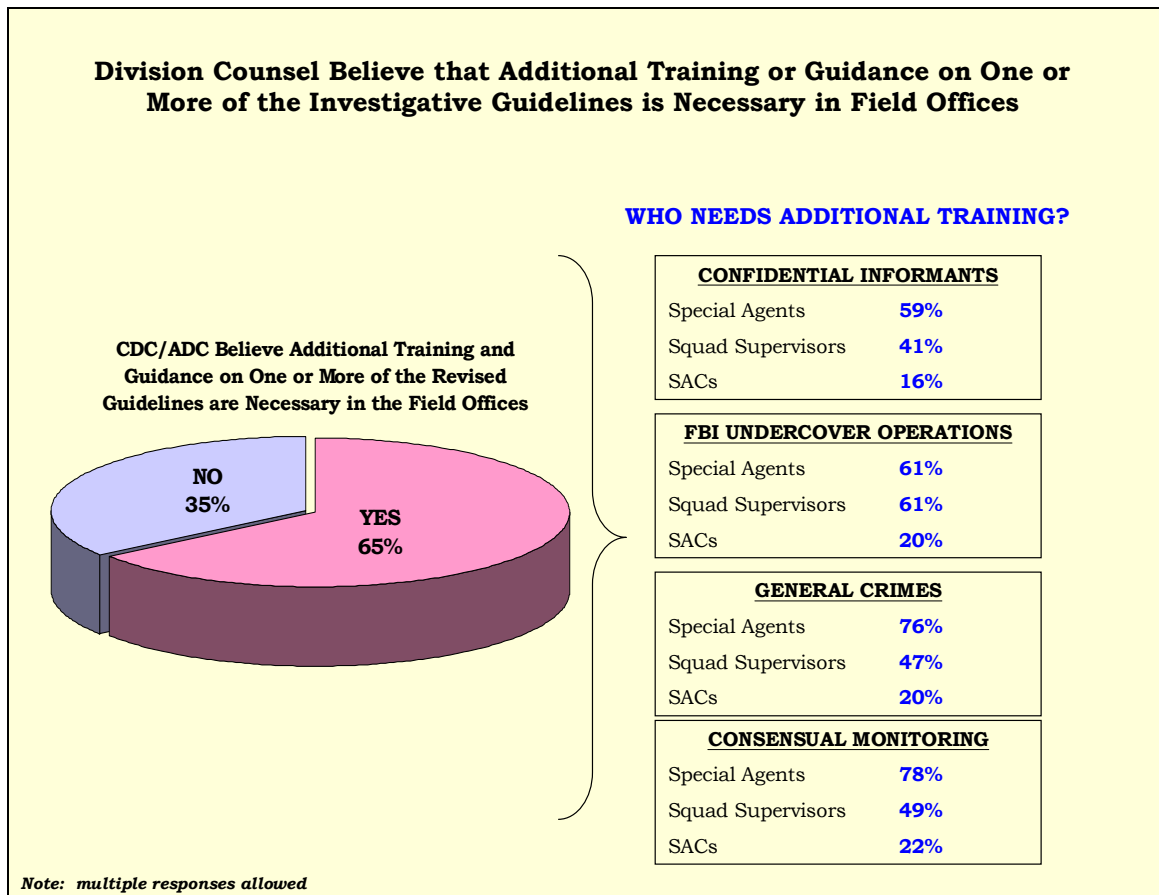
**Division Counsel Reporting of Special Agents who have Received Training on the Investigative Guidelines in Their Field Offices as of March 2004**



Our surveys further revealed that 65 percent of surveyed Division Counsel said they believed additional training or guidance on the revised Guidelines was necessary in their respective field offices. A high percentage of Division Counsel told us that agents and squad supervisors require additional training.

## DIAGRAM 8.2

### Division Counsel's Views on the Need for Investigative Guidelines Training

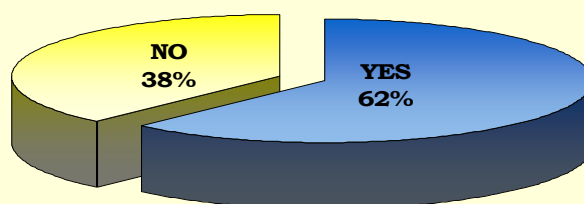


We also found that 63 percent of surveyed Division Counsel, 62 percent of Informant Coordinators, and 50 percent of surveyed Undercover Coordinators said they believed they needed additional training on the Investigative Guidelines. The diagram below summarizes the views of Informant Coordinators:

**DIAGRAM 8.3**

**Confidential Informant Coordinators' Views on the Need for Investigative Guidelines Training**

**Most Confidential Informant Coordinators Believe They Need Additional Guidelines Training**



**Type of Training Confidential Informant Coordinators Believe Would be Most Useful**

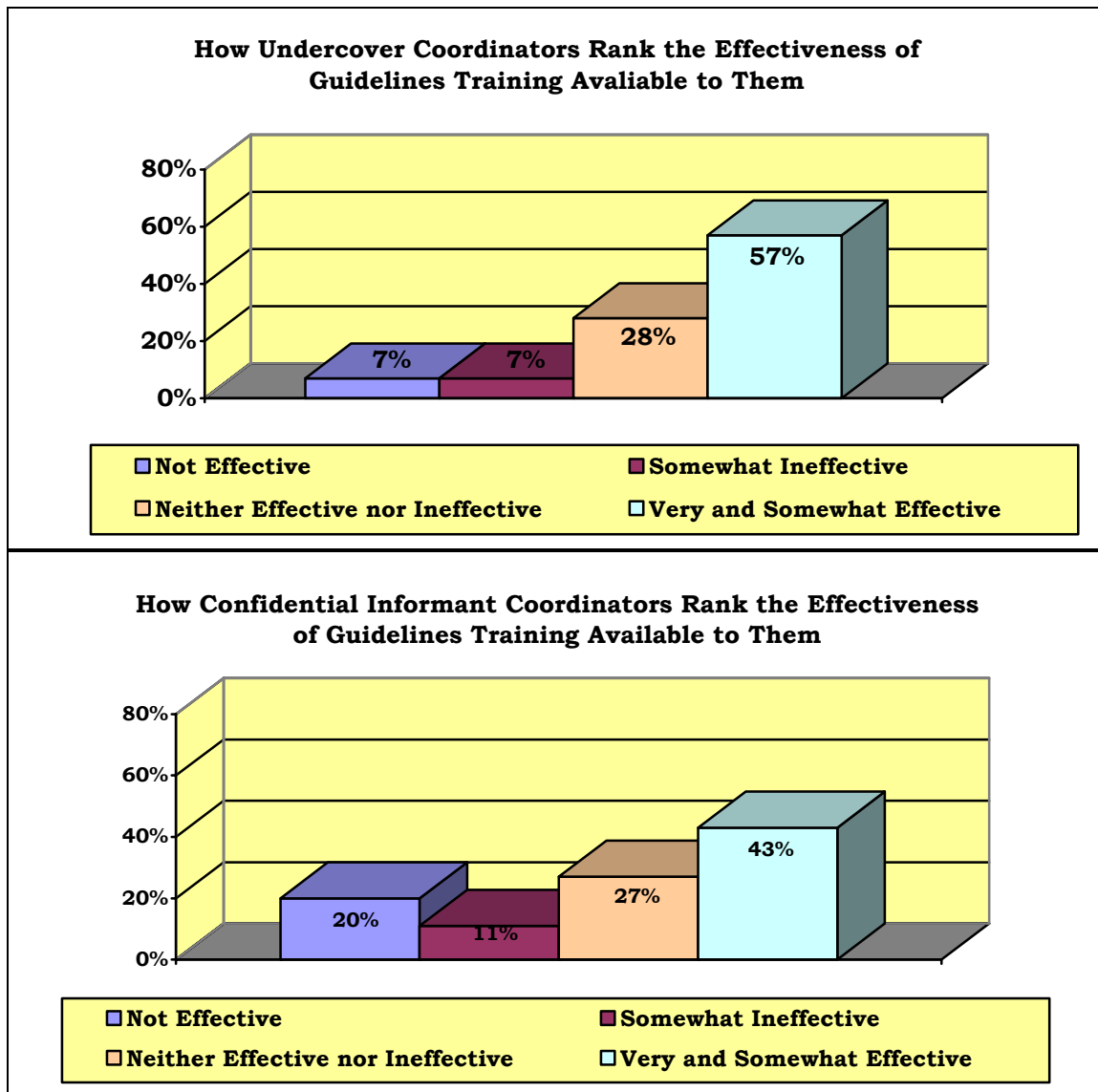
CIP Coordinator conferences	91%
Post answers to frequently asked questions on the Intranet	57%
Web-based courses	49%
Instructional CD-ROMs available at all field offices	40%
Quantico In-Service training	37%
Joint Training with the U.S. Attorneys' Offices	29%

*Note: multiple responses allowed*

The reported effectiveness of the Investigative Guidelines training received by Informant Coordinators, Undercover Coordinators, and Division Counsel since the May 2002 revisions also is noteworthy. As the following diagrams reveal, a far greater percentage of Informant Coordinators than Undercover Coordinators reported receiving Guidelines training that they deemed “not effective.”

**DIAGRAM 8.4**

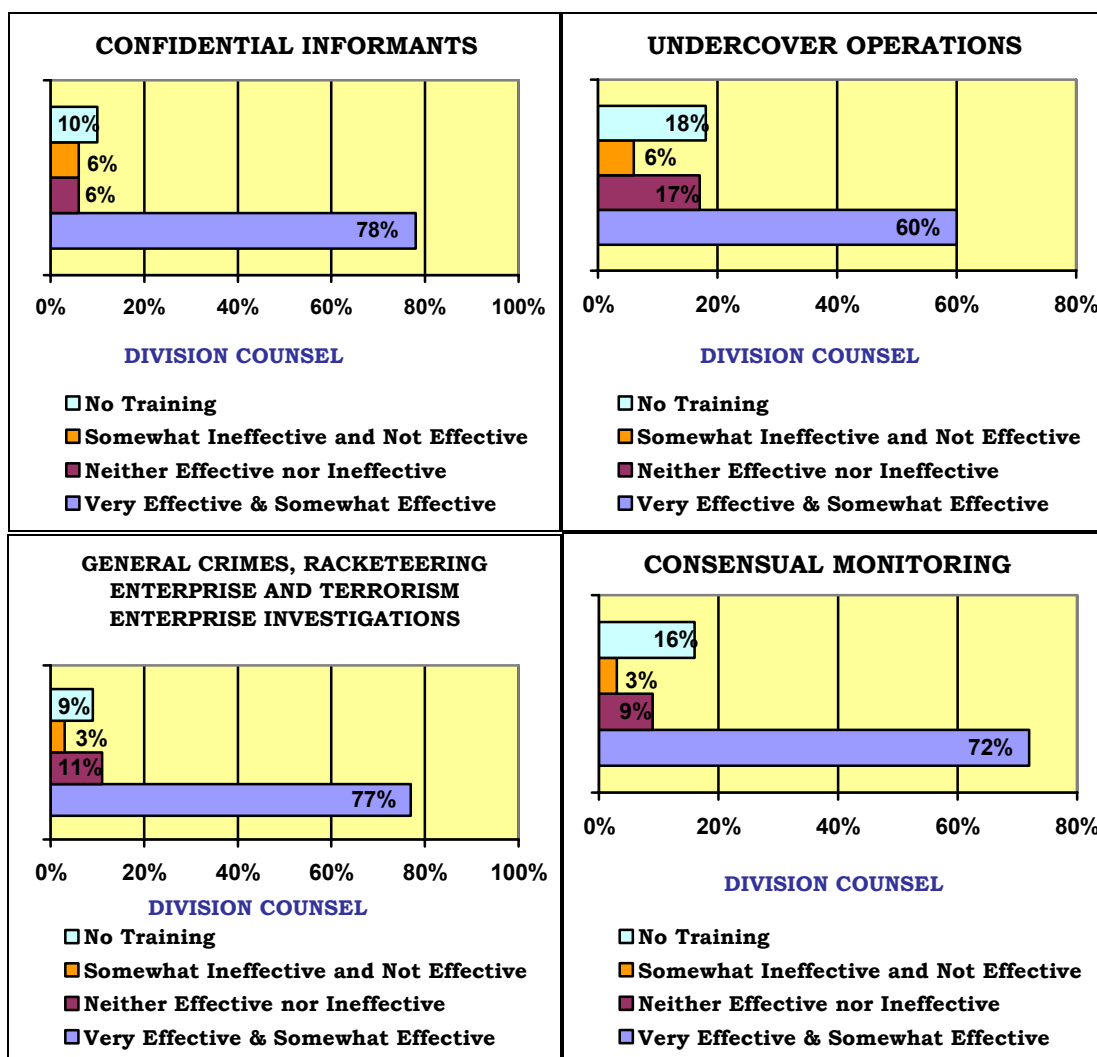
**Effectiveness of Training of Confidential Informant Coordinators and Undercover Coordinators on the Investigative Guidelines**



In addition, approximately 10 to 24 percent of surveyed Division Counsel reported receiving no training or ineffective training on each of the Guidelines in the first 21 months after the revised Guidelines were issued.

**DIAGRAM 8.5**

**Division Counsel's Views of the Effectiveness of Their Training on the Investigative Guidelines**



**D. Administrative Support, Including Mechanisms to Promote Accountability**

Compliance with regulations and policy requirements such as the Investigative Guidelines can be significantly enhanced through basic administrative measures, including use of accurate and up-to-date reference materials and standard forms, and adherence to procedures that ensure review by experienced personnel. As explained below, our review identified multiple deficiencies in the FBI's administrative support of the revised

Guidelines. These included year-long delays in updating the MIOG and other administrative materials used to promote adherence to the Guidelines.

The MIOG is the FBI's official reference guide on operational procedures. It is compiled by the Manuals Desk of the FBI's Records Management Division (RMD), which maintains the document in electronic format on the FBI Intranet. The Manuals Desk revises the MIOG periodically at the request of FBI components. When the Manuals Desk receives such a request, it logs the revision into SOFTBOOK, the mainframe automated manuals application. After SOFTBOOK assigns a manual change number to the electronic communication requesting the revision, Manuals Desk personnel edit, type, proofread, and correct the amendments prior to uploading them into SOFTBOOK. SOFTBOOK tracks the upload date, manual change number, responsible division, and history associated with each manual citation. The date of the electronic communication requesting a manuals change is reflected as the "effective date" of the change in the text of the MIOG. However, this is not the date the change is uploaded to SOFTBOOK. Documentation provided to the OIG by RMD shows that many changes took as long as a year or more to appear in the "official" downloadable MIOG text available to agents on SOFTBOOK.

According to RMD, electronic communications amending the MIOG to conform to the revised Guidelines were submitted by OGC on July 23, 2002, September 23, 2002, and April 4, 2003; by the CTD on June 3, 2003; and by the CID on August 6, 2002.<sup>391</sup> The FBI stated that SOFTBOOK uploads were completed for those five electronic communications on eight dates between April 2003 and July 2004.<sup>392</sup> SOFTBOOK upload dates do not appear anywhere in the text of the MIOG. Thus, RMD did not receive all requests for MIOG revisions until more than one year after the Guidelines were modified and did not complete all the necessary changes until more than two years after the revised Guidelines were issued.

In contrast, USOU posted revisions to its operations manual on the FBI Intranet soon after revision of the Guidelines. For undercover operations, agents typically refer to the Field Guide which is available on the FBI's Intranet. To incorporate changes prompted by the revised Guidelines, USOU submitted a revised Field Guide to the Investigative Technology Operations Division within two weeks of the effective date of the new changes, which then uploaded it on the FBI Intranet.

---

<sup>391</sup> The FBI also provided documents which showed that OGC submitted a manuals change electronic communication concerning the revised Guidelines to RMD on September 30, 2002, and that the CID did the same on January 3, 2003.

<sup>392</sup> There were significant delays with the SOFTBOOK uploads. The dates of the uploads were April 8, 2003, November 4, 2003, November 12, 2003, March 2, 2004, March 3, 2004, March 4, 2004, March 10, 2004, and July 12, 2004.

In addition to examining the timing of the revisions to the MIOG and Field Guide, we also compared their text with the Guidelines, noting omissions and differences in language. We identified nine significant discrepancies between the Guidelines and their corresponding sections of the MIOG or field guides that were available to the field from May 2002 to May 2004. These differences range from omissions of Guidelines' requirements to contradictions in language.

### **Confidential Informants**

- Registration of Confidential Informants. The Confidential Informant Guidelines identify seven categories of information that must be documented in a CI's files upon registration. The MIOG omits one of these requirements – the requirement to document the promises or benefits that are given to a CI by any prosecuting office.
- Contingency Payments to Confidential Informants. The Confidential Informant Guidelines provide that payments to a confidential informant shall not be contingent upon the conviction or punishment of any individual. Neither the MIOG nor the FBI's Confidential Funding Guide contains a corresponding provision.
- Deactivation of Confidential Informants. The Confidential Informant Guidelines establish procedures when a CI is deactivated "for cause or for any other reason." For CIs who are not deactivated "for cause," the MIOG does not include the notification and documentation requirements contained in the Guidelines.

### **Undercover Operations**

- Preparation of Undercover Employees, Informants, and Cooperating Witnesses. The Undercover Guidelines require the Special Agent in Charge (SAC) or Supervisory Special Agent (SSA) to review with an undercover employee the conduct that the undercover employee is expected to undertake, conduct that may be necessary during an operation, and any sensitive or fiscal circumstances that are reasonably likely to occur. The Field Guide omits the requirement to discuss sensitive or fiscal circumstances.
- Application/Notification to FBI Headquarters, Sensitive Circumstances. The MIOG omits the Undercover Guidelines' requirement that the letter from the "appropriate federal

prosecutor” that is included in the FBI approval package for Group I UCOs provide a cost/benefit statement.<sup>393</sup>

### **General Crimes, Racketeering Enterprise and Terrorism Enterprise Investigations**

- Authorizations for Openings and Renewals of Terrorism Enterprise Investigations. The General Crimes Guidelines provide that approval of initiations and renewals of terrorism enterprise investigations may be made by the SAC with notice to FBI Headquarters. The MIOG requires Headquarters approval for the initiation of TEIs by requiring concurrence of an appropriate Section Chief in the FBI’s Counterterrorism Division.<sup>394</sup>
- Use of Mail Covers in Preliminary Inquiries. The revised Guidelines authorize the use of mail covers in preliminary inquiries in general crimes investigations. The MIOG prohibits mail covers in these investigations.

### **Consensual Monitoring**

- Duration of Consensual Monitoring. We believe an ambiguity exists in the Consensual Monitoring Guidelines and MIOG regarding the authorization period for monitorings that do not involve the sensitive circumstances set forth in Section II.A of the Guidelines. For consensual monitorings that require DOJ approval, Section III.A.6 of the Consensual Monitoring Guidelines and the corresponding section of the MIOG (Part 2 § 10-10.3(9)(f)) impose a 90-day limit on authorizations. For non-sensitive matters, Section V of the Guidelines requires that the records for the monitoring include the information set forth in Section III.A, which provides that the request must “state the length of time needed for the monitoring” and establishes the 90-day authorization period described above (emphasis added). The MIOG provides, however, that in non-sensitive consensual monitorings,

---

<sup>393</sup> We construe the Undercover Guidelines’ requirement that this letter “include a finding” that the benefits of the undercover operation outweigh its costs as adding something more to the letter than that the prosecutor “agrees with the proposal and its legality.” As explained in Chapter Four, we found numerous instances when the authorization letter from the U.S. Attorney’s Office did not meet the requirements of the Guidelines.

<sup>394</sup> In Chapter Five, we discuss the Attorney General’s May 30, 2002, statements that the purpose of the Guidelines revisions delegating authority to field offices to approve TEIs was to eliminate “procedural red tape . . . [and to] free field agents to counter potential terrorist threats swiftly and vigorously without waiting for headquarters to act.” Remarks of Attorney General John Ashcroft (May 30, 2002).



the SAC or ASAC may approve the monitoring “for the duration of the investigation,” which, as explained in Chapter Six, the FBI has converted into a standard practice of authorizing non-sensitive monitorings for an extended period of time beyond 90 days.

- Emergency Procedures for Consensual Monitorings That Do Not Require DOJ Approval. The Consensual Monitoring Guidelines require the establishment of procedures for emergency authorizations in cases that do not require DOJ approval. The MIOG does not include such procedures.<sup>395</sup>

In addition to delays in revising the MIOG and these discrepancies, we encountered numerous instances where the administrative support the FBI provided to implement the Guidelines was outdated or inadequate. For example, some standard forms in use in the field offices we visited were not current and contained requirements that had been superseded by the 2002 revisions.

## **II. OIG Analysis and Recommendations**

Our review extended over a period of fundamental organizational change within the FBI in response to the terrorist attacks of September 11, 2001. Notwithstanding these significant challenges, we believe the May 2002 revisions to the Investigative Guidelines warranted more comprehensive implementation planning and training to ensure that they were effectively communicated to the field, understood, and followed.

Our review of the FBI’s actions following the May 2002 revisions to the Guidelines showed that the FBI did not provide sufficient training, guidance, administrative support, and oversight to ensure adequate implementation of the revised Guidelines. Although we found that some FBI components took important actions to implement the Guidelines, such as the Undercover and Sensitive Operations Unit and the Office of the General Counsel, taken as a whole, the FBI’s implementation process was insufficient.

In some respects, the FBI’s efforts were destined to fall short because it failed to develop even a rudimentary plan for how it intended to disseminate and implement the revised Guidelines. This occurred despite the FBI’s input on and prior knowledge of the impending Guidelines changes. We believe that someone at FBI Headquarters should have been assigned responsibility for overseeing implementation of the new Guidelines, in advance of their effective date.

---

<sup>395</sup> A table listing these discrepancies is attached as Appendix F.

Of all the implementation-related functions we examined, training on the revised Investigative Guidelines likely was hindered most significantly by the lack of inter-division coordination. For example, our interviews revealed that no entity in the FBI made decisions regarding the Guidelines training that should be provided throughout the FBI and the form it should take. As explained above, the Training Division does not have budgetary or operational authority over all training at the FBI, a fact which has been the topic of other reports critical of the FBI's training programs.<sup>396</sup> In 2001, DOJ commissioned a study of FBI management, which concluded as follows: "The FBI's training and development function is fragmented across the organization, resulting in confusion among employees, duplication of efforts, gaps in training offerings and inefficient use of resources."<sup>397</sup> Our review confirmed that training on the revised Investigative Guidelines suffered from similar deficiencies. Our surveys of FBI employees nearly two years after revision of the Guidelines showed that while 100 percent of agents in some offices had received training on individual Guidelines, agents in other offices had received no training, and most Informant Coordinators and Division Counsel believed that they, along with agents in their offices, still required additional training or guidance on the revised Guidelines.

We also found that certain of the FBI's administrative actions to support compliance with the Guidelines were outdated or otherwise deficient. For example, it took more than two years for the FBI to fully update the MIOG to account for the May 2002 Guidelines changes, even though the MIOG is the FBI's primary investigative resource manual. Moreover, during our field work in the summer 2004, we identified field-generated forms that field Divisions used to record information relevant to Guidelines compliance that were not current and that did not account for the May 2002 revisions.<sup>398</sup> When preparing for future Guidelines changes, the FBI should ensure that its resource manuals and supporting materials are updated promptly.

Moreover, our comparison of the Investigative Guidelines and FBI policy manuals identified several discrepancies. These included omissions from the MIOG that addressed the contents of informant files, informant deactivation procedures, and the preparation of undercover employees. We also identified a conflict between the General Crimes Guidelines and the MIOG concerning authorizations for terrorism enterprise investigations.

---

<sup>396</sup> See, e.g., Arthur Andersen, *Management Study of the Federal Bureau of Investigation* (December 14, 2001) at 159-160.

<sup>397</sup> *Id.* at 159.

<sup>398</sup> For example, as Table 3.7 in Chapter Three illustrates, 6 of the 12 field offices we visited during this review used one or more field-generated "ponies" or forms that failed to address important measures of the suitability of proposed confidential informants.

We learned in the course of our review that OGC distributed copies of the revised Guidelines to all Chief Division Counsel the day after they became effective and announced their upcoming availability on the FBI Intranet. Thereafter, OGC and other FBI Headquarters divisions disseminated guidance to the field describing the modifications to the Guidelines in a reasonably prompt fashion. The Undercover and Sensitive Operation Unit did an especially good job in this regard, and distributed its guidance and announced a revised version of its field guide addressing key interpretive questions less than two weeks after the revised Guidelines became effective.

However, the guidance with regard to certain of the new counterterrorism authorities in the General Crimes Guidelines was not sufficient. As we explained in Chapter Five, our survey of Division Counsel in the FBI's field offices revealed that guidance relating to Part VI, which authorizes the FBI to visit public places without particularized predication, was not timely and comprehensive. We found, for example, that 86 percent of Division Counsel said they had been consulted about whether it was permissible to retain information derived from the surveillance of or attendance at public events, and that 63 percent of those Division Counsel believed there was inadequate guidance about these matters when the revised Investigative Guidelines were issued. When we surveyed them 21 months after the revised Guidelines were issued, their views on the clarity of guidance improved only slightly to 55 percent.<sup>399</sup> Other communication gaps we identified appeared to have resulted from agents not knowing that guidance was issued or not consulting with others knowledgeable of the issues and current developments.

We recommend that the FBI take the following steps.

(44) Assign some person or unit at FBI Headquarters the responsibility to develop a plan to ensure proper and timely execution of future Attorney General Guidelines' revisions and to coordinate implementation of the revisions over time.

(45) Distribute revised Attorney General Guidelines to Chief Division Counsel, together with a concise summary or listing of the changes, sufficiently in advance of the new Guidelines' effective date to allow field personnel to familiarize themselves with the revisions and to allow those Headquarters and field personnel who provide training on the revisions to develop training materials and a schedule for providing training. In

---

<sup>399</sup> As we also described in Chapter Five, a far greater percentage of surveyed Division Counsel were satisfied with the quality of the guidance generally on privacy and civil liberties issues: 37 percent found the guidance "fully satisfactory," 34 percent found it "somewhat satisfactory," and only 9 percent found it either "somewhat unsatisfactory" or "not satisfactory."

addition, near the effective date of the revision, the FBI should develop and distribute standardized forms and other administrative support tools, issue field guidance, and identify a Headquarters point of contact who can address questions concerning the revisions.

(46) Ensure that revisions to the MIOG accurately reflect any changes to the Attorney General Guidelines and are made on or about the effective date of such changes.

(47) Make appropriate changes to the MIOG to reconcile the discrepancies between the Attorney General Guidelines and the MIOG that are identified in this report.<sup>400</sup>

---

<sup>400</sup> We understand that the discrepancies we identify in this report concerning the Confidential Informant Guidelines may be overtaken by proposed changes to the FBI's internal rules for handling all human sources, including confidential informants. The FBI should decide whether it nonetheless should revise the MIOG in the interim period before the Guidelines revisions are made.

[BLANK PAGE]

## **CHAPTER NINE**

### **CONCLUSION**

On May 30, 2002, the Attorney General announced revisions to four investigative Guidelines that govern virtually all aspects of the Federal Bureau of Investigation's (FBI) authority to investigate crimes committed by individuals, criminal enterprises and groups, as well as investigating those who may be threatening to commit crimes.

The FBI does not operate under a general legislative charter. Nor are some of its key investigative authorities, such as the use of informants, undercover techniques, or non-telephonic consensual monitoring activities, subject to statutory restrictions. Rather, these activities are governed and constrained by these Attorney General Guidelines.

Our review found that the FBI's compliance with these four Attorney General Guidelines varied considerably by program and field office. We found the most serious compliance problems in the FBI's Criminal Informant Program, particularly with respect to the Guidelines' provisions requiring periodic suitability evaluations of confidential informants; the timely communication of instructions to informants; and the authority of confidential informants to engage in otherwise illegal activity.

We believe the principal reasons for these compliance problems were inadequate administrative and technological support; the FBI's failure to hold first-line supervisors and case agents accountable for Guidelines violations; burdensome collateral duties assigned to many Confidential Informant Coordinators; and inadequate training for case agents, Supervisory Special Agents, Informant Coordinators, and Division Counsel. Particularly with regard to the Criminal Informant Program, the Guidelines violations we found were troubling and merit immediate attention.

To address these compliance problems, we believe the FBI should take a series of steps. First, it must ensure that agents understand the Informant Guidelines. It should also provide administrative and technological support to agents, including standardized forms, a field guide, and compliance checklists. Additional training on the Guidelines for Special Agents, Supervisory Special Agents, Confidential Informant Coordinators, and Division Counsel is also needed. In addition, the FBI should hold agents and their supervisors more accountable for non-compliance with the Guidelines. We concluded – and some senior FBI field managers we interviewed agreed – that frequently voiced concerns about the complexity and burdens of adhering to the Informant Guidelines would diminish if the FBI adequately implemented steps to support compliance in the field.

We believe these steps should be implemented regardless of whether the FBI continues to operate under the existing Confidential Informant Guidelines or if it modifies them in response to the ongoing effort to streamline its human intelligence program. Given the importance of the FBI's human intelligence program and the risks of violations of Guidelines' requirements, these steps should be taken regardless of the eventual placement or restructuring of the FBI's program for operating informants or other human sources.

In contrast to the Confidential Informant Guidelines, we found that the FBI generally was compliant with the Undercover Guidelines. The Headquarters unit supporting undercover operations was well managed and effective. It generated an up-to-date field guide and standardized forms, and it used technology, such as a centralized database which permits effective monitoring of undercover operations, to aid field office compliance with the Undercover Guidelines and Headquarters' oversight of the Guidelines.

However, we identified a limited number of undercover operations with authorization-related deficiencies and several noteworthy documentation-related errors, including failure to describe adequately authorizations of otherwise illegal activity and to document field management's oversight of undercover employees. We also believe the positive compliance record for criminal undercover operations could be improved further if agents participating in undercover operations coordinated more closely with Undercover Coordinators and Division Counsel.

Our analysis of the authorities contained in the Attorney General's Guidelines for General Crimes, Racketeering Enterprise and Terrorism Enterprise Investigations found that the FBI generally adhered to the provisions of these Guidelines. With respect to the conduct of preliminary inquiries, however, we found a notable failure to adhere to the requirement to document in a timely fashion the extension or closure of preliminary inquiries, or the conversion of a preliminary inquiry to a full investigation. We found general compliance with respect to the FBI's use of criminal intelligence investigations, though we identified certain documentation errors, especially as concerns notifications to DOJ and U.S. Attorneys.

We were unable to conduct a parallel compliance analysis of the FBI's use of its new authorities under Part VI of the General Crimes Guidelines. These Guidelines allow FBI agents to visit public places and attend public events for the purpose of detecting and preventing terrorist activities in the absence of particularized suspicion that a crime has been, is being, or is likely to be committed. Neither the Guidelines nor FBI policy require agents to obtain supervisory approval before engaging in such Part VI activities, and the methodology used for documenting

these visits and the information obtained from the visits does not generate easily retrievable information. As a result, we could not determine in this review if the FBI is using these Part VI authorities within the constraints of the Guidelines – including the prohibition on retaining information derived from these activities where no information indicating terrorist or criminal activity is obtained.

However, the FBI Headquarters and field personnel we interviewed expressed recognition of the civil liberties implications of the use of these Part VI authorities. We also found periodic guidance on this subject issued by FBI Headquarters and periodic communications between Headquarters and the field through the Headquarters point-of-contact on this issue whose position was established in April 2003.

A survey we administered found that 86 percent of surveyed FBI Division Counsel have been consulted about the propriety of retaining information derived from conducting surveillance of or visiting public places pursuant to these authorities. Yet, the same survey, taken 21 months after the Guidelines were issued, found that more than half of the surveyed Chief Division Counsel believed that the FBI's guidance on the use of Part VI authorities was unclear. We believe the FBI should develop additional guidance and procedures to ensure that these authorities – including restrictions on record retention, indexing, and dissemination – are used appropriately throughout the FBI and can be reviewed adequately.

With regard to the Guidelines for conducting non-telephonic consensual monitoring under the Attorney General's Procedures for Lawful, Warrantless Monitoring of Verbal Communications, we found the FBI was largely compliant. However, we found that 9 percent of the monitorings were recorded prior to obtaining the requisite approval.

Our review also examined the FBI's process for implementing the May 2002 revisions to the Attorney General Guidelines. We reviewed planning for implementation of the revised Guidelines, communication and guidance regarding the revisions, and training and administrative support for the revisions. We concluded that the FBI's implementation process was problematic. For example, no FBI official was responsible for ensuring that the need for training was adequately identified, that the FBI's administrative processes and forms used to support compliance with the Guidelines were updated in a timely fashion, and that sufficient guidance was provided on the revisions.

However, we did find that the Office of the General Counsel and the Undercover and Sensitive Operations Unit (USOU) in the Criminal Investigative Division communicated guidance and delivered training on the revised Guidelines. In addition, the Asset/Informant Unit (A/IU) initiated reinspections of field offices with exceptionally high



non-compliance in the Criminal Informant Program. We also found significant initiative and resourcefulness by some Informant Coordinators, Undercover Coordinators, and Division Counsel in developing individual field level “tickler” systems, checklists, manuals, and training to fill in the gaps left by the lack of adequate support for Guidelines compliance by FBI Headquarters. However, we believe the FBI should provide consistent administrative support and training and not depend upon the patchwork of individual initiatives that have emerged to fill these significant gaps.

Our review also analyzed the FBI’s internal enforcement mechanisms that promote compliance with the Investigative Guidelines. We found that the A/IU’s efforts from June 2003 through November 2004 (which were thereafter discontinued) to coordinate reinspections of field offices with high non-compliance rates were effective in improving compliance with the Confidential Informant Guidelines. We believe these reinspections should be reinstituted. We also found that the on-site reviews currently coordinated by the USOU for undercover operations highlight important compliance and performance issues, but should be more comprehensive in scope.

The FBI’s Inspection Division also plays an important role in promoting compliance with the Investigative Guidelines and in handling disciplinary matters arising from their violation. In its own inspections of field offices, the Inspection Division found many Guidelines violations. For example, with respect to the Criminal Informant Program, Inspection reports catalogued frequent failures to deliver timely instructions to confidential informants and less frequent failures either to obtain proper authorization for an informant to engage in otherwise illegal activity or to report unauthorized illegal activity. However, we identified gaps in the Inspection Division’s coverage of key Guidelines’ provisions in the Criminal Informant Program. We also found areas in which the Inspection process could be more effective if it were more aggressive in conducting follow up inspections when identified problems persisted, either within a field or Headquarters division or in particular programs.

Finally, we found that the joint FBI-DOJ committees that approve and provide oversight over certain informant and criminal undercover matters are generally functioning well and in accordance with their charters. The Criminal Undercover Operations Review Committee (CUORC) approves and monitors criminal undercover operations involving “sensitive” circumstances. The Confidential Informant Review Committee (CIRC) approves and monitors high level, long-term, “privileged” and media-affiliated confidential informants, and certain other types of informants. We found that both committees foster a candid exchange of information about the legal, practical, and prudential judgments regarding the use of informants and undercover operations,

and that both committees help to promote compliance with the Guidelines.

In sum, for nearly 30 years the Attorney General's Guidelines have provided direction to FBI employees in using their broad authorities to investigate crimes and threats of crime. The revisions to the Guidelines issued in May 2002 took into account the FBI's changed priorities by giving it additional authority to conduct more expansive investigations; delegating to field managers significant new authorities with respect to preliminary inquiries, criminal intelligence investigations, and undercover operations; reemphasizing the important constraints on the FBI's use of confidential informants; and authorizing visits to public places without particularized predication to address terrorist threats. But the use of these additional authorities must be in compliance with the Attorney General's Guidelines. We believe that our recommendations, if implemented, can help ensure that the FBI utilizes these additional authorities within the constraints of the Guidelines while also fulfilling its critical missions.

---

Date

---

Glenn A. Fine  
Inspector General