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

Total Deleted Page(s) = 30
Page 31 ~ b5 - 1; b7E - 4;
Page 32 ~ Duplicate;
Page 33 ~ b5 - 1;
Page 34 ~ b5 - 1; b7E - 4;
Page 35 ~ b5 - -1;
Page 36 ~ b5 - 1; b7E - 4;
Page 37 ~ b5 - 1; b7E - 4;
Page 38 ~ b5 - 1;
Page 39 ~ b5 - 1;
Page 40 ~ b5 - 1;
Page 41 ~ b5 - 1;
Page 42 ~ b5 - 1;
Page 43 ~ b5 - 1; b7E - 4;
Page 44 ~ b5 - 1; b7E - 4;
Page 45 ~ b5 - 1; b7E - 4;
Page 46 ~ b5 - 1; b7E - 4;
Page 47 ~ b5 - 1; b7E - 4;
Page 48 ~ b5 - 1; b7E - 4;
Page 49 ~ b5 - 1;
Page 50 ~ b5 - 1;
Page 51 ~ b5 - 1;
Page 52 ~ b5 - 1; b7E - 4;
Page 53 ~ b5 - 1; b7E - 4;
Page 54 ~ b5 - 1; b7E - 4;
Page 55 ~ b5 - 1; b7E - 4;
Page 56 ~ b5 - 1; b7E - 4;
Page 57 ~ b5 - 1; b7E - 4;
Page 58 ~ b3 - 1; b5 - 1; b7A - 1; b7E - 1;
Page 59 ~ b3 - 1; b5 - 1; b7A - 1; b7E - 1;
Page 60 ~ b3 - 1; b5 - 1; b7E - 1;

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

INSPECTION DIVISION
EXTERNAL AUDIT AND COMPLIANCE

COMPLIANCE AND MITGATION UNIT REPORT

DOMESTIC INVESTIGATIONS AND OPERATIONS GUIDE: AN AUDIT OF ASSESSMENTS AND INVESTIGATIONS OPENED BETWEEN MAY 1, 2013 and APRIL 30, 2014

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 12

V. (U) SELECTED FIELD OFFICE COMPLIANCE ANALYSIS 14

VI. (U) CONCLUSION 15

VII. (U) OBSERVATIONS AND RECOMMENDATIONS 16

VIII.(U) LIST OF ATTACHMENTS 22

Attachment A: Inspection Staffing Roster

Attachment B: Abbreviations

Attachment C: Audit Questions

Attachment D: Assessments/Predicated Investigations Eliminated

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 6/15/2012, with the most recent update published on 11/16/2013.

(U) Instant DIOG audit had two primary objectives. First, a 100% review of all Enterprise Investigations (EI) and a representative sampling of all Type 3-6 Assessments opened between 05/01/2013 and 04/30/2014. Second, a representative sampling of Type 1 and 2 Assessments, Guardian Leads, Preliminary Investigations (PIs), and Full Investigations (FIs) from six select field offices (FO) opened during this same timeframe. The FO chosen were selected based upon potential under and/or over self reporting of substantial noncompliance to the Office of Integrity and Compliance (OIC). As initial results of PI compliance revealed errors, a determination was made to broaden the audit and take a representative sampling across the remaining 50 FO to assess this aspect nationwide.

(U) Six areas of DIOG compliance were selected to audit: a) Initiation of the Assessment /Investigation; b) Sensitive Investigative Matters (SIMs); c) Undisclosed Participation (UDP); d) Unauthorized Use of Investigative Methods; e) Undercover Operations (UCOs); and f) PI approvals/extensions. The audit also focused on policies unique to certain types of Assessments including: documentation of the screening method utilized in Type 5 Assessments involving groups; the description requirements of individual subjects of Type 5 Assessments; required closing statements in Assessments; and documentation of FBIHQ approval for Type 6 Assessments.

(U) A total of 1,894 Assessments/Predicated Investigations were audited for compliance with 215 errors identified in 195 (10.3%) Assessments/Predicated Investigations (20 Assessment /Predicated Investigations had two compliance errors). In no instance was an Assessment /Investigation found to have been opened based on a subject's First Amendment Activities or Protected Characteristics. Eighty-two (38.1%) compliance errors were associated with PIs; 73 (34.0%) compliance errors were associated with the initiation of an Assessment/ Investigation; 23 (10.7%) were associated with SIMs; six (2.8%) involved the unauthorized use of an investigative method; and 31 (14.4%) involved closing notifications. There were no compliance errors identified involving UCO or UDP.

(U) In the 82 compliance errors associated with PIs, 69 occurred when the PI was not concluded or extended prior to the expiration date; 13 of which also had investigative activity conducted during the lapse. All 82 instances were deemed "Substantial Non-Compliance."

(U) Seventy of the 73 errors associated with the initiation of an Assessment/Investigation were related to the initiation of EIs lacking SC approval. All 70 were deemed "Substantial Non-Compliance."

(U) In addition, of the 1,894 Assessments/Predicated Investigations audited, 23 had SIM related errors. Specifically, 10 (43.5%) of the 23 SIM errors occurred when there was a failure to recognize and identify the matter as a SIM, resulting in "Substantial Non-Compliance." Thirteen (56.5%) of these 23 were appropriately identified as SIMs yet lacked the requisite DIOG documented approvals. Specifically, eight (61.5%) were determined to be "Substantial Non-Compliance" with a lack of SAC approval and CDC review (7) or a lack of SAC approval (1). The remaining five SIM errors were deemed "Other Non-Compliance" based upon a lack of CDC review.

(U) There were six "Substantial Non-Compliance" errors involving the unauthorized use of investigative methods in Assessments. Four (66.7%) lacked documented approval for an initial surveillance period, while one (16.7%) lacked documented approval for surveillance to go [redacted] The remaining instance of unauthorized use of investigative methods (16.7%) included the use of six Grand Jury subpoenas in one Type 3 Assessment. b7E -4

(U/~~FOUO~~) Of the total 215 errors, 176 (81.9%) were deemed "Substantial Non-Compliance"; the remaining 39 errors (18.1%) were deemed "Other Non-Compliance." This represents a slight rise in the total substantial non-compliance rate over last year (79.5%), although last year's DIOG audit did not evaluate PIs[1].

(U) Overall, CID had the largest number of compliance errors, with 101 (47.0%); CTD accounted for 45 (21.0%); IP 31 (14.5%); and CD 24 (11.2%). No other program had more than 10 errors. PIs accounted for 82 (38.1%) of the compliance errors; EIs accounted for 70 (32.6%) of the compliance errors; Type 3 Assessments accounted for 28 (13.0%) and Type 5 Assessments accounted for 21 (9.8%). No other type of Assessment/Investigation accounted for more than three compliance errors.

[1] Absent an evaluation of PIs this year, the overall substantial non-compliance rate would have been 70.7%, an 8.8% drop from last year. Additionally, if the current EI SC errors are backed out, the substantial non-compliance rate drops to 38.1% this year, a significant drop from last year.

II. (U) SCOPE AND METHODOLOGY

A. (U) Identification of Assessments/Predicated Investigations

(U) Initially, INSD planned to audit 100% of all EI and a representative sampling of all Type 3-6 Assessments opened between 05/01/2013 and 04/30/2014 as well as a representative sampling of Type 1 and 2 Assessments, Guardian Leads, PIs, and FIs from six select FO opened during this same timeframe. The FO chosen were selected based upon potential under and/or over self reporting of substantial noncompliance to OIC. As initial results of PI compliance revealed errors, a determination was made to broaden the audit and take a representative sampling across the remaining 50 FO to assess this aspect nationwide.

(U) The representative sampling of 1,945 Assessments/Investigations was randomly selected from a total of 10,477 Assessment/Investigations to provide a 95% confidence level with a 5% level of precision[2].

(U) During the audit, 51 (2.6%) of the total Assessments/Predicated Investigations were eliminated for various reasons, to include: case consolidation (the file contained an insufficient number of serials to review); administrative cases were mistakenly opened as full investigative cases (ex: National Academy Candidate Nominations, Security Background Investigations, and BuCar Accident Reviews); and full investigations were opened (per DIOG Section 12) to provide technical assistance to local police departments (343A/343V matters). This resulted in 1,894 Assessments/Predicated Investigations being audited. A complete listing of eliminated Assessments/Predicated Investigations is included at Attachment D. The exact breakdown of the audited items is depicted in the chart below:

Table 1: Assessments/Predicated Investigations Audited

Assessments/Predicated Investigations Type	Audited
Type 1&2 Assessments	65
[redacted]	279
Type 3 Assessments – Potential targets or vulnerabilities	308
Type 4 Assessments – Intelligence analysis to determine threats	18
Type 5 Assessments – Identify or assess human sources	328
Type 6 Assessments – Positive Foreign Intelligence Assessment	8
Preliminary Investigations	486
Full Investigations	315
Enterprise Investigations	87
Total	**1,894**

b7E -3

[2] 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%.

B. (U) Methodology

(U) From 07/21/2014 – 07/31/2014, a team of 12 AIIPs from various field offices and FBIHQ conducted the audit. The AIIPs were assisted and co-located with the UC, Compliance and Mitigation Unit, three INSD Team Leaders (TL), two OGC attorneys, a representative from the OIC, and two DIOG subject matter experts from the Internal Policy Office (IPO). All of the AIIPs previously received DIOG training and successfully passed the DIOG exam required following publication of the 10/15/2011 DIOG. In addition, DIOG refresher training was provided at the start of the audit by OGC.

(U) A specific five step review process was used to identify any instances of Non-Compliance. The first step was identification of the potential Non-Compliance error by the AIIP. The second step was review of the potential Non-Compliance error by one of the OGC attorneys to confirm the correct interpretation/application of the DIOG. The third step was review by a TL to confirm the relevant systems [redacted] or Sentinel) did not contain any further information which would mitigate the potential Non-Compliance error. The fourth step was review of the Non-Compliance error by a DIOG subject matter expert and TL, who 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 Non-Compliance errors documented during the audit went through the five steps described above. When the field office had previously identified and reported the Non-Compliance error to OIC, an email was not sent during the audit by INSD. b7E -3

III. (U) COMPLIANCE AREAS AND ERRORS

(U) The Assessments/Predicated Investigations audited were reviewed for compliance in six areas: a) Initiation of the Assessment/Investigation; b) SIMs; c) UDP; d) Unauthorized Use of Investigative Methods; e) UCOs; and f) PI approvals/extensions. The audit also focused on policies unique to certain types of Assessments including: documentation of the screening method utilized in Type 5 Assessments involving groups; the description requirements of individual subjects of Type 5 Assessments; required closing statements in Assessments; and documentation of FBIHQ approval for Type 6 Assessments.

(U) A total of 1,894 Assessments/Predicated Investigations were audited for compliance with 215 errors identified in 195 (10.3%) Assessments/Predicated Investigations (20 Assessment /Predicated Investigations had two compliance errors each). In no instance was an Assessment/Investigation found to have been opened based on a subject's First Amendment Activities or Protected Characteristics. Eighty-two (38.1%) compliance errors were associated with PIs; 73 (34.0%) compliance errors were associated with the initiation of an Assessment/ Investigation; 23 (10.7%) were associated with SIMs; six (2.8%) involved the unauthorized use of an investigative technique; and 31 (14.4%) involved closing notifications. There were no compliance errors identified involving UCO or UDP.

(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, a compliance error was noted if the facts did not meet in accordance with any of the DIOG requirements. If the non-compliance had been previously reported to OIC, it was not counted again by INSD.

A. (U) Preliminary Investigations

i. (U) Analysis:

(U//~~FOUO~~) The DIOG establishes the timeframes and approving authorities for Preliminary Investigations. The DIOG, Section 6.7.2 states "A Preliminary Investigation must be concluded within six months of its opening but may be extended for up to six months by the SAC (delegable to the ASAC)…Extensions of Preliminary Investigations beyond a year are discouraged and may only be approved by the appropriate FBIHQ operational section for 'good cause' (AGG-Dom, Part II.B.4.a.ii)."

(U//~~FOUO~~) In addition, the DIOG, Section 6.7.3 states [redacted] b7E -4

ii. (U) Compliance Errors:

(U//~~FOUO~~) Eighty two compliance errors were identified with PIs; 61 occurred when the PI was not concluded or extended prior to the initial six month period; 8 occurred when the PI was not timely approved by the appropriate FBIHQ operational section at the one year anniversary; and 13 occurred when investigative activity was conducted during the lapse. All 82 PI errors were deemed "Substantial Non-Compliance." This error rate accounted for 38.1% of the overall DIOG audit error rate.

(U//~~FOUO~~) There were no instances identified wherein [redacted] Nevertheless, some periods of lapse were extensive, ranging as high as 268 days to a low of one day, with the average at 41 days. In eight instances, auditors found the PI had expired and no extension request had been made by the field nor had the case been closed at the time of the audit. A complete breakdown of the 69 lapses with frequency is depicted in the chart below:

Table 2: Range of Preliminary Investigation Lapses

Days Elapsed	Amount Found
1-5	14
6-10	14
11-20	8
21-40	12
41-60	4
61-80	6
81-100	4
Over 100	5
Over 200	2
Total	69

B. (U) Initiation of an Assessment/Investigation

i. (U) Analysis:

(U/~~FOUO~~) The DIOG establishes the standards for the initiation of each level of investigative activity (Assessment, PI, and FI). The DIOG, Section 5.1 states "Assessments authorized under the AGG-Dom do not require a particular factual predication but do require an authorized purpose and clearly defined objective(s). Assessments may be carried out to detect, obtain information about, or prevent or protect against Federal crimes or threats to the national security or to collect foreign intelligence (AGG-Dom, Part II and Part II.A). Although 'no particular factual predication' is required, the basis of an Assessment cannot be arbitrary or groundless speculation, nor can an Assessment be based solely on the exercise of First Amendment protected activities or on the race, ethnicity, national origin or religion of the subject. Although difficult to define, 'no particular factual predication' is less than 'information or allegation' as required for the initiation of a preliminary investigation (PI)."

(U/~~FOUO~~) In addition, the DIOG establishes a variety of requirements specific to each particular type of Assessment/Investigation. For example, the DIOG, Section 5.6.3.4.3.2 addresses the opening EC as part of the "Evaluation/Recruitment Phases" of Type 5 Assessments

[redacted] b7E -4

ii. (U) Compliance Errors:

(U) None of the 1,894 Assessments/Predicated Investigations audited were initiated based solely on the exercise of First Amendment protected activities or on the race, ethnicity, national origin or religion of the subject. Seventy three compliance errors were identified with the initiation of an Assessment/Predicated Investigation. Seventy of these were deemed

Substantial Non-Compliance, while the remaining three were found to be Other Non-Compliance. The following details the compliance errors:

- (U//~~FOUO~~) The 70 Substantial Non-Compliance errors all involved EIs and the field offices' failure to document SC approval as mandated in DIOG, Section 8.6.3.1. The lack of SC approval constituted Substantial Non-Compliance as defined by DIOG, Section 2.8.1.1 which states "Substantial noncompliance…includes the following: *...the failure to obtain required supervisory approval."* All field offices with this DIOG deviation were notified by INSD of their non-compliance and similar responses were received from several field offices. Specifically, several FO noted the investigation was meant to be opened as an FI; however, the case agent mistakenly selected the wrong investigative type in Sentinel. Other offices advised they misunderstood the definition of "Enterprise Investigation" in DIOG and selected the EI case designation in Sentinel because they were investigating a criminal enterprise. The CID accounted for 59 (84.3%) of the total 70 errors identified.

- (U//~~FOUO~~) In 3 Assessments/Predicated Investigations, the compliance error was "other" or non-substantial. In two instances, the Other Non-Compliance resulted from Type 5 Assessments which did not contain all of the information required by DIOG, Sections 5.6.3.4.3.1 and 5.6.3.4.4.1. The requirements vary based on whether or not a specific individual or group of individuals for recruitment had been identified and require the opening communication to contain a variety of information. For example, if a specific individual has been identified then the opening communication must include the threat the potential CHS (PCHS) can report on and the PCHS's placement and access to intelligence. [redacted] b7E -4 In the remaining Other Non-Compliance error, the opening EC lacked sufficient predication, although additional supporting facts were located in the file, resulting in Other Non-Compliance.

C. (U) Sensitive Investigative Matters

i. (U) Analysis

(U//~~FOUO~~) Per DIOG, Section 10.1.2.1, a SIM is defined as "an investigative matter involving the activities of a domestic public official or political candidate (involving corruption or a threat to national security); religious or political organizations or an individual prominent in such organizations; news media; a specified academic nexus; or any other matter which, in the judgment of the official authorizing an investigation, should be brought to the attention of FBIHQ and other DOJ officials." [redacted] b7E -4 (DIOG, Sections 5.7, 6.10, 7.10, and 10.1.4). Additionally, an Assessment or Predicated Investigation opened beyond five days involving a SIM must have been reviewed by the CDC and approved by the SAC (DIOG, Section 10.1.4).

(U) The audit evaluated whether the Assessment/Investigation involved a SIM; whether the Assessment/Investigation was correctly titled; and whether the field office identified the Assessment/Investigation as a SIM and if so, whether the field office obtained the appropriate approvals. A compliance error was identified if the matter was not correctly identified as a SIM, the matter was not correctly titled, or if either the required CDC review or SAC approval was missing.

ii. (U) Compliance Errors:

(U) Of the 1,894 Assessments/Predicated Investigations audited, 23 had SIM related errors. Specifically, 10 (43.5%) of the 23 SIM errors occurred when there was a failure to recognize and identify the matter as a SIM, resulting in "Substantial Non-Compliance." Thirteen (56.5%) of the 23 were appropriately identified as SIMs yet lacked the requisite DIOG documented approvals. Specifically, eight (61.5%) were determined to be "Substantial Non-Compliance" with a lack of SAC approval and CDC review (7) or a lack of SAC approval (1). The remaining five SIM errors were deemed "Other Non-Compliance" based upon a lack of CDC review. [redacted] b7E -4

(U) The following table displays the number of Assessments/Predicated Investigations where the SIM was not identified by category:

Table 2: Frequency of SIM Categories/Errors

Type of SIM	Failure to Identify	Totals	Percent
Domestic Public Official	1	1	10
Domestic Political Candidate	0	0	0
Domestic Political Organization or Individual Prominent in Such an Organization	4	4	40
Religious Organization or Individual Prominent in Such an Organization	1	1	10
Member of the News Media or a News Organization	0	0	0
Academic Nexus	4	4	40
Total	10	10	100

(U) The following table breaks down the SIM errors by instance and Type of Assessment/Predicated Investigation:

Table 3: SIM Error by Instance and Assessment/Predicated Investigation Type

SIM Instances	Type 1 & 2	Type 3	Type 4	Type 5	Type 6	PI	FI	EI	Total
Lacked SAC Approval						1			1
Lacked CDC Review		3				1	1		5
Lacked SAC Approval and CDC Review	3			1		1	1	1	7
Failed to Identify SIM		4		4		1	1		10
Sub-Total	3	7	0	5		4	3	1	23

(U//~~FOUO~~) The failure to identify SIMs occurred most often with Type 3 and Type 5 Assessments. Each involved Domestic Political Organizations (DPO) and/or an Academic Nexus; [redacted] b7E -4

D. (U) Unauthorized Use of Investigative Methods

i. (U) Analysis

(U//~~FOUO~~) With the exception of FIs and EIs, which can utilize all investigative methods, the DIOG, Section 18 limits the types of investigative methods which may be utilized in Assessments/Predicated Investigations. The audited Assessments/Predicated Investigations were examined to determine if the investigative methods utilized were authorized. A compliance error resulted when a method not authorized for an Assessment/Predicated Investigation was utilized.

ii. (U) Compliance Errors

(U//~~FOUO~~) The audit identified five Substantial Non-Compliance errors wherein surveillance was utilized in an Assessment; four errors occurred when the initial authorization period was not properly approved; one additional occurred when the surveillance was [redacted] b7E -4 in accordance with DIOG, Section 18.5.8.3.2. [redacted] In these five instances, surveillance was conducted without documented approval. These errors constituted Substantial Non-Compliance as defined by DIOG, Section 2.8.1.1 which states "Substantial Non-Compliance…includes the following: *...the failure to obtain required supervisory approval.*"

(U//~~FOUO~~) The remaining error included the use of an investigative method not authorized in DIOG, Section 18.6.5. This error included the use of six Grand Jury Subpoenas in a Type 3 Assessment.

E. (U) Undisclosed Participation (UDP)

i. (U) Analysis

(U//~~FOUO~~) UDP "takes place when anyone acting on behalf of the FBI, including but not limited to an FBI employee or CHS, becomes a member or participates in the activity of an organization on behalf of the U.S. Government without disclosing FBI affiliation to an appropriate official of the organization" (DIOG, Section 16.1).

(U//~~FOUO~~) [redacted] (DIOG, Section 16.9.3). [redacted] DIOG, Section 16.9.3. [redacted]

b7E -3,4

ii. (U) Compliance Errors:

(U) The audit did not identify any instances of UDP and found no compliance errors. A statistically valid evaluation of compliance with the DIOG requirements related to UDP [redacted]

F. (U) Undercover Operations (UCOs)

i. (U) Analysis

(U//~~FOUO~~) The DIOG, Section 18.6.13, [redacted] The DIOG, Section 18.6.13.4.2, [redacted]

b7E -4

b7E -4

G. (U) Closing Caveats

i. (U) Analysis

(U//~~FOUO~~) The DIOG, Section 5.12.1 provides guidance on marking closed Assessments that contain personal information. Specifically, the DIOG requires closing caveat language to be clearly annotated in the closing EC to protect personally identifiable information from further dissemination. Within the 727 Assessments audited, 339 were closed. Auditors identified 31 (9.1%) instances of noncompliance associated with the failure to have the requisite "closing caveats." All 31 errors were deemed "Other Non-Compliance."

IV. (U) NON-COMPLIANCE ANALYSIS/TRENDS

(U//~~FOUO~~) Of the total 1,894 audited Assessments/Predicated Investigations, 215 errors were identified in 195 Assessments/Predicated Investigations (20 Assessments/Predicated Investigations had two compliance errors) resulting in an overall error rate of 10.3%. Within this count, 176 errors, 81.9%, were deemed "Substantial Non-Compliance"; the remaining 39 errors, 18.1% were deemed "Other Non-Compliance." The chart below compares last year's DIOG overall error results to the current audit. Although the Substantial Non-Compliance rates have risen slightly, this year's DIOG audit encompassed PIs, which were not included in last year's audit. In addition, PI noncompliance accounted for the largest majority of errors this year (82/38.1%).

Table 4: DIOG Error Rates by Audit Year/Level of Non-Compliance

Type of Non-Compliance	2013 Audit	2014 Audit
Substantial Non-Compliance Errors	210 (79.5%)	176 (81.9%)
Other Non-Compliance Errors	54 (20.5%)	39 (18.1%)
Totals	264	215

(U//~~FOUO~~) Conversely, instant audit identified seventy-three total errors associated with the initiation of an Assessment/Predicated Investigation. Seventy of the 73 constituted Substantial Non-Compliance and all involved Enterprise Investigations failing to obtain Section Chief Approval in violation of DIOG, Section 8.6.3.1. The chart below shows the comparison of this data to last year's DIOG audit results.

Table 5: Initiation Compliance Errors by Year

Initiation Non-Compliance	2013 Audit	2014 Audit
Lacked Authorized Purpose/Predication	5 (3.5%)	1 (1.4%)
Type 5 Subject Error	19 (13.4%)	0
Type 5 Group Error	23 (16.2%)	2 (2.7%)
EI: Lacked SC Approval	95 (66.9%)	70 (95.9%)
Totals	142 (53.8%)	73 (33.0%)

(U//~~FOUO~~) Instant audit identified 23 total errors associated with SIMs. Specifically, 10 of the 23 SIM errors occurred when there was a failure to recognize and identify the SIM. The charts below shows the comparison of this data to last year's DIOG audit results in regards to failure to identify and the category of SIMs missed most often.

Table 6: SIM Compliance Errors by Year

SIM Non-Compliance	2013 Audit	2014 Audit
Failed To Identify SIM	46 (45%)	10 (44%)
Lacked CDC Review and SAC Approval	49 (48%)	7 (30%)
CDC Review Missing	7 (7%)	5 (22%)
Lacked SAC Approval	0	1 (4%)
Totals	102 (38.6%)	23 (10.7%)

Table 7: SIM Failure to Identify Errors by Category

Category	2013 Audit	2014 Audit
Domestic Public Official	3	1
Domestic Political Candidate	1	0
Domestic Political Organization or Individual Prominent in Such an Organization	12	4
Religious Organization or Individual Prominent in Such an Organization	8	1
Member of the News Media or a News Organization	1	0
Academic Nexus	21	4
Totals	46	10

(U//~~FOUO~~) Lastly, this year's audit identified 6 total errors involving the use of Investigative Methods in violation of DIOG, Section 18. These errors were all deemed "Substantial Non-Compliance." A comparison of prohibited investigative method usage from

last year to this year is depicted in the chart below. The failure to obtain approval for physical surveillance continues to be the most prevalent error with Assessments.

Table 8: Compliance Errors Involving Investigative Methods

Non-Compliance	2013 Audit	2014 Audit
Grand Jury Subpoenas	2	1
No approval for initial surveillance period		4
No approval for surveillance [redacted]	13	1
Other Unauthorized Methods	4	0
Total	19	6

b7E -4

(U) The CID had the largest number of the 215 compliance errors, with 101 (47.2%); CTD accounted for 45 (21.0%); IP had 31 (14.5%) and CD had 24 (11.2%). No other program had more than 10 errors. EIs accounted for 70 (32.6%) of the compliance errors; Type 3 Assessments accounted for 28 (13.0%) and Type 5 Assessments accounted for 21 (9.8%). No other Assessment/Predicated Investigation accounted for more than three errors.

V. SELECTED FIELD OFFICE COMPLIANCE ANALYSIS

(U) INSD analyzed the compliance errors of the select six FO to determine if there was any correlation between potential under/over self reporting of substantial non-compliance to OIC. Specifically, whether any instances of substantial non-compliance had been identified yet not reported to OIC (i.e., potential under-reporters – OC, IP, JN, and PD) or conversely whether a field office's positive history of reporting substantial non-compliance to OIC was indicative of the office identifying substantial non-compliance (potential over-reporters – AL, CO). Auditors identified 23 (10.7%) instances of substantial non-compliance from within these six FO; with none of them having been previously recognized/reported by the FO. The breakdown was as follows:

Table 9: Substantial Non-Compliance Identified at Select Field Offices

Field Office	SIM – Failure to Identify	SIM – Lack of SAC Approval/CDC Review	PI – Expiration	PI – Investigative Activity During Lapse	EI – Lack of SC Approval	Total
Oklahoma City		1	1		2	4
Indianapolis			1	1	2	4
Chicago	1	1	3	1		6
Portland			1			1
Atlanta	1	1				2
Columbia		1	4	1		6
Total	2	4	10	3	4	23

(U//~~FOUO~~) An examination of substantial non-compliance identified at all FO indicated 48 (85.7%) of all FO had at least one error determined to be "Substantial Non-Compliance." The top three FO were: NY (16), LA (13), and BS (9), with the average across the 48 being 3.6 substantial non-compliance errors. Both CO and JN fall above the average, yet CO was selected as a possible over-reporter to OIC, while JN was chosen for possibly under-reporting to OIC. Based on the foregoing, INSD did not find any correlation between the frequency of FO reporting substantial non-compliance to the OIC and the actual amount of substantial non-compliance that existed.

VI. (U) CONCLUSION

(U) INSD developed a methodology to audit a representative sampling of Assessments/ Predicated Investigations opened since the significant revision of the DIOG effective 10/15/2011. INSD conducted an audit of 1,894 Assessments/Predicated Investigations which included Assessments/Predicated Investigations from all 56 field offices. Each Assessment/ Predicated Investigation was reviewed and evaluated in six areas of DIOG compliance.

(U) The audit identified 215 total compliance errors; 176 deemed "Substantial Non-Compliance" errors. The most significant causes of Substantial Non-Compliance stemmed from field offices failing to timely conclude or extend PIs, as well as failing to obtain SC approval upon initiation of an EI.

(U) The 101 errors in the CID accounted for 47.0% of the 215 total compliance errors. CTD had the second highest number of errors with 45 (21.0%) total.

(U) To mitigate these errors in the future, INSD makes the following 5 Observations/ Recommendations.

VII. (U) OBSERVATIONS AND RECOMMENDATIONS

(U//~~FOUO~~) **Observation 1:** Field Offices did not timely conclude or extend Preliminary Investigations (PI).

(U//~~FOUO~~) **Analysis 1:** DIOG Section 6.7.2 required a PI must be concluded within six months of its opening but may be extended for up to six months by the SAC (delegable to the ASAC). Extensions of PIs beyond a year are discouraged and may only be approved by the appropriate FBIHQ operational section for "good cause."

(U//~~FOUO~~) Sixty-one (12.6%) of the 486 audited PIs failed to obtain the appropriate approval for an extension within the initial six month period of the investigation. Of these 60 PIs, 13 (21.7%) conducted investigative activity during the lapse period.

(U//~~FOUO~~) In addition, eight (1.6%) of the 486 PIs audited did not have approval from the appropriate FBIHQ operational section to extend beyond one year within the required time frame.

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

(U//~~FOUO~~) **Observation 2:** Field offices did not obtain SC approval prior to initiating an EI.

(U//~~FOUO~~) **Analysis:** DIOG Section 8.6.3 states the opening of an EI by an FBI field office requires the prior approval of the appropriate FBIHQ SC, as well as written notification to the USAO and DOJ.

(U//~~FOUO~~) Seventy (80.5%) of the 87 EIs audited lacked SC approval. Fifty-nine (84.3%) of these errors derived from the criminal program, four (5.7%) from the counterintelligence program, five (7.1%) from the counterterrorism program, and two (2.9%) from the cyber program.

(U//~~FOUO~~) DIOG Section 8.4 states "A Full Investigation of a group or organization may be opened as an Enterprise Investigation if there is an articulable factual basis for the investigation that reasonably indicates the group or organization may have engaged, or may be engaged in, or may have or may be in engaged in planning or preparation or provision of support for: racketeering activity (92 and 305A matters), international terrorism (415 matters), domestic terrorism (100 matters)."

(U//~~FOUO~~) Sixty-five (92.9%) of the 70 EIs opened without SC approval were not associated with the matters expressly defined within DIOG Section 8.4 and should not have been designated within Sentinel as a "Enterprise Investigation."

(U//~~FOUO~~) Comparison of these results to last year's 2013 DIOG Audit highlighted a continual issue within the criminal program. The 2013 DIOG Audit indicated 84 (88.4%) of the 95 errors originated from the criminal program.

(U//~~FOUO~~) **Instruction 2a:** [redacted]

(U//~~FOUO~~) **Recommendation 2b:** [redacted] b5 -1

(U//~~FOUO~~) **Recommendation 2c:** [redacted]

(U//~~FOUO~~) **Observation 3**: Field offices did not appropriately identify, designate, or obtain approval for Sensitive Investigative Matters (SIM).

(U//~~FOUO~~) **Analysis 3a**: DIOG Section 10.1.2.1 defines a SIM as, "an investigative matter involving the activities of a domestic public official or domestic political candidate (involving corruption or a threat to the national security), a religious or domestic political organization or individual prominent in such an organization, or the news media; an investigative matter having an academic nexus; or any other matter which, in the judgment of the official authorizing the investigation, should be brought to the attention of FBI Headquarters (FBIHQ) and other DOJ officials."

(U) Of the total cases reviewed, there were 23 (1.2%) instances of non-compliance with SIMs. Ten (43.5%) of the 23 SIMs related errors occurred when there was a failure to identify the SIM when the facts involved the activities of one of the delineated categories:

SIM Categories	Incidents of Non-Compliance	Percentage of Non-Compliance
Domestic Public Official	1	10%
Domestic Political Candidate	0	0%
Domestic Political Organization or Individual Prominent in Such an Organization	4	40%
Religious Organization or Individual Prominent in Such an Organization	1	10%
Member of the News Media or a News Organization	0	0%
Academic Nexus	4	40%
Totals:	10	100%

(U//~~FOUO~~) **Analysis 3b**: DIOG Section 10.1.4.1 requires an Assessment involving a SIM to be reviewed by the CDC and approved by the SAC as soon as practicable, but no later than five (5) business days after the opening or after the identification of a SIM to authorize the Assessment to continue. Additionally, DIOG Sections 6.7.1.1 and 7.7.1.1 require prior CDC review and SAC approval for the opening of a PI or FI designated as a SIM. Should a SIM arise after the opening of a PI or FI, investigative activity may continue, but the matter must be reviewed by the CDC and approved by the SAC as soon as practicable, but no more than five (5) business days thereafter to continue the investigation.

(U//~~FOUO~~) The audit determined 13 (56.5%) of the SIMs identified lacked documentation of CDC review, SAC approval, or lacked both CDC review and SAC approval as required. A breakdown of these SIM errors was as follows:

SIM Instances	Incidents of Non-Compliance
Lacked CDC Review	5 (38.5%)
Lacked SAC Approval	1 (7.7%)
Lacked both SAC Approval and CDC Review	7 (53.8%)
Totals	13

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

(U) **Recommendation 3b:** [redacted]

(U//~~FOUO~~) **Observation 4:** Field offices failed to include the required closing caveats in Assessments.

(U//~~FOUO~~) **Analysis 4:** DIOG Section 5.12.1 provides guidance on marking closed Assessments that contain personal information. The specified closing caveat language "must be included in the synopsis section of the closing EC." INSD audited 727 Type 1 – 6 Assessments of which 339 were closed. The following non-compliance errors associated with the failure to use the closing caveat were identified:

Assessment Type	Audited	Assessments in Closed Status	Incidents of Non-Compliance	Percentage of Non-Compliance
Type 1&2	65	56	0	0%
Type 3	308	73	19	26%
Type 4	18	4	1	25%
Type 5	328	206	11	5.3%
Type 6	8	0	0	0%

(U//~~FOUO~~) **Recommendation 4:** [redacted] b5 -1

(U//~~FOUO~~) **Observation 5:** Sentinel incorrectly calculated Preliminary Investigation (PI) initiation, extension, and expiration dates.

(U//~~FOUO~~) **Analysis 5:** Sentinel automatically populated PI initiation and extension dates based on dates the documents (ECs) were drafted, and not dates of approvals, which resulted in incorrect PI expiration dates. Per DIOG section 6.7.1.1, the effective date of a PI is the date the final approval authority (e.g., SSA or SAC) approves the EC [redacted]

b5 -1
b7E -4

(U//~~FOUO~~) **Recommendation 5:** [redacted]

VIII. (U) LIST OF ATTACHMENTS

Attachment A: Inspection Staffing Roster

Attachment B: Abbreviations

Attachment C: Audit Questions

Attachment D: Assessments/Predicated Investigations Not Audited

Attachment A: Inspection Staffing Roster

Section Chief
Laura R. Ingber (INSD)

Compliance and Management Unit
[redacted] (INSD)
[redacted] (INSD)
[redacted] (INSD)
[redacted] (INSD)
[redacted] (INSD)

b6 -1
b7C -1

Team Leaders
[redacted] (NY)
[redacted] (NK)
[redacted] (HO)

Assistant Inspectors-in-Place
[redacted] (NS)
[redacted] (DE)
[redacted] (NK)
[redacted] (NY)
[redacted] (WF)
[redacted] (WF)
[redacted] (CJIS)
[redacted] (CTD)
[redacted] (CV)
[redacted] (CV)
[redacted] (KX)
[redacted] (BS)

Attachment B: Abbreviations

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

A/	Acting
ACS	Automated Case Support System
AD	Assistant Director
ADC	Associate Division Counsel
ADD	Associate Deputy Director
AG	Attorney General
AGG	Attorney General Guidelines
AIIP	Assistant Inspector-in-Place
ALAT	Assistant Legal Attaché
AOB	Average on Board
AOR	Area of Responsibility
ASAC	Assistant Special Agent in Charge
ASC	Assistant Section Chief
AUSA	Assistant United States Attorney
CCP	Computer Crimes Program
CD	Counterintelligence Division
CDC	Chief Division Counsel
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
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
CORE	Collection Operations and Requirements Environment
CPD	Corporate Policy Directive
CPN	Corporate Policy Notice
CPO	Corporate Policy Office
CR	Civil Rights
CRP	Civil Rights Program
CS	Computer Scientist
CSO	Chief Security Officer
CT	Counterterrorism
CTD	Counterterrorism Division
CTP	Counterterrorism Preparedness
CyP	Cyber Program

 b6 -1
b7C -1

CyD	Cyber Division
DAD	Deputy Assistant Director
[redacted]	b7E -6
DCO	Division Compliance Officer
DD	Deputy Director
DI	Directorate of Intelligence
DIN	Domain Intelligence Note
DIOG	Domestic Investigations and Operations Guide
DLAT	Deputy Legal Attaché
DMC	Domain Management Coordinator
DO	Director's Office
DOJ	Department of Justice
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
[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
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
FOASR	Field Office Annual Source Reporting
FOIA	Freedom of Information Act
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
HUMINT	Human Intelligence
IA	Intelligence Analyst
IB	Intelligence Bulletin
[redacted]	b7E -3
IG	Inspector General
I/Is	Indictments/Informations
IIC	Inspector-in-Charge
IINI	Innocent Images National Initiative
IIR	Intelligence Information Report
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
ISF	Intelligence Submission Form
ISPs	Internet Service Providers
IT	International Terrorism
ITP	International Terrorism Program
ITSD	Information Technology Services Division
JTTF	Joint Terrorism Task Force
LA/SWBT	Latin America/Southwest Border Threat
LA/SWBTP	Latin America/Southwest Border Threat Program
LD	Laboratory Division
LEGAT	Legal Attaché
LOA	LEGAT Operations Assistant
MAOP	Manual of Administrative Operations and Procedures
MAPA	Management and Program Analyst
MIOG	Manual of Investigative Operations and Guidelines
MOU	Memorandum of Understanding
MST	Mobile Surveillance Team
MST-A	Mobile Surveillance Team-Armed
NA	FBI National Academy

NAACP	National Association for the Advancement of Colored People
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]	
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
OTD	Operational Technology Division
PAL	Prioritized Action List
PC	Public Corruption
PCOR	Program Coordinator
PCP	Public Corruption Program
PFI	Principal Firearms Instructor
PI	Preliminary Investigation
PIOB	Potential Intelligence Oversight Board
PM	Program Manager
[redacted]	
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

b7E -5

SAPR	Semi-Annual Program Review
SC	Section Chief
SCI	Sensitive Compartmented Information
SCIF	Sensitive Compartmented Information Facility
SecD	Security Division
SES	Senior Executive Service
SIA	Supervisory Intelligence Analyst
SIOC	Strategic Information and Operations Center
SIR	Situational Information Report
SME	Subject Matter Expert
SMS	Strategy Management System
SOS	Staff Operations Specialist
SPS	Strategy Performance Session
SSA	Supervisory Special Agent
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
TOCT	Transnational Organized Crime Threat
TOCTP	Transnational Organized Crime Threat Program
TPD	Third Party Draft
TRP	Threat Review and Prioritization
TSC	Terrorist Screening Center
TSL	Target Staffing Level
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
USIC	United States Intelligence Community
USMS	United States Marshals Service
VC	Violent Crime
VCAC	Violent Crimes Against Children
VCP	Violent Crimes Program

VCT	Violent Criminal Threat
VCTF	Violent Crimes Task Force
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