FEDERAL BUREAU OF INVESTIGATION
FOI/PA
DELETED PAGE INFORMATION SHEET
FOI/PA# 21-cv-2434

Total Deleted Page(s) = 8
Page 28 ~ b5 - 1; b7E - 4;
Page 29 ~ b5 - 1; b7E - 4;
Page 30 ~ b5 - 1; b7E - 4;
Page 31 ~ b5 - 1; b7E - 4;
Page 32 ~ b5 - 1; b7E - 4;
Page 33 ~ b5 - 1; b7E - 4;
Page 34 ~ b5 - 1;
Page 35 ~ b3 - 1; b5 - 1; b7E - 1;

XXXXXXXXXXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X For this Page X
XXXXXXXXXXXXXXXXXXXXXXXX

INSPECTION DIVISION
EXTERNAL AUDIT AND COMPLIANCE

COMPLIANCE AND MITGATION UNIT REPORT

DOMESTIC INVESTIGATIONS AND OPERATIONS GUIDE: AN AUDIT OF ASSESSMENTS AND INVESTIGATIONS OPENED BETWEEN 01/01/2015 and 06/30/2016

Nancy McNamara
Assistant Director
Inspection Division

TABLE OF CONTENTS

Contents

I. (U) EXECUTIVE SUMMARY 2

II. (U) SCOPE AND METHODOLOGY 4

III. (U) COMPLIANCE AREAS AND ERRORS 5

IV. (U) NON-COMPLIANCE ANALYSIS/TRENDS 9

V. (U) FIELD OFFICE COMPLIANCE ANALYSIS 11

VI. (U) CONCLUSION 14

VII. (U) OBSERVATIONS AND RECOMMENDATIONS 15

VIII. (U) LIST OF ATTACHMENTS 18

Attachment A: Inspection Staffing Roster

Attachment B: Abbreviations

Attachment C: Audit Questions

Attachment D: Assessments/Predicated Investigations Eliminated

21-CV-2434-671

I. (U) EXECUTIVE SUMMARY

(U) Following the signing of *The Attorney General's Guidelines for Domestic FBI Operations* (AGG-Dom) on 09/29/2008, the FBI published the Domestic Investigations and Operations Guide (DIOG) on 12/16/2008. The purpose of the DIOG was to standardize policy in criminal, national security, and foreign intelligence investigative activities. A major revision of the DIOG, with mandatory training, became effective on 10/15/2011. Subsequent updates were published on 06/15/2012, 10/16/2013, and 03/03/2016, with the most recent update published on 09/28/2016.

(U) The objective of the DIOG Audit was to review a representative sampling consisting of 1,679 investigative cases from all field offices opened between 01/01/2015 and 06/30/2016. Specifically, 945 Assessments and 699 Predicated Investigations were included in the sample. Thirty-five non-investigative cases were eliminated from the sample.

(U) In consultation with the Office of Integrity and Compliance (OIC) and the Internal Policy Office (IPO), three categories of DIOG compliance were selected to audit: a) Online Investigative Methods; b) Otherwise Illegal Activity (OIA); and c) Unauthorized Use of Investigative Methods.

(U) The audit topics were chosen based on several criteria, including OIC reports of violations of the DIOG, and DIOG-related Policy Guides. First OIC reviewed file 319O-HQ-A1561245-OIC and determined which DIOG non-compliance errors were most often reported by the field. For example, an error related to consensual monitoring documentation was found to be prevalent. Second, other topics were considered based on their new entries into the DIOG such as the recording of interviews and computer trespassing. Lastly, other topics were considered which had not been recently audited by INSD or any other entity. INSD, in correlation with OIC and IPO, selected topics which covered the spectrum of the DIOG; and no topic was weighted greater than another.

(U) A total of 1,679 Assessments and Predicated Investigations were audited for compliance, with 30 (1.8%) errors identified in 28 investigative cases. Two cases had two compliance errors each. Of the 30 compliance errors, sixteen (53.3%) were associated with Assessments; six (20.0%) were associated with Preliminary Investigations; and eight (26.7%) were associated with Full Investigations.

(U) Twenty-nine out of 30 compliance errors (96.7%) were found in the Unauthorized Use of Investigative Methods category. One compliance error (0.3%) was found in Otherwise Illegal Activity. There were no compliance errors found in the Online Investigative Methods category.

(U) Out of the 29 compliance errors found in the Unauthorized Use of Investigative Methods category, 16 (55.2%) were found in Assessments. All 16 of these errors were associated with the Physical Surveillance topic. Thirteen (81.3%) out of 16 errors were due to a lack of documented supervisor approval to initially conduct surveillance in an Assessment.

21-CV-2434-672

Three (18.7%) out of 16 errors occurred when the surveillance [redacted] b7E -4

(U) Fourteen (46.7%) out of the 30 total compliance errors were found to be associated with Predicated Investigations. Thirteen (43.3%) of the 30 total compliance errors were associated with the Unauthorized Use of Investigative Methods category. In this category, 11 (84.6%) out of 13 compliance errors were associated with the Consensual Monitoring topic. Five (45.5%) of the 11 errors found in this topic were due to the FD-472 (Consent to Record) form missing in both Sentinel [redacted] Five (45.5%) errors involved the FD-472 missing in Sentinel [redacted] and one (9.0%) error was due to a lack of supervisor approval to conduct consensual monitoring. b7E -3

(U) The remaining two (15.4%) out of 13 errors associated with Predicated Investigations also fell within the Unauthorized Use of Investigative Methods category. One was in the CCTV topic which involved an error due to a missing FD-759 (Notification of Authority Granted for Use of Electronic Monitoring Equipment-Not Requiring a Court Order) form. The other error occurred in the Surreptitiously Recorded Interviews topic due to a missing record of ELSUR evidence in the Sentinel file.

(U) One (3.3%), of the 30 total compliance errors was associated with the OIA category. This error was identified due to the lack of a documented request to conduct OIA.

(U) Overall, Criminal programs had the largest number of compliance errors with 12 (40%) out of 30; Intelligence programs accounted for eight (26.7%); Counterterrorism programs had five (16.7%); Counterintelligence programs had four (13.3%); and Cyber programs had one (3.3%).

21-CV-2434-673

II. (U) SCOPE AND METHODOLOGY

A. (U) Identification of Assessments/Predicated Investigations

(U) The representative sampling of 1,679 Assessments/Predicated Investigations was randomly selected from a total of 98,272 cases to provide a 95% confidence level with a 5% level of precision[1].

(U) During the audit, 35 (2.1%) of the total cases were eliminated for various reasons, including cases created for RMD bulk transfer to archive, internal investigations, enhanced security investigations and case consolidations. This resulted in 945 Assessments and 699 Predicated Investigations totaling 1,644 cases being audited. A complete listing of eliminated cases is included at Appendix D. The exact breakdown of the audited items is depicted in the chart below:

Table 1: Assessments and Predicated Investigations Audited

Assessments/ Predicated Investigations	Cases Audited
Type 1 Assessments	237
Type 3 Assessments	297
Type 4 Assessments	46
Type 5 Assessments	340
Type 6 Assessments	25
Preliminary Investigations	349
Full Investigations	350
Cases Eliminated	35
Total Cases Audited	**1,679**

B. (U) Methodology

(U) From 09/20/2016 – 09/28/2016, a team of 12 Assistant Inspectors-in-Place (AIIP) and one Auditor from various field offices and FBIHQ conducted the audit under the direction of the SC, External Audit and Compliance Section, the UC and SSA, Compliance and Mitigation Unit, two Office of Inspections Team Leaders (TL), one OGC attorney, two representatives from OIC, and two DIOG subject matter experts from IPO. All of the AIIPs previously received DIOG training and successfully passed the DIOG exam required following publication of the 10/15/2011 DIOG.

(U) A specific four step review process was used to identify any instances of non-compliance. The first step was identification of the potential compliance error by the AIIP. The second step was review of the potential compliance error by one of the TLs. The third step was

[1] The "level of precision" is known as the "margin of error." The margin of error shows how closely a sample size will predict results of an entire population. Standard statistical practice is 95%.

21-CV-2434-674

review by one of the IPO or OIC representatives to confirm the correct interpretation and application of the DIOG. The fourth step was a review by the SC, who subsequently sent an e-mail to the Division Compliance Officer (DCO) and CDC at the effected field office. The final review was conducted by the field office, as the e-mail requested the field office to provide a factual correction, if any such correction existed. An example of a factual correction would be a required approval found on a hard copy document not visible within Sentinel. All compliance errors documented during the audit went through the four steps described above.

III. (U) COMPLIANCE AREAS AND ERRORS

(U) The Assessments/Predicated Investigations audited were reviewed for compliance in three areas: a) Online Investigative Methods; b) OIA; c) and Unauthorized Use of Investigative Methods. The Unauthorized Use of Investigative Methods category had the following topics associated with it: Physical Surveillance; Surreptitiously Recorded Non-Custodial Interviews; Consensual Monitoring; CCTV; and Intercepting the Communications of a Computer Trespasser. Specifically, the audit questions were broken down as follows:

Table 2: Categories and Topics for Audit Questions

Audit Questions	Assessment	Predicated Investigation
Online Investigations	✓	✓
Otherwise Illegal Activity		✓
Unauthorized Use of Investigative Methods:		
◆ Physical Surveillance	✓	
◆ Surreptitiously Recorded Non-Custodial Interviews		✓
◆ Consensual Monitoring		✓
◆ Intercepting the Communications of a Computer Trespasser		✓
◆ CCTV		✓

(U) A total of 1,679 Assessments/Predicated Investigations were audited for compliance with 30 errors identified in 28 (1.7%) cases. Two Assessments/Predicated Investigations had two compliance errors each. Sixteen (53.3%) out of 30 compliance errors were associated with Assessments and 14 (46.7%) out of 30 compliance errors were associated with Predicated Investigations.

Table 3: Errors Identified by Investigation Type

Assessments/Predicated Investigations	Compliance Errors
Type 1 Assessments	5
Type 3 Assessments	6
Type 5 Assessments	5
Total Assessment Errors	**16**

21-CV-2434-675

Assessments/Predicated Investigations	Compliance Errors
Preliminary Investigations	6
Full Investigations	8
Total Predicated Investigation Errors	**14**
Total Errors	**30**

Table 4: Errors Identified by Category and Investigation Type

Assessments/Predicated Investigations	Online Investigative Methods	OIA	Unauthorized Use of Investigative Techniques	**Total Errors**
Type 1 Assessments			5	**5**
Type 3 Assessments			6	**6**
Type 5 Assessments			5	**5**
Total Assessment Errors	0	0	**16**	**16**
Preliminary Investigations			6	**6**
Full Investigations		1	7	**8**
Total Predicated Investigation Errors	0	**1**	**13**	**14**
Total Errors	**0**	**1**	**29**	**30**

(U//~~FOUO~~) For all types of compliance errors, DIOG, Section 2.8.1.1, defines Substantial Non-Compliance as "Non-Compliance that is of significance to the matter and is more than a minor deviation from a DIOG requirement. Non-Compliance that relates solely to administrative or peripheral requirements is not substantial." DIOG Section 2.8.1.2 defines "Other Non-Compliance" as non-compliance that is "not substantial." During the audit, an error was noted if there was noncompliance with the DIOG.

A. (U) Online Investigative Methods

i. (U) Analysis:

(U//~~FOUO~~) The DIOG, Appendix L, establishes policies for investigative methods conducted online by FBI employees. Appendix L states "This appendix only applies to investigative methods conducted online by FBI employees, as they are defined in DIOG Section 3. This appendix seeks to set out the standards for these investigative methods engaged in online by FBI employees in both affiliated and nonaffiliated capacities and in both public and private forums."

ii. (U) Compliance Errors:

(U//~~FOUO~~) There were no instances identified wherein an error was found in the Online Investigative Methods category during the review.

21-CV-2434-676

B. (U) OIA

i. (U) Analysis:

(U//~~FOUO~~) The DIOG, Section 17, establishes the standards for OIA. Section 17 states, "Otherwise Illegal Activity (OIA) is conduct in the course of duties by an FBI employee (to include an undercover employee (UCE)) or a confidential human source (CHS) which constitutes a crime under local, state, or federal law if engaged in by a person acting without authorization. Certain types of OIA cannot be authorized, such as participation in conduct that would constitute an unlawful investigative technique (e.g., an illegal wiretap) or participation in an act of violence. In this context, "participation in an act of violence" does not include acts taken in self-defense and defense of others by the FBI employee or CHS because such actions would not be illegal."

(U//~~FOUO~~) In addition, the DIOG defines the purpose and scope of OIA as follows, "The use of OIA may be approved in the course of undercover activities or operations that involve an FBI employee or that involve use of a CHS. When approved, OIA should be limited or minimized in scope to only that which is reasonably necessary under the circumstances including the duration and geographic area to which approval applies, if appropriate."

ii. (U) Compliance Errors:

(U) One of the 1,679 Assessments/Predicated Investigations audited, one was found to have a compliance error associated with OIA. The error was associated with a Full Investigation where a request to conduct OIA was not located in the file.

C. (U) Unauthorized Use of Investigative Methods

i. (U) Analysis

(U//~~FOUO~~) DIOG, Section 18, contains policies associated with Investigative Methods. Section 18.1.3 provides a general overview as follows: "The conduct of Assessments, Predicated Investigations (Preliminary Investigations and Full Investigations) and other activities authorized by the Attorney General's Guidelines for Domestic FBI Operations (AGG-Dom) may present choices between the use of different investigative methods (formerly investigative "techniques") that are each reasonable and effective based upon the circumstances of the investigation, but that are more or less intrusive, considering such factors as the effect on the privacy and civil liberties of individuals and the potential damage to reputation. The least intrusive method if reasonable based upon the circumstances of the investigation is to be used in such situations. However, the choice of methods is a matter of judgment. The FBI is authorized to use any lawful method consistent with the AGG-Dom, even if intrusive, where the degree of intrusiveness is warranted in light of the seriousness of a criminal or national security threat or the strength of the information indicating its existence, or in light of the importance of the foreign intelligence sought to the United States' interests. (AGG-Dom, Part I.C.2.) The availability of a particular investigative method in a particular investigation may depend upon the level of investigative

21-CV-2434-677

activity (Assessment, Preliminary Investigation, Full Investigation, and Assistance to Other Agencies)."

(U) Due to the broad range of investigative methods which can be used in investigations, the focus of the audit was narrowed down to Physical Surveillance used in Assessments, and Surreptitiously Recorded Non-Custodial Interviews, Consensual Monitoring, CCTV, and Intercepting the Communications of a Computer Trespasser used in Predicated Investigations.

ii. (U) Compliance Errors:

(U) Of the 1,679 Assessments/Predicated Investigations audited, 29 of the 30 errors identified during the audit occurred in the Unauthorized Use of Investigative Methods category. Sixteen of the 29 errors were related to Physical Surveillance used in Assessments. Specifically, 13 (81.2%) of the 16 Physical Surveillance errors occurred when there was a failure to obtain prior documented supervisor approval to conduct surveillance in an Assessment. Three (18.8%) of the 16 errors related to Physical Surveillance were encountered when the surveillance [redacted] b7E -4

(U) There was one error associated with Surreptitiously Recorded Non-Custodial Interviews topic due to the lack of an ELSUR evidence record in the file.

(U) The Consensual Monitoring topic within the Unauthorized Use of Investigative Methods category contained 11 compliance errors. Five were associated with an FD-472 (Consent to Record) missing in both Sentinel and [redacted] five were associated with an FD-472 located in [redacted] but missing from a Sentinel ELSUR subfile, and one was found to lack supervisor approval for consensual monitoring. b7E -3

(U//~~FOUO~~) DIOG Section 18.6.1.8.1 addresses [redacted] b7E -3,4

(U) CCTV was the only other Unauthorized Use of Investigative Methods topic to contain a compliance error. One error was found due to a missing FD-759.

(U) The following table contains the type of investigation associated with each error found in the Unauthorized Use of Investigative Methods category.

21-CV-2434-678

Table 5: Unauthorized Use of Investigative Techniques Errors by Investigation Type

Assessments/ Predicated Investigations	Physical Surveillance	Surreptitiously Recorded Non-Custodial Interviews	Consensual Monitoring – FD-472 Missing	Consensual Monitoring – FD-472 in [redacted] but not in Sentinel	CCTV – FD-759 Missing
Type 1 Assessments	5				
Type 3 Assessments	6				
Type 5 Assessments	5				
Total Assessment Errors	**16**				
Preliminary Investigations			3	2	1
Full Investigations		1	3	3	
Total Predicated Investigation Errors		**1**	**6**	**5**	**1**
Total Errors	**16**	**1**	**6**	**5**	**1**

b7E -3

IV. (U) NON-COMPLIANCE ANALYSIS/TRENDS

(U//~~FOUO~~) Of the total 1,679 audited Assessments/Predicated Investigations, 30 errors were identified in 28 Assessments/Predicated Investigations (Two Assessments/Predicated Investigations had two compliance errors) resulting in an overall error rate of 1.8%. The table below details the errors found by the type of investigation:

Table 6: Compliance Errors by Investigation Type

Assessments/Predicated Investigations	Online Investigative Methods	OIA	Unauthorized Use of Investigative Methods	**Total Errors**
Type 1 Assessments			5	**5**
Type 3 Assessments			6	**6**
Type 5 Assessments			5	**5**
Total Assessment Errors			**16**	**16**
Preliminary Investigations			6	**6**

21-CV-2434-679

Assessments/Predicated Investigations	Online Investigative Methods	OIA	Unauthorized Use of Investigative Methods	**Total Errors**
Full Investigations		1	7	**8**
Total Predicated Investigation Errors		**1**	**13**	**14**
Total Errors	**0**	**1**	**29**	**30**

Table 7: Details of Compliance Errors

Compliance Error	OIA	Unauthorized Use of Investigative Techniques
OIA – No request to conduct OIA	1	
Total OIA Errors	**1**	
Physical Surveillance:		
◆ No prior documented supervisor approval		13
◆ Surveillance in [redacted]		3
Total Physical Surveillance Errors		**16**
Surreptitious Interviews – no record of ELSUR evidence in the file		1
Total Surreptitiously Recorded Non-Custodial Interview Errors		**1**
Consensual Monitoring		
◆ No supervisor approval		1
◆ FD-472 missing in Sentinel [redacted]		5
◆ FD-472 in [redacted] but not in the Sentinel		5
Total Consensual Monitoring Errors		**11**
CCTV – missing FD-759		1
Total CCTV Errors		**1**
Total Errors	**1**	**29**

b7E -3,4

(U) The largest number of the 30 compliance errors fell within Criminal programs which had 12 (40%) out of 30; Intelligence programs accounted for eight (26.7%); Counterterrorism programs had five (16.7%); Counterintelligence programs had four (13.3%); and Cyber programs had one (3.3%). The following table depicts the compliance errors by Headquarters Division, Program, and Threat:

21-CV-2434-680

Table 8: Errors by Headquarters Division, Program and Threat

Headquarters Division	Program	Threat	OIA	Unauthorized Use of Investigative Methods
CD	CI	*Classified at higher level*		1
	CI	*Classified at higher level*		2
	CI	*Classified at higher level*		1
Total CD				**4**
CID	CR	CR		1
	CFC	FIF		1
	Latin American/ Southwest Border	TOC Mexico		1
	PC	Corruption of Domestic Public Officials		3
	PC	Violations of the Foreign Corrupt Practices Act and Antitrust		1
	VCAC	VCAC	1	3
	VC	Violent Gangs		1
Total CID			**1**	**11**
CTD	DT	All Other DT Threats		1
	DT	White Supremacy Extremists		1
	IT	AQAP		1
	IT	Homegrown Violent Extremists		2
Total CTD				**5**
CyD	Computer Intrusion	Cyber-Criminal		1
Total CyD				**1**
DI	Intelligence	Type 3		3
	Intelligence	Type 5		5
Total DI				**8**
Total Errors			**1**	**29**

V. FIELD OFFICE COMPLIANCE ANALYSIS

(U) Compliance errors were identified in 23 (41%) of the 56 field offices during the audit. New York, San Francisco, and Pittsburgh had three compliance errors each, and Sacramento had two compliance errors. The remaining 19 field offices had one error each. The table below provides details of each field office where a compliance error was found.

21-CV-2434-681

Table 9: Compliance Errors Identified by Field Offices

Field Office	Type	OIA	Unauthorized Use of Investigative Techniques	**Total Findings**
Albany	A5		1	**1**
Charlotte	Preliminary Investigation		1	**1**
Cleveland	Full Investigation		1	**1**
Detroit	A3		1	**1**
Honolulu	Full Investigation		1	**1**
Houston	Full Investigation		1	**1**
Jacksonville	Full Investigation		1	**1**
Kansas City	A5		1	**1**
Little Rock	A3		1	**1**
Los Angeles	Full Investigation		1	**1**
Miami	A5		1	**1**
Minneapolis	Preliminary Investigation		1	**1**
New Haven	Preliminary Investigation		1	**1**
New Orleans	Preliminary Investigation		1	**1**
New York	Full Investigation	1	2	**3**
Newark	Preliminary Investigation		1	**1**
Oklahoma City	Preliminary Investigation		1	**1**
Phoenix	A1		1	**1**
Pittsburgh	A1		3	**3**
Richmond	A3		1	**1**
Sacramento	A5 and A3		2	**2**
Salt Lake City	A3		1	**1**
San Francisco	A1, A3, and A5		3	**3**
Total Findings		**1**	**29**	**30**

(U) As detailed above, 29 of the 30 compliance errors identified during the audit occurred in the Unauthorized Use of Investigative Methods category. The following table shows each error broken down by field office.

21-CV-2434-682

Table 10: Unauthorized Use of Investigative Methods Errors by Field Office

Field Office	Physical Surveillance	Surreptitiously Recorded Non-Custodial Interviews	Consensual Monitoring – FD-472 or FD-759 Missing	Consensual Monitoring – FD-472 in [redacted] but not Sentinel	CCTV
Albany	1				
Charlotte			1		
Cleveland				1	
Detroit	1				
Honolulu			1		
Houston				1	
Jacksonville				1	
Kansas City	1				
Little Rock	1				
Los Angeles		1			
Miami	1				
Minneapolis			1		
New Haven					1
New Orleans			1		
New York			2		
Newark				1	
Oklahoma City				1	
Phoenix	1				
Pittsburgh	3				
Richmond	1				
Sacramento	2				
Salt Lake City	1				
San Francisco	3				
Total Findings	**16**	**1**	**6**	**5**	**1**

b7E -3

21-CV-2434-683

VI. (U) CONCLUSION

(U) INSD developed a methodology to audit a representative sampling of Assessments/ Predicated Investigations opened during the review period of 01/01/2015 through 06/30/2016. INSD conducted an audit of 1,679 Assessments/Predicated Investigations which included Assessments/Predicated Investigations from all 56 field offices. Each Assessment/ Predicated Investigation was reviewed and evaluated in three areas of DIOG compliance.

(U) The audit identified 30 total compliance errors. The most significant causes of non-compliance stemmed from field offices failing to follow DIOG procedures for conducting Physical Surveillance in Assessments, and for missing FD-472s when conducting Consensual Monitoring.

(U) The 12 errors in Criminal programs accounted for 40% of the 30 total compliance errors. Intelligence programs had the second highest number of errors with eight (26.7%) total.

(U) To mitigate these errors in the future, INSD makes the following Observations/ Recommendations.

21-CV-2434-684

VII. (U) OBSERVATIONS AND RECOMMENDATIONS

(U) **Observation 1:** Field offices failed to document approval to conduct surveillance in Assessments.

(U//~~FOUO~~) **Analysis 1:** DIOG Section 18.5.8.3.2 stated an FBI employee must use the FD-71 [redacted] or an EC [redacted] b7E -3,4

[redacted]

(U) INSD audited 945 Assessments and identified 16 (1.7%) instances of unauthorized surveillance. Of the 16 instances noted, five were in a Type 1, six were in a Type 3 and five were in Type 5 Assessments.

(U) **Recommendation 1:** [redacted] b5 -1

[redacted]

21-CV-2434-685

(U) **Observation 2:** Field offices did not document and file an FD-472 when conducting consensual monitoring.

(U//~~FOUO~~) **Analysis 2:** DIOG Section 18.6.1.8.1 [redacted] b7E -3,4

[redacted]

(U) INSD audited 699 Predicated Investigations and identified 11 (1.6%) instances where an FD-472 was missing. In six of the 11 instances, the FD-472 was not found in Sentinel [redacted] In five of the 11 instances, the FD-472 was found in [redacted] but not in Sentinel.

(U) **Recommendation 2a:** [redacted]

(U) **Recommendation 2b:** [redacted] b5 -1 b7E -4

21-CV-2434-686

(U) **Observation 3:** DIOG, Appendix L, 4.6.2 did not address "screenshots" related to real-time online communications and whether they require consensual monitoring authority to record.

(U//~~LES~~) **Analysis 3:** DIOG, Appendix L, Section 4.6.2 stated, "Significant amounts of real-time online communications are private communications (e.g., instant messaging or restricted chat rooms) requiring consensual monitoring authority to record. The AGG-Dom limits the use of consensual monitoring to predicated cases. [redacted] b7E -4

[redacted]

(U) **Recommendation 3:** [redacted] b5 -1

[redacted]

21-CV-2434-687

VIII. (U) LIST OF ATTACHMENTS

Attachment A: Inspection Staffing Roster

Attachment B: Abbreviations

Attachment C: Audit Questions

Attachment D: Assessments/Predicated Investigations Not Audited

21-CV-2434-688

Attachment A: Inspection Staffing Roster

Section Chief
James C. Langenberg (INSD)

Compliance and Mitigation Unit (CAMU)
[redacted] (INSD)
[redacted] (INSD)
[redacted] (INSD)
[redacted] (INSD)
[redacted] (INSD)

b6 -1
b7C -1

Team Leaders
[redacted] (EP) - CAMU
[redacted] OM) – Office of Inspections
[redacted] (NY) – Office of Inspections

Assistant Inspectors-in-Place
[redacted] TP
PH
[redacted] JN
[redacted] AT
[redacted] IR
MM
[redacted] HO
[redacted] WMD
[redacted] IR
[redacted] WF
[redacted] SJ
[redacted] LS

21-CV-2434-689

Attachment B: Abbreviations

The following abbreviations are utilized in the body of inspection reports:

A/	Acting
AD	Assistant Director
ADC	Associate Division Counsel
ADD	Associate Deputy Director
ADIC	Assistant Director in Charge
AFOSI	Air Force Office of Special Investigations
AG	Attorney General
AGG	Attorney General Guidelines
AIIP	Assistant Inspector-in-Place
AIS	Analytical Integrity Standards
ALAT	Assistant Legal Attaché
AOB	Average on Board
AOR	Area of Responsibility
ASAC	Assistant Special Agent in Charge
ASC	Assistant Section Chief
ATF	Bureau of Alcohol, Tobacco, Firearms, and Explosives
AUSA	Assistant United States Attorney
CAM	Collection Awareness Message
CAP	Collection Action Plan
CBP	US Customs and Border Protection Agency
CD	Counterintelligence Division
CDC	Chief Division Counsel
CDefC	Cleared Defense Contractors
CFC	Complex Financial Crime
CFCP	Complex Financial Crime Program
CHS	Confidential Human Source
CHSC	Confidential Human Source Coordinator
CHSPG	Confidential Human Source Police Implementation Guide
CI	Counterintelligence
CIA	Central Intelligence Agency
CID	Criminal Investigative Division
CIO	Chief Information Officer
CIP	Computer Intrusion Program
CIRG	Critical Incident Response Group
CJIS	Criminal Justice Information Services Division
CMC	Crisis Management Coordinator
COB	Close of Business
CollMC	Collection Management Coordinator
CPD	Corporate Policy Directive
CPN	Corporate Policy Notice
CPO	Corporate Policy Office
CRO	Chief Reports Officer

CR	Civil Rights
CRP	Civil Rights Program
CS	Computer Scientist
CSCC	Central Strategic Coordinator Component
CSG	Consolidated Strategy Guide
CSO	Chief Security Officer
CT	Counterterrorism
CTD	Counterterrorism Division
CTP	Counterterrorism Preparedness
CyP	Cyber Program
CyD	Cyber Division
CTT	Cyber Threat Team
DAD	Deputy Assistant Director
[redacted]	b7E -6
DCO	Division Compliance Officer
DD	Deputy Director
DEA	Drug Enforcement Administration
DHS	Department of Homeland Security
DI	Directorate of Intelligence
DIA	Defense Intelligence Agency
DIN	Domain Intelligence Note
DIOG	Domestic Investigations and Operations Guide
DLAT	Deputy Legal Attaché
DMC	Domain Management Coordinator
DO	Director's Office
DOD	Department of Defense
DOE	Department of Energy
DOJ	Department of Justice
DOR	Depth of Review
DPD	Division Policy Directive
DT	Domestic Terrorism
DTA	Division Threat Analysis
DTO	Drug Trafficking Organization
DTP	Domestic Terrorism Program
[redacted]	b7E -3
EAD	Executive Assistant Director
EC	Electronic Communication
ECPA	Electronic Communications Privacy Act
ECT	Evidence Control Technician
[redacted]	b7E -6
ELSUR	Electronic Surveillance
EM	Executive Management
E-mail	Electronic Mail
EOD	Enter On Duty
ERT	Evidence Response Team
FACE	Freedom of Access to Clinic Entrances

 b6 -1 b7C -1

FAM	Federal Air Marshal
FATG	Fraud Against the Government
FBI	Federal Bureau of Investigation
FBIHQ	FBI Headquarters
FCI	Foreign Counterintelligence
FD	Finance Division
FI	Full Investigation
[redacted]	b7E -3
FIF	Financial Institution Fraud
FIG	Field Intelligence Group
FISA	Foreign Intelligence Surveillance Act
FISAMS	Foreign Intelligence Surveillance Act Management System
FISC	Foreign Intelligence Surveillance Court
FLSD	Facilities and Logistics Services Division
FM	Financial Manager
FO	Field Office
FOASR	Field Office Annual Source Reporting
FOI	Field Office Inspection
FOIA	Freedom of Information Act
FOSP	Field Office Strategic Plan
FPO	Federal Prosecuting Official
FSL	Funded Staffing Level
FTR	Federal Travel Regulations
FY	Fiscal Year
GAGAS	Generally Accepted Government Auditing Standards
G/CEP	Gang/Criminal Enterprise Program
GPC	Government Purchase Card
HCF	Health Care Fraud
HIDTA	High Intensity Drug Trafficking Area
HRD	Human Resources Division
HQC	Headquarters City
HSI	Homeland Security Investigation
HUMINT	Human Intelligence
IA	Intelligence Analyst
IB	Intelligence Bulletin
IDQ	Intelligence Directed Query
[redacted]	
IG	Inspector General
I/Is	Indictments/Informations
IIC	Inspector-in-Charge
IINI	Innocent Images National Initiative
IIR	Intelligence Information Report
IM	Intelligence Memo
IN	Intelligence Note
INSD	Inspection Division
IOB	Intelligence Oversight Board

IOD	International Operations Division
IP	Intelligence Program
IPC	Intelligence Program Coordinator
IPM	Intelligence Program Manager
IPO	Internal Purchase Order
IPR	Intellectual Property Rights
IRAM	Inspection Risk Assessment Matrix
IS	Intelligence Study
ISPs	Internet Service Providers
IT	International Terrorism
ITP	International Terrorism Program
ITSD	Information Technology Services Division
JTTF	Joint Terrorism Task Force
LD	Laboratory Division
LEGAT	Legal Attaché
LLD	Less Lethal Device
LOA	LEGAT Operations Assistant
LSRT	Laboratory Shooting Reconstruction Team
MAOP	Manual of Administrative Operations and Procedures
MAPA	Management and Program Analyst
MIOG	Manual of Investigative Operations and Guidelines
MOU	Memorandum of Understanding
NA	FBI National Academy
NAACP	National Association for the Advancement of Colored People
NASA	National Aeronautics and Space Administration
NCIS	Naval Criminal Investigative Service
NJTTF	National Joint Terrorism Task Force
NPR	National Program Review
NSA	National Security Agency
NSB	National Security Branch
NSL	National Security Letter
NSLB	National Security Law Branch
[redacted]	b7E -5
NTPs	National Threat Priorities
OC	Organized Crime
OCP	Organized Crime Program
OCA	Office of Congressional Affairs
OCDETF	Organized Crime Drug Enforcement Task Force
OCKO	Office of the Chief Knowledge Officer
OEEOA	Office of Equal Employment Opportunity Affairs
OGA	Other Government Agency
OGC	Office of the General Counsel
OIA	Otherwise Illegal Activity
OIC	Office of Integrity and Compliance
OIG	Office of the Inspector General
OLEC	Office of Law Enforcement Coordination

OPA	Office of Public Affairs
OPR	FBI - Office of Professional Responsibility
Op Order	Operations Order
OST	Operational Support Technician
OTD	Operational Technology Division
PAL	Prioritized Action List
PAR	Performance Appraisal
PC	Public Corruption
PCHS	Potential Confidential Human Source
PCIR	Public Corruption Information Report
PCOR	Program Coordinator
PCP	Public Corruption Program
PFI	Principal Firearms Instructor
PI	Preliminary Investigation
PIOB	Potential Intelligence Oversight Board
PM	Program Manager
[redacted]	b7E -5
QSSR	Quarterly Supervisory Source Report
RA	Resident Agency
RCFL	Regional Computer Forensics Laboratory
RFI	Request For Information
RIP	Recruitment in Place
RMA	Resource Management and Allocation
RMD	Records Management Division
RPO	Resource Planning Office
RO	Reports Officer
SA	Special Agent
SABT	Special Agent Bomb Technician
SAC	Special Agent in Charge
SAS	Supervisory Administrative Specialist
SC	Section Chief
SCI	Sensitive Compartmented Information
SCIF	Sensitive Compartmented Information Facility
SDR	Source Directed Requirement
SecD	Security Division
SES	Senior Executive Service
SETA	Special Event Threat Assessment
SFOS	Supervisory Financial Operations Specialist
SIA	Supervisory Intelligence Analyst
SIOC	Strategic Information and Operations Center
[redacted]	
SIR	Situational Information Report
SIRG	Shooting Incident Review Group
SIRT	Shooting Incident Review Team
SITREP	Situational Report
SME	Subject Matter Expert

SMS	Strategy Management System
SOG	Special Operations Group
SOP	Standard Operating Procedure
SOS	Staff Operations Specialist
SPC	Strategic Partnership Coordinator
SPS	Strategy Performance Session
SSA	Supervisory Special Agent
SSG	Special Surveillance Group
SSIA	Senior Supervisory Intelligence Analyst
SSRA	Supervisory Senior Resident Agent
SSTF	Safe Streets Task Force
STTF	Safe Trails Task Force
SWAT	Special Weapons and Tactics
TD	Training Division
TDY	Temporary Duty
TF	Task Force
TFA	Task Force Agent
TFO	Task Force Officer
TMS	Threat Mitigation Strategy
TMT	Threat Mitigation Team
TOC-E	Transnational Organized Crime - Eastern
TOC-W	Transnational Organized Crime - Western
TPD	Third Party Draft
TRIP	Travel Request Initiation & Payment
TRP	Threat Review and Prioritization
TS	Top Secret
TSC	Terrorist Screening Center
TSL	Target Staffing Level
TTP	Tactical Targeting Package
TURK	Time Utilization Record Keeping
UC	Unit Chief
UCE	Undercover Employee
UCO	Undercover Operation
UDP	Undisclosed Participation
UIA	Unauthorized Illegal Activity
U.S.	United States
USA	United States Attorney
USAO	United States Attorney's Office
USG	United States Government
USIC	United States Intelligence Community
USMS	United States Marshals Service
USPER	US Person
USSS	United States Secret Service
VC	Violent Crime
VCAC	Violent Crimes Against Children
VCP	Violent Crimes Program

VCTF	Violent Crimes Task Force
VCT	Violent Criminal Threat
VCTP	Violent Criminal Threat Program
WCC	White Collar Crime
WCCP	White Collar Crime Program
WG	Working Group
WMD	Weapons of Mass Destruction
WMDD	Weapons of Mass Destruction Directorate
WMDP	Weapons of Mass Destruction Program