

THIS FILE IS MADE AVAILABLE THROUGH THE DECLASSIFICATION EFFORTS AND RESEARCH OF:

THE BLACK VAULT

THE BLACK VAULT IS THE LARGEST ONLINE FREEDOM OF INFORMATION ACT / GOVERNMENT RECORD CLEARING HOUSE IN THE WORLD. THE RESEARCH EFFORTS HERE ARE RESPONSIBLE FOR THE DECLASSIFICATION OF THOUSANDS OF DOCUMENTS THROUGHOUT THE U.S. GOVERNMENT, AND ALL CAN BE DOWNLOADED BY VISITING:

[HTTP://WWW.BLACKVAULT.COM](http://www.blackvault.com)

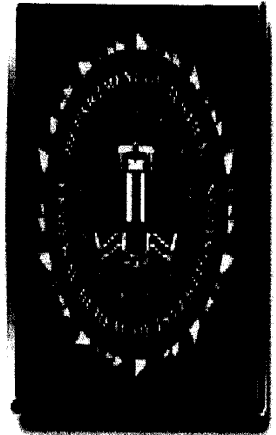
YOU ARE ENCOURAGED TO FORWARD THIS DOCUMENT TO YOUR FRIENDS, BUT PLEASE KEEP THIS IDENTIFYING IMAGE AT THE TOP OF THE .PDF SO OTHERS CAN DOWNLOAD MORE!

UNCLASSIFIED//FOUO

FEDERAL BUREAU OF INVESTIGATION
BRIEFING TO THE SENATE JUDICIARY COMMITTEE

OVERALL CLASSIFICATION:

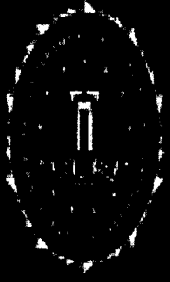
Domestic Investigations and Operations Guide (DIOG)



FEDERAL
BUREAU OF
INVESTIGATION

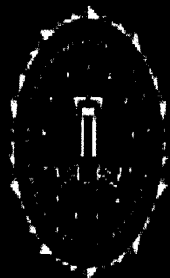
November
2009

UNCLASSIFIED//FOUO



DIOG Overview

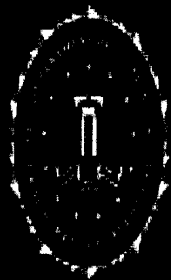
- The DIOG was written to implement The Attorney General's Guidelines for Domestic FBI Operations (AGG-DOM) and applies to all domestic investigative activities and intelligence collection conducted by the FBI.
- The Domestic Investigations and Operations Guide (DIOG) was approved by FBI Director Robert Mueller on December 16, 2008.
- The purpose of the DIOG is to standardize policy to ensure that criminal, national security, and foreign intelligence investigative activities are consistent throughout the FBI.
- The DIOG applies to all FBI employees, Task Force Officers, and all other individuals operating under FBI authority.



Investigation Progression

The DIOG provides guidance throughout the FBI investigative process. Investigations progress through the following three phases:

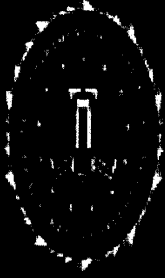
- Assessment
- Preliminary Investigation
- Full Investigation



Assessments

Prior to opening an assessment, an FBI employee must:

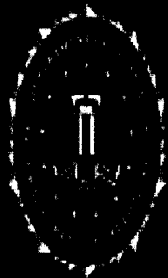
- determine an authorized purpose;
- follow specific work flows for management and documentation;
- not initiate based solely on the exercise of these First Amendment rights; (unless a group exercising its First Amendment rights also threatens or advocates violence or destruction of property)
- and must ensure that the assessment is an appropriate use of personnel and financial resources.



Preliminary Investigations

A Preliminary Investigation may be initiated if:

- a federal crime or a threat to the national security has, is or may occur, or;
- an individual, group, property or activity is or may be a target of federal criminal activity or threats to the national security; and
- the investigation may obtain information relating to the subject(s) involvement in such activities or protect against the activity or threat.

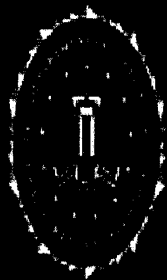


Full Investigations

The AGG-DOM authorizes a third level of investigative activity-predicated investigations. Full Investigations may be initiated if there is an “articulable factual basis” of possible criminal or national threat activity.

The three types of Full Investigations include:

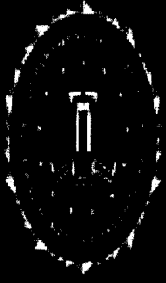
- Single and Multi-subject
- Enterprise
- Positive Foreign Intelligence.



Sensitive Investigative Matters

Investigations and Assessments are deemed “Sensitive Investigative Matters (SIMs)” when they involve activities of:

- A domestic public official (involving corruption or national security threat)
- A political candidate (involving corruption or national security threat)
- A religious or political organization, or individual prominent in such
- News media
- Matters having an academic nexus
- Any other matter which should be brought to the attention of FBIHQ or DOJ, in the judgment of authorizing official



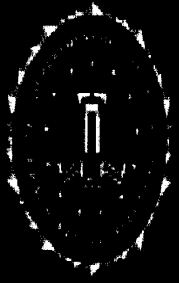
Undisclosed Participation (UDP)

- Policy driven by EO 12333
- AGG-Dom required a UDP policy and AG approval of that policy
- FBI Policy seeks uniformity in National Security Investigations and Criminal investigations

-



b2
b7E

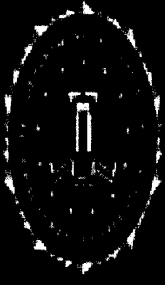


Undisclosed Participation (UDP)

General Undisclosed Participation (UDP):

- General UDP occurs when an FBI employee or Confidential Human Source (CHS), acting on behalf of the FBI, becomes a member or participates in the activity of an organization without disclosing FBI affiliation to an appropriate official of the organization
- “Organization” means an association of two or more persons formed for any lawful purpose (social, political, religious, business, etc.)

b2
b7E



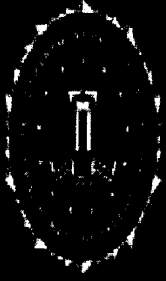
Undisclosed Participation (UDP) Approval Levels

Approval Level	Approval Authority



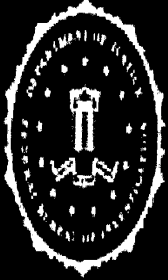
b2
b7E





Investigative Summary Charts

The following charts outline Investigative Methods and approval requirements for these methods, as well as the categories of Investigations.



Field Office Investigations Chart

Field Office Investigations Chart							
Investigation	Purpose	Duration	Documentation	Approval	Justification Review	SIM	Responsible Entity
Type 1	Activities constituting violations of federal criminal law or threats to the national security	As long as necessary to achieve purpose and objective; No time limit	FD-71 or Guardian as soon as practical	Any employee can initiate; SSA or SIA Approval	Every 30 days	CDC review; SAC approval	Investigative Squad
Type 2	The involvement or role of individuals, groups, or organizations in such activities (#1 above)						
Type 3					Every 90 days, if probationary employee, every 60 days		FIG (Collection Team) or Investigative Squad
Type 4	Obtaining information to inform or facilitate intelligence analysis and planning	As long as necessary to achieve purpose and objective; No time limit	EC before initiating	Prior SSA or SIA Approval	Every 90 days, if probationary employee, every 60 days	CDC review; SAC approval	FIG (Investigative Squad can support)
Type 5	Identify, assess, validate or maintain the cover or credibility of a CHS	CHSP Mand AGG-CHS	classification	CHSPM and AGG-CHS	CHS Manual	Not addressed in DIOG; Follow CHS Manual	FIG or Investigative Squad
Investigation	Predication	Duration	Documentation	Approval	Justification Review	SIM	Responsible Entity
PI	Initiated on the basis of "information or an allegation" indicating the existence of a circum stance described in DIOG Section 8.5	6 months; One extension by SAC not to exceed 1 year; HQ is to be notified of any extension	EC	Prior SSA Approval (CI also requires FBIHQ notice)	Every 90 days; If probationary employee, every 60 days	CDC Review, SAC Approval; Notification to USAO or DOJ & HQ within 30 days	Investigative Squad
Full	Initiated if there is an "articulable factual basis" that reasonably indicates circumstances described in DIOG Section 7.5 exist	Not time limit; Factual predication determines outcome	EC	Prior SSA with FBIHQ (& DOJ notice on NSB USPER matters)	Every 90 days; If probationary employee, every 60 days	CDC Review, SAC Approval; Notification to USAO or DOJ & HQ within 30 days	Investigative Squad
Enterprise Full	Investigation is predicated when there is an articulable factual basis for the investigation that reasonably indicates the group or organization is engaged in Racketeering, IT, DT, or other. See DIOG Section 8.4	Not time limit; Factual predication determines outcome	EC	Prior SSA with FBIHQ and DOJ notice	Every 90 days; If probationary employee, every 60 days	CDC Review, SAC Approval; Notification to USAO or DOJ & HQ within 30 days	Investigative Squad
PFI Full	Investigation may obtain Positive Foreign Intelligence (PI) that is responsive to a foreign intelligence requirement	Until the requirements met; No time limit	EC	Prior DII/CMS approval; notice to DOJ/NSO within 30 days	Every 90 days; If probationary employee, every 60 days	CDC Review, SAC Approval; Section Chief approval	FIG

b2
b7E



Investigative Methods Summary

Authorized Methods for Assessments and Predicated Investigations

Note: Red indicates methods not allowed under a particular operational activity; Green indicates methods allowed.

Assessments	Preliminary Investigations	Full Investigations
-------------	----------------------------	---------------------

Obtain publicly available information

Access and examine FBI and other DOJ records, and obtain information from any FBI or DOJ personnel

Access and examine records maintained by, and request information from, other federal, state, local, tribal, or foreign governmental entities or agencies

Use online services and resources (whether nonprofit or commercial)

Use and recruit human sources in conformity with AG Guidelines Regarding the Use of FBI Confidential Human Sources

Interview or request information from members of the public and private entities

Accept information voluntarily provided by governmental or private entities

Engage in observation or surveillance not requiring a court order

Mail covers

Physical searches of personal or real property where a warrant or court order is not legally required because there is no reasonable expectation of privacy (e.g., trash covers)

Consensual monitoring of communications, including consensual computer monitoring, is subject to legal review by the CDC or the FBI OGC. Where a sensitive monitoring circumstance is involved, monitoring must be approved by the Criminal Division or, if the investigation concerns foreign intelligence or a threat to the national security, by the National Security Division

Use of closed-circuit television, direction finders, and other monitoring devices, subject to legal review by the CDC or FBI OGC

Polygraph examinations

Undercover operations

Compulsory process as authorized by law, including Federal Grand Jury and other subpoenas and National Security Letters (Federal Grand Jury subpoenas for telephone and electronic mail subscriber records can be used during type 1 and 2 Assessments only)

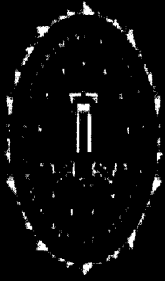
Accessing stored wire and electronic communications and transactional records

Use of pen registers and trap and trace devices

Electronic surveillance

Foreign Intelligence collection under Title VII of FISA

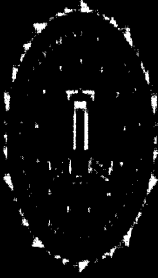
Physical searches, including mail openings, where a warrant or court order is legally required because there is an expectation of privacy



Investigative Methods Approval Summary

Approved Method/Description		Approval/Assessment/Requirement/Exception		
		Assessments	Predicated	Foreign Intelligence
1	5.9A Obtain publicly available information	None Required	None Required	None Required
	Tasking a LCE to attend religious service	Not Permitted	SSA Approval	SSA Approval
2	5.9B Physical surveillance of a person or group (Consult the DIOG for handheld photo and video surveillance with no reasonable expectation of privacy)	[Redacted] consult DIOG for requirements	None Required	None Required
		[Redacted]	Field Office Approval	Field Office Approval
		[Redacted]	ASAC Approval	ASAC Approval
3	5.9C Access and examine FBI and other Department of Justice (DOJ) records and obtain information from any FBI or other DOJ personnel	None Required	None Required	None Required
4	5.9D Access and examine records maintained by, and request information from, other federal, state, local, or tribal, or foreign governmental entities or agencies	None (Unless such approval is required by MOU or other agreements)	None (Unless such approvals required by MOU or other agreements)	None (Unless such approval is required by MOU or other agreements)
5	5.9E Use online services and resources (whether nonprofit or commercial)	None Required	None Required	None Required
6	5.9F Interview or request information from members of the public and private entities	None Required except for contact with represented persons, members of U.S. Congress or their staffs, White House personnel or other substantive division requirements	None Required except for contact with represented persons, members of U.S. Congress or their staffs, White House personnel, other substantive division requirements	None Required except for contact with represented persons, members of U.S. Congress, or their staffs, White House personnel, or other substantive division requirements
7	5.9G Accept information voluntarily provided by governmental or private entities	None Required	None Required	None Required
8	5.9H Use and recruit human sources	None Required (utilize [Redacted])	None Required (utilize Delta)	None Required (utilize Delta)
	Tasking a CHS to attend religious service	SAC Approval	SSA Approval	SSA Approval
9	5.9I Federal Grand Jury subpoenas or telephonic or electronic subscriber information	USA Attorney Office Approval (Type 1 and 2 Assessments Only)	USA Attorney Office Approval	Not Permitted
10	5.9C Pattern Based Data Mining	SCRC	SCRC	SCRC

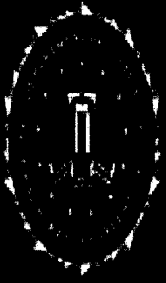
b2
b7E



Investigative Methods Approval Summary (cont.)

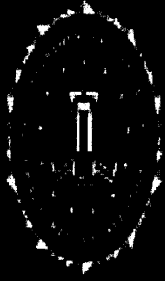
		Assessments	Predicated	Foreign Intelligence
11	11.3	Mail covers		
12	11.4	Physical searches of personal or real property where a warrant or court order is not legally required because there is no reasonable expectation of privacy (e.g. [redacted])		
13	11.5	Consensual monitoring of communications, including consensual computer monitoring	CDC or OGC Review SSA Approval	CDC or OGC Review SSA Approval
14	11.5	Consensual monitoring of communications, including consensual computer monitoring, with a sensitive monitoring circumstance	Not Permitted	CDC or OGC Review, SAC Approval, DOJ Criminal or DOJ NSD Approval
15	11.6	Use of closed-circuit television, direction finders, and other monitoring devices		
16	11.7	Polygraph examinations	SSA Approval	SSA Approval
17	11.8	Undercover operations, Group II	CDC Review, SAC or ASAC with delegated authority; National Security cases also require NSD unit UACB	CDC Review, SAC or ASAC with delegated authority, NSB-Unit/UACB Approval
18	11.8	Undercover operations, Group I	CDC review, SAC, and AD and C UORC or UCR (EAD/DD certain cases) Approval	CDC review, SAC and AD and UCR (EAD/DD certain cases) Approval
19	11.9	Compulsory process as authorized by law; Federal Grand Jury and trial subpoenas	US Attorney's Office Approval	
20	11.9	Administrative Subpoenas: Drugs	SAC, ASAC, SSRA, or Drug Squad SSA	Not Permitted
		Administrative Subpoenas: Sexual Exploitation		
		Administrative Subpoenas: Healthcare Fraud	U.S. Attorney's Office Approval	
21	11.9	National Security Letters	Field Office: CDC Review, ADIC or SAC Approval.	Not Permitted
			HQ: NSLB Review; DD or EAD-NSB or AD & DADs CT/CD/CyD or GC or Deputy GC-NSLB Approval	Not Permitted
22	11.10	Accessing stored wire and electronic communications and transactional records	Statute/Court Order, Consult DIOG	Not Permitted
23	11.11	Use of pen registers and trap and trace devices	FISA Court or District Court Order	Only Available for Non-USPER by FISA Court order
24	11.12	Electronic surveillance		
25	11.13	Physical searches, where there is reasonable expectation of privacy, including mail openings		
26	11.14	Acquisition of foreign intelligence information in conformity with Title VII of the Foreign Intelligence Surveillance Act	FISA Court Order	FISA Court order

b2
b7E



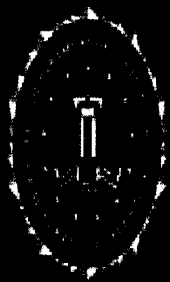
Protection of Civil Liberties

- Section 4 of the DIOG, *Privacy and Civil Liberties, and Least Intrusive Methods* outlines the FBI's oversight, self-regulation, and strict adherence to the Constitution of the United States.
- Throughout section 4, the DIOG discusses the protection of First Amendment rights (Freedom of Speech, Freedom of the Press, Freedom of Peaceful Assembly and to Petition of Government for Redress of Grievances, and Exercise of Religion), civil liberties and privacy issues, and Equal Protection of all Americans under the Fourteenth Amendment.
- Section 4.4 of the DIOG requires FBI employees to use the "Least Intrusive" means or method possible to obtain intelligence or evidence.



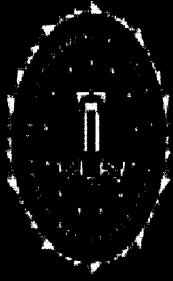
Use of Race and Ethnic Identity in Assessments and Investigations

- The DIOG reiterates Department of Justice (DOJ) guidance which permits the consideration of ethnic and racial identity information based on specific reporting (i.e. eyewitness accounts).
- Consideration of race or ethnicity is permitted in investigative or collection scenarios, if relevant. Examples may include investigations of ethnic-based gangs or terrorist organizations known to be comprised of members of the same ethnic grouping.



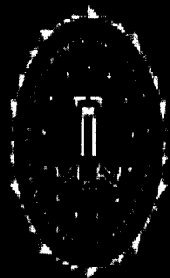
Collecting and Analyzing Demographics

- The DIOG also reiterates DOJ guidance permitting the collection and analysis of demographics if the identification of concentrated ethnic communities will reasonably aid in the analysis of potential threats and vulnerabilities or assist domain awareness for the purpose of performing intelligence analysis.
- In addition, the locations of ethnic-oriented businesses or other facilities may be collected if their locations will reasonably contribute to an awareness of threats and vulnerabilities and intelligence collection opportunities.



Collecting and Analyzing Demographics

- If the collection of ethnic/racial demographics is legally allowable in an investigation, it may also be “mapped” using sophisticated computer geo-mapping technology.
- These maps may be used for domain awareness of an area of responsibility, to track crime trends, or to identify specific communities or areas of interest to support specific assessments or investigations.
- Regardless of the purpose for its use, the relevance of the ethnic or racial information must be clearly demonstrated and documented.



Information Withheld Publicly from the DIOG

The FBI determined that several types of information should be redacted in the Public Release of the DIOG. These types of information include:

Redaction: FBI Policy Directives

Justification: These are internal FBI policies that govern administrative and operational matters not directly related to the DIOG.

Redaction: Terms and Definitions

Justification: Knowledge of specific FBI terms and definitions could allow for circumvention of investigations and spoofing.

Redaction: Collection and/or Analysis of Information

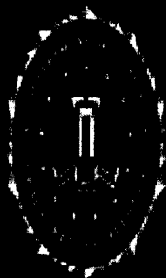
Justification: Knowledge of these internal decision-making criteria could allow for circumvention of collection and analytical techniques.

Redaction: FBI Data Systems

Justification: Many data systems used by the FBI are proprietary.

Redaction: Scenarios & Examples

Justification: Many scenarios and examples used in the DIOG involve sensitive information, such as the names actual terrorist organizations, and provide insight into targeting, recruitment, or FBI assimilation of such organizations.



Information Withheld Publicly from the DIOG

Redaction: Surveillance and Monitoring Techniques

Justification: Knowledge of these specific criteria could allow for circumvention of the techniques.

Redaction: Time Periods

Justification: Knowledge of time period requirements for investigative techniques could damage the effectiveness of the technique or allow for circumvention. For example, a person who believes he may be under investigation may stop using his cellular phone for the specified period of time, thereby hindering the investigation.

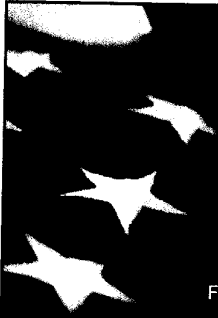
Redaction: Notes

Justification: Notes in the DIOG provide internal guidance to FBI operators and Intelligence Analysts.

Redaction: Internal Web and E-mail Addresses

Justification: Publicly releasing contact information of FBI staff could allow for harassment, spam, or spoofing.

UNCLASSIFIED//FOUO

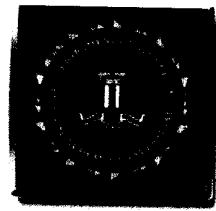


FEDERAL BUREAU OF INVESTIGATION

OVERALL CLASSIFICATION:
UNCLASSIFIED

FBIHQ DIOG Training Session A

UNCLASSIFIED//FOUO



FEDERAL
BUREAU OF
INVESTIGATION



Course Overview

Overall Training Objective:

Provide an instructional foundation on the DIOG and then apply the knowledge gained by using hypothetical examples and scenarios. Upon completing this course of instruction you should have a firm grasp of the concepts and principles underpinning the DIOG.



Course Overview

Participation Standards:

Questions are welcome; however, if your question is about a specific set of facts that may divert the training objective, please direct your question to one of the Training team members at a break for a response.

During the scenario exercises, participants will be called upon to provide their response to particular facts or circumstances. Each Unit/Section should select a representative to speak for the Unit/Section and rotate that responsibility among the group. The scenarios are meant to prompt discussion, but the presenters must keep the scenario moving forward. Please understand that everyone may not be able to voice their perspective in the group setting. Keep in mind there may be several avenues to reach the same justified conclusion. You may use your handouts and training aids to inform your decision.



Course Overview

Course Completion:

- You must complete the entire mandatory 16.5 hours of training. You must score an 80% or higher to pass. You will be notified of your score via e-mail. If you do not pass the first time, you will be permitted to take the test again.
- Please annotate on the attendance sheet your presence at the training if you pre-registered. If you did not pre-register, please print your name, division, and the items requested on the attendance roster.
- After the course is complete, you will be receiving a survey e-mail containing questions that will test your knowledge and understanding of the material presented. The test is open book.



AGG-Dom: Overview

- Provides ability to FBI authorities to be more proactive and preventative, and the flexibility to deal with complex threats that do not fall neatly into individual programs
- Provides clarity and improves compliance by combining several sets of guidelines into one consistent set of guidelines
- Removes discrepancies, sets uniform rules for criminal, national security, and foreign intelligence collection cases. Each program will have a program-specific policy guide (PG)



AGG-Dom: Overview

- Reduces reporting requirements, particularly in the national security area
- Recognizes Special Events and Domain Management as part of the FBI's mission
- Recognizes the FBI's obligation to provide investigative assistance and joint operational support to other agencies, including the U.S. intelligence community
- Creates a new category outside of predicated investigations named "Assessments"



Policy Environment for Domestic Operations

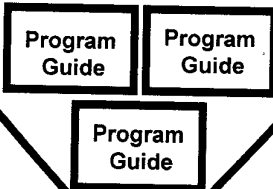
Constitution, Statutes, and Executive Orders

AG GUIDELINES (AGG-Dom)

Apply to domestic national security and criminal investigative activities, including interagency coordination and intelligence analysis.

FBI's Domestic Investigations and Operations Guide (DIOG)

Program Policy Implementation Guides





DIOG Section 1: Scope & Purpose

- **DIOG applies to all investigative and intelligence collection activities conducted by the FBI**
 - within the United States
 - in the United States territories
 - outside the territories of all countries
- **DIOG does not apply to investigative and intelligence collection activities of the FBI in foreign countries**
 - governed by AGGs for Extraterritorial FBI Operations (national security and criminal)



DIOG Section 1: Scope & Purpose

- The primary purpose of the AGG-DOM and the DIOG is to standardize policy so that criminal, national security and foreign intelligence investigative activities are performed in a legal and consistent manner
- The DIOG replaces numerous FBI manuals, electronic communications, letterhead memoranda and other policy documents. The DIOG is located on the Corporate policy Office (CPO) Policy and Guidance Library web site
- The changes implemented by the DIOG better equip you to protect the people of the United States against crime and threats to the national security
- The DIOG stresses the importance of oversight and self-regulation to ensure compliance



DIOG Section 2: General Authorities & Principles

- **The AGG-Dom replaces six guidelines:**
 - The Attorney General's Guidelines on General Crimes, Racketeering Enterprise and Terrorism Enterprise Investigations (May 30, 2002)
 - The Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection (October 31, 2003) *
 - The Attorney General's Supplemental Guidelines for Collection, Retention, and Dissemination of Foreign Intelligence (November 29, 2006)



DIOG Section 2: General Authorities & Principles

- **The AGG-Dom also replaces:**
 - The Attorney General Procedure for Reporting and Use of Information Concerning Violations of Law and Authorization for Participation in Otherwise Illegal Activity in FBI Foreign Intelligence, Counterintelligence or International Terrorism Intelligence Investigations (August 8, 1988) *
 - The Attorney General's Guidelines for Reporting on Civil Disorders and Demonstrations Involving a Federal Interest (April 5, 1976)
 - The Attorney General's Procedures for Lawful, Warrantless Monitoring of Verbal Communications (May 30, 2002) (only portion applicable to FBI)



DIOG Section 2: General Authorities & Principles

Note: Regarding Extraterritorial FBI's Operations, the AGG-Dom did not repeal or supersede certain portions of the prior guidelines (marked * in prior slides). These national security extraterritorial portions continue to remain in effect pending the approval of new Attorney General's Guidelines for Extraterritorial FBI Operations for both national security and criminal investigations. Additionally, the classified Attorney General Guidelines for Extraterritorial FBI Operations and Criminal Investigations (1993) continue to remain in effect pending approval of the new guidelines.



DIOG Section 2: General Authorities & Principles

The FBI is authorized to:

- Conduct investigations and collect evidence (criminal and national security) and collect foreign intelligence (AGG-Dom, Part II)
- Provide investigative assistance to federal, state, local, tribal, and foreign agencies (AGG-Dom, Part III) and (DIOG Section 12)
- Collect information necessary for and conduct intelligence analysis & planning (AGG-Dom, Part II & IV) and (DIOG Section 15)
- Retain and share information (AGG-Dom, Part VI) and (DIOG Section 14)



DIOG Section 2: General Authorities & Principles

The word “Assessment” has two distinct meanings:

- The AGG-Dom authorizes as an investigative activity an “assessment” which requires an authorized purpose and objective as discussed in DIOG Section 5.
- The U.S. intelligence community uses the word “assessment” to describe written intelligence products as discussed in DIOG Section 15.7.B.



DIOG Section 2: General Authorities & Principles

- **The FBI is an intelligence agency as well as a law enforcement agency**
- **The FBI is authorized to engage in intelligence analysis and planning, using all lawful sources of information:**
 - development of overviews and analysis
 - research and analysis to produce reports and assessments
 - operate intelligence systems that facilitate and support investigations through ongoing compilation and analysis of data and information



DIOG Section 2: General Authorities & Principles

- **The FBI is the “lead federal agency” in the following areas:**
 - Federal Crimes of Terrorism (listed in DIOG Section 2.4.C)
 - Other non-Terrorism federal crimes (listed in DIOG Section 2.4.D)
 - Counterintelligence and Espionage (listed in DIOG Section 2.4.F)
 - Criminal Investigations (some listed in DIOG Section 2.4.G; see also CID PGs)



DIOG Section 2: General Authorities & Principles

Departures from the AGG – Dom:

In Advance: FBI Director, Deputy Director, or EAD (NSB or Criminal Cyber Response and Services Branch) must approve with notice to the General Counsel.

In Emergency: Approving authority who authorizes the departure must give notice as soon thereafter as practical to Director, Deputy Director or EAD with notice to General Counsel – OGC must keep records of all departures to advise DOJ, as required.



DIOG Section 2: General Authorities & Principles

Departures from the DIOG:

In Advance: Appropriate substantive AD or DAD must approve with notice to the General Counsel or appropriate Deputy General Counsel (DGC).

In Emergency: Approving authority who authorizes the departure must give notice as soon thereafter as practical; SAC or HQ Section Chief must provide written notice to appropriate substantive AD and the General Counsel.



DIOG Section 2: General Authorities & Principles

The AGG-Dom and DIOG apply to all FBI domestic investigations and operations conducted by “FBI employees” – defined as:

- applicable support personnel
- intelligence analysts
- special agents
- task force officers (TFO)
- detailees
- FBI contractors
- confidential human sources (CHS)



DIOG Section 2: General Authorities & Principles

Authorities of an FBI Special Agent:

1. Investigate violations of the laws, including the criminal drug laws, of the United States (21 U.S.C. § 871; 28 U.S.C. §§ 533, 534 and 535; 28 C.F.R. § 0.85)
2. Collect evidence in cases in which the United States is or may be a party in interest (28 C.F.R. § 0.85 [a]) as redelegated through exercise of the authority contained in 28 C.F.R. § 0.138 to direct personnel in the FBI
3. Make arrests (18 U.S.C. §§ 3052 and 3062)
4. Serve and execute arrest warrants and seize property under warrant; issue and/or serve administrative subpoenas; serve subpoenas issued by other proper authority; and make civil investigative demands (18 U.S.C. §§ 3052, 3107; 21 U.S.C. § 876; 15 U.S.C. § 1312)



DIOG Section 2: General Authorities & Principles

Authorities of an FBI Special Agent (cont.):

5. Carry firearms (18 U.S.C. § 3052)
6. Administer oaths to witnesses attending to testify or depose in the course of investigations of frauds on or attempts to defraud the United States or irregularities or misconduct of employees or agents of the United States (5 U.S.C. § 303)
7. Seize property subject to seizure under the criminal and civil forfeiture laws of the United States (e.g., 18 U.S.C. §§ 981 and 982)
8. Perform other duties imposed by law



DIOG Section 2: General Authorities & Principles

The AGG-Dom did not limit other authorized FBI activities, such as:

- Conducting background checks and inquires concerning applicants and employees under federal personnel security programs
- Maintenance and operation of national criminal records systems and preparation of national crime statistics
- Forensic assistance and administration functions of the FBI Laboratory



DIOG Section 3: FBI's Core Values

The FBI's Core Values are:

- Rigorous obedience to the U.S. Constitution
- Respect for the dignity of all those we protect
- Compassion
- Fairness
- Uncompromising personal integrity and institutional integrity
- Accountability by accepting responsibility for our actions and decisions and their consequences
- Leadership, by example, both personal and professional



DIOG Section 3: Compliance

Everyone's Responsibility:

- To learn and understand the laws, rules and regulations that govern their activities
- To fully comply with all laws, rules and regulations governing investigations, operations, programs and activities
- To report to proper authority any known or suspected failures to adhere to the law, rules or regulations



DIOG Section 3: Deputy Director Roles and Responsibilities

DIOG Section 3.2:

- DD is the proponent of the DIOG and subordinate implementing procedural directives and specific policy implementation guides (PGs)
- DD has oversight of DIOG compliance, monitoring and auditing processes
- DD has responsibility for DIOG training
- DD, through the Corporate Policy Office (CPO), will ensure the DIOG is updated one year from implementation, and every three years thereafter



DIOG Section 3: Special Agent, Intelligence Analyst, Task Force Officer, FBI Contractor, and Others - Roles and Responsibilities

DIOG Section 3.3:

- Comply with AGG-Dom and DIOG standards for initiation, conducting, and closing investigative activity; collection activity; or use of an investigative method
- Obtain training on DIOG standards relevant to their position and perform activities consistent with those standards
- Ensure all investigative activity complies with all laws and policy
- Identify victims, offer FBI assistance, and furnish information to the FBI Victim Specialist



DIOG Section 3: Special Agent, Intelligence Analyst, Task Force Officer, FBI Contractor, and Others - Roles and Responsibilities

(Continued – DIOG Section 3.3)

- Ensure civil liberties and privacy are protected throughout the assessment or investigative process
- Conduct no investigative activity solely on the basis of activities protected by the 1st Amendment or solely on the basis of race, ethnicity, national origin or religion of the subject
- Report non-compliance to the proper authority



DIOG Section 3: Supervisor Roles and Responsibilities

DIOG Section 3.4.A – Supervisor Defined:

- Field Office or FBIHQ personnel, including: SIA, SSA, SSRA, UC, ASAC, ASC, SAC, DAD, AD, ADIC, and EAD



UNCLASSIFIED//FOUO

DIOG Section 3: Supervisor Roles and Responsibilities

DIOG Section 3.4.B - Supervisor Responsibilities:

- Determine whether the DIOG standards are satisfied for initiating, approving, conducting and closing an investigative activity, collection activity, or investigative method
- Ensure all investigative activity complies with all laws and policy
- Obtain training on DIOG standards relevant to their position and conform their decisions to those standards
- Ensure civil liberties and privacy are protected throughout the assessment or investigative process

UNCLASSIFIED//FOUO

29



DIOG Section 3: Supervisor Roles and Responsibilities

Continued DIOG Section 3.4.B - Supervisor Responsibilities:

- If encountering a practice that does not comply with the law, rules, or regulations, the supervisor must:
 - 1. report that compliance concern to the proper authority
 - 2. take action to maintain compliance, when necessary
- Ensure no retaliation or adverse action is taken against persons who raise compliance concerns



DIOG Section 3: Supervisor Roles and Responsibilities

DIOG Section 3.4.C - Supervisory Delegation:

- Any DIOG requirement imposed on a Supervisor may be delegated/performed by a designated Acting, Primary, or Secondary Relief supervisor as indicated below, unless specified otherwise by federal statute, EO, PD, AGG, FBI Policy or any other regulation.
 - Supervisor may delegate authority to a supervisor one level junior to himself/herself (e.g. SAC to ASAC; or SC to Assistant/SC)
 - Must identify the task delegated
 - Must identify the supervisory position given approval authority
 - Must be in writing
 - Must be retained appropriately
 - Higher level Supervisors in the same chain-of-command as the original supervisor may approve a particular activity without written delegation documentation



DIOG Section 3: Supervisor Roles and Responsibilities

DIOG Section 3.4.D - Investigative File Reviews:

- Conducted by full-time supervisors or primary relief supervisors with subordinates
 - (other relief supervisors must have written SAC authority to conduct)
- Conducted with all Agents, Resident Agents, TFOs, analysts, detailees, and FBI contractors, as appropriate
- Conducted in-person or by telephone when necessary
- Conducted in private
- Documented/noted on ACS ICMC report, FD-71 or Guardian
- Conducted at least every 60 days for Probationary Agents, recommended every 30 days



DIOG Section 3: Supervisor Roles and Responsibilities

Assessment Justification/File Reviews:

- Conducted for every 30 day period for Type 1 and 2 Assessments
 - (with 10 additional days to complete and document)
- Conducted for every 90 day period for Type 3, 4, and 6 Assessments
 - (with 30 additional days to complete and document)
- Supervisor Must:
 - Evaluate progress made toward the achievement of authorized purpose and objective
 - Ensure activities that occurred during prior period were appropriate
 - Determine whether it is reasonably likely that information may be obtained that is relevant to the authorized objective – thus warranting an extension for another 30/90 day period
 - Determine whether adequate predication has been developed to open a predicated investigation
 - Determine whether the assessment should be terminated



DIOG Section 3: Supervisor Roles and Responsibilities

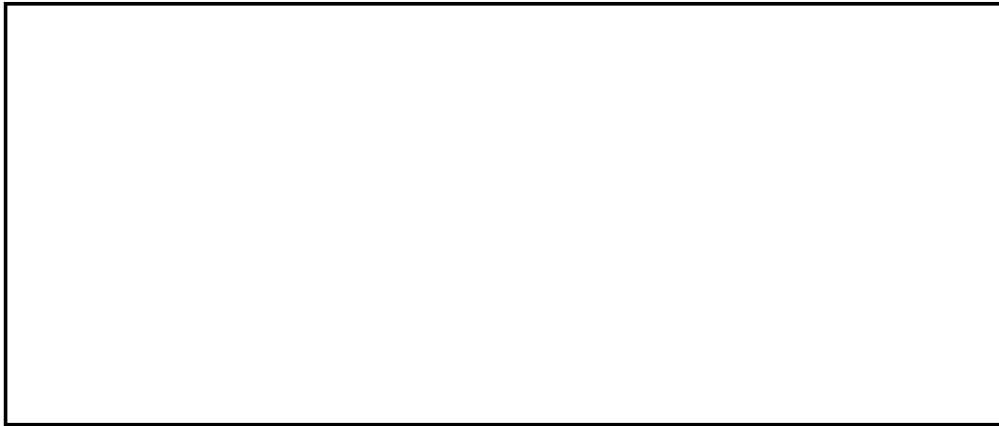
Predicated (Preliminary and Full) Investigation File Reviews:

- Conducted for every 90 day period
 - (with 30 additional days to complete and document)
- Supervisor Must:
 - Evaluate progress made toward the achievement of authorized purpose and objective
 - Ensure activities that occurred during prior period were appropriate
 - Determine whether it is reasonably likely that information may be obtained that is relevant to the authorized objective – thus warranting an extension for another 90 day period
 - Determine whether adequate predication has been developed to open/or continues to justify a predicated investigation



DIOG Section 3: Unaddressed Work

-
-
-
-



Note: the FD-71 provides a new mechanism to assign an Assessment to an electronic Unaddressed Work File in the appropriate classification

b2
b7E



DIOG Section 3: CDC's Role and Responsibilities

CDC's Role and Responsibilities:

1. Must review all Assessments, Preliminary Investigations (PI) and Full Investigations (FI) that involve a "Sensitive Investigative Matter" (SIM)
2. Must review particular investigative methods as mandated by DIOG Section 5 and 11
3. Requirements imposed on the CDC may be performed by an Associate Division Counsel, Legal Advisor, or designated Acting CDC. All delegations must be in writing and retained appropriately.



DIOG Section 3: CDC Roles and Responsibilities

CDC Determinations:

The primary purpose of the CDC's review is to ensure the legality of the actions proposed. In this context, the review includes a determination that the:

- Investigative activity is not legally objectionable (can be overruled by OGC)
 - Activity is not based solely on the exercise of 1st Amendment rights or on the race, ethnicity, national origin or religion of the subject
- The investigation is founded upon an "authorized purpose" (Assessments) or have adequate factual predication (Preliminary and Full)
- Advise as to the "wisdom" of the proposed action



DIOG Section 3: CDC Roles and Responsibilities

Continued: CDC Determinations

The CDC's determination is based on facts known at the time of the review and recommendation.

The CDC may require additional reviews or provide guidance as to monitoring the results of investigative activity to ensure that the authorized purpose and/or factual predication remain intact after additional facts are developed.



DIOG Section 3: OGC Roles and Responsibilities

OGC Role: In coordination with the DOJ NSD, the OGC is responsible for conducting regular reviews of all aspects of FBI national security and foreign intelligence activities.

The primary purpose of the OGC's review is to ensure the legality of the actions proposed. These reviews, conducted in the field offices and in HQ Units, broadly examine such activities for compliance with the AGG-Dom and other requirements. In this context, the review includes a determination that the:

- Investigative activity is not legally objectionable (Activity is not based solely on the exercise of 1st Amendment rights or on the race, ethnicity, national origin or religion of the subject)
- The investigation is founded upon an "authorized purpose" (Assessments) or have adequate factual predication (Preliminary and Full) and meets the standards in the DIOG
- Advise as to the "wisdom" of the proposed action



DIOG Section 3: OGC Roles and Responsibilities

Continued: OGC Determinations

- The OGC's determination above is based on facts known at the time of the review and recommendation.
- The OGC may require additional reviews or provide guidance as to monitoring the results of investigative activity to ensure that the authorized purpose and/or factual predication remain in tact after facts are developed



DIOG Section 3: Other Roles and Responsibilities

CPO = Corporate Policy Office: Oversight and Implementation of the DIOG; Report compliance risks to OIC (DIOG Section 3.7)

OIC = Office of Integrity and Compliance: Identify compliance risk areas, adequacy of policy and training programs, monitor DIOG compliance (DIOG Section 3.8)

DCO = Division Compliance Officer: One identified in each Field Office to assist the OIC to identify potential non-compliance risk areas and report them to proper authority and OIC (DIOG Section 3.10)

PM = Program Manager: HQ entity that identifies, prioritizes, and analyzes compliance risks and takes appropriate corrective action (DIOG Section 3.9)



DIOG Section 4: Privacy and Civil Liberties, and Least Intrusive Methods

- Responsibility to protect the American public, not only from crime and terrorism, but also from incursions into their constitutional rights; accordingly, all investigative activities must fully adhere to the Constitution and the principles of civil liberty and privacy.
- Provisions of the AGG-Dom, other AG guidelines, and oversight from DOJ components, are designed to ensure FBI's activities are lawful, appropriate, and ethical, as well as effective in protecting civil liberties and privacy.
- DOJ and FBI's Inspection Division, Office of Integrity and Compliance, the OGC, other Bureau components, and **you** share responsibility for ensuring the FBI meets these goals.



DIOG Section 4: Privacy and Civil Liberties, and Least Intrusive Methods

- No investigation or assessment can be commenced based solely on race, ethnicity, national origin, religion of the subject or the exercise of First Amendment rights.
- Corollary to this AGG requirement is the Privacy Act, which states that each agency that maintains a system of records shall “maintain no record describing how any individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute or by the individual about whom the record is maintained or **unless pertinent to and within the scope of an authorized law enforcement activity.** 5 U.S.C. 552a(e)(7).



DIOG Section 4 Scenario

-

- What can you do with this information?

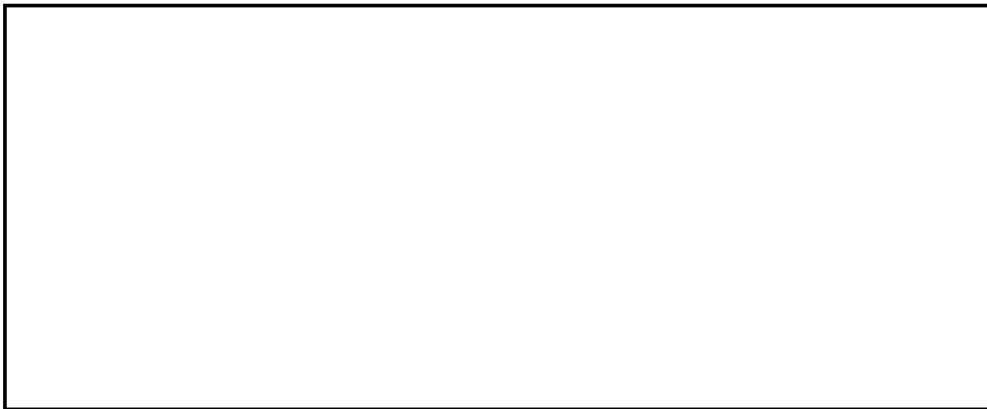
-
-
-
-

b2
b7E



DIOG Section 4 Scenario

-
-



b2
b7E



DIOG Section 4: Privacy and Civil Liberties, and Least Intrusive Methods

FIRST AMENDMENT RIGHTS:

Individuals or groups who communicate with each other or with members of the public in any form in pursuit of social or political causes—such as opposing war or foreign policy, protesting government actions, promoting certain religious beliefs, championing particular local, national, or international causes, or a change in government through non-criminal means, and actively recruit others to join their causes—have a fundamental constitutional right to do so. An assessment may not be initiated based solely on the exercise of these First Amendment rights. If, however, a group exercising its First Amendment rights also threatens or advocates violence or destruction of property, an assessment would be appropriate



DIOG Section 4: Privacy and Civil Liberties, and Least Intrusive Methods

FIRST AMENDMENT RIGHTS (cont.):

- No investigative activity, including assessments, may be taken solely on the basis of activities that are protected by the First Amendment or on the race, ethnicity, national origin or religion of the subject.
- If an assessment or predicated investigation touches on or is partially motivated by First Amendment activities, race, ethnicity, national origin or religion, it is particularly important to identify and document the basis for the assessment with clarity



DIOG Section 4: Privacy and Civil Liberties, and Least Intrusive Methods

All activities must be consistent with the Attorney General's 2003 Guidance Regarding the Use of Race by Federal Law Enforcement Agencies (forbids the use of racial profiling and requires activities involving the investigation or prevention of threats to the national security to comply with the Constitution and laws of the United States)

The DIOG stresses several points in each section:

- No investigation or assessment can be commenced based solely on race, ethnicity, national origin, religion, or exercise of First Amendment rights
- The FBI must use the least intrusive method that is feasible under the circumstances
- In connection with Foreign Intelligence collection, agents must operate openly and consensually with U.S. Persons, to the extent practicable
- All investigative activities must have an "authorized purpose"



DIOG Section 4: Use of Race or Ethnicity

DIOG Guidance on use of Race or Ethnicity

As to individuals:

1. Permits the consideration of ethnic and racial identity information based on specific reporting;
2. The race or ethnicity of suspected members, associates, or supporters of an ethnic-based gang or criminal enterprise may be collected when gathering information about or investigating the organization; or
3. Ethnicity may be considered in evaluating whether a subject is—or is not—a possible associate of a criminal or terrorist group that is known to be comprised of members of the same ethnic grouping—as long as it is not the dominant factor for focusing on a particular person



DIOG Section 4: Use of Race or Ethnicity

DIOG Guidance on use of Race or Ethnicity

As to a community:

1. Collecting and analyzing demographics – if these locations will reasonably aid the analysis of potential threats and vulnerabilities, and, overall, assist domain awareness
2. Geo-Mapping ethnic/racial demographics – if properly collected
3. General ethnic/racial behavior – cannot be collected, unless it bears a rational relationship to a valid investigative or analytical need
4. Specific and relevant ethnic behavior
5. Exploitive ethnic behavior – by criminal or terrorist groups



DIOG Section 4: Least Intrusive Investigative Method

The AGG-DOM and the DIOG require that the “least intrusive” means or method be considered and, if operationally sound and effective, used to obtain intelligence or evidence in lieu of a more intrusive method



DIOG Section 4: Privacy and Civil Liberties, and Least Intrusive Methods

By emphasizing the use of less intrusive means, employees will be able to balance:

Our need for evidence/intelligence

vs.

Mitigating potential negative impact on the privacy and civil liberties of people/public



DIOG Section 4: Privacy and Civil Liberties, and Least Intrusive Methods

Primary factor in determining “intrusiveness”:

- The degree of procedural protection that the law and the AGG-DOM provide for the use of the particular method.
 - Examples of “more intrusive” methods: Search Warrants, wiretaps, UCOs
 - Examples of “less intrusive” methods: checks of government databases, state or local criminal record checks, commercial databases, interviews



DIOG Section 4: Privacy and Civil Liberties, and Least Intrusive Methods

Items to consider when determining the relative intrusiveness of an investigative method:

- Is method permitted prior to the initiation of an assessment?
- Is the method relevant to the assessment or investigation?
- Will the information collected or obtained likely further the investigative objective?
- What alternatives exist for gathering the same information?
- Are those alternatives relatively less intrusive?
- What time span is involved in using the investigative method (days, weeks, months)?
- What confidence level is associated with the information gathered using the investigative method?
- Will the method resolve a pending investigative issue quickly?



DIOG Section 4: Least Intrusive Investigative Method

Factors to Determine “Intrusiveness”:

1. Nature of the information sought
2. Scope of the information sought
3. Scope of the use of the investigative method
4. Source of the information sought
5. Risk of public exposure



DIOG Section 5 & 11: Investigative Methods

Authorized Methods for Assessments and Predicated Investigations

Note: Red indicates methods not allowed under a particular operational activity; Green indicates methods allowed.

Assessments

Preliminary
InvestigationsFull
Investigations

Obtain publicly available information

Access and examine FBI and other DOJ records, and obtain information from any FBI or DOJ personnel

Access and examine records maintained by, and request information from, other federal, state, local, tribal, or foreign governmental entities or agencies

Use online services and resources (whether nonprofit or commercial)

Use and recruit human sources in conformity with AG Guidelines Regarding the Use of FBI Confidential Human Sources

Interview or request information from members of the public and private entities [includes pretextual interviews]

Accept information voluntarily provided by governmental or private entities

Engage in observation or surveillance not requiring a court order

Mail covers

Physical searches of personal or real property where a warrant or court order is not legally required because there is no reasonable expectation of privacy (e.g., trash covers)

Consensual monitoring of communications, including consensual computer monitoring, is subject to legal review by the CDC or the FBI OGC. Where a sensitive monitoring circumstance is involved, monitoring must be approved by the Criminal Division or, if the investigation concerns foreign intelligence or a threat to the national security, by the National Security Division

Use of closed-circuit television, direction finders, and other monitoring devices, subject to legal review by the CDC or FBI OGC

Polygraph examinations

Undercover operations

Compulsory process as authorized by law, including Federal Grand Jury and other subpoenas and National Security Letters (Federal Grand Jury subpoenas for telephone and electronic mail subscriber records can be used during type 1 and 2 Assessments only)

Accessing stored wire and electronic communications and transactional records

Use of pen registers and trap and trace devices

Electronic surveillance

Foreign Intelligence collection under Title VII of FISA

Physical searches, including mail openings, where a warrant or court order is legally required because there is an expectation of privacy



Investigative Methods/Approvals Chart

			Assessments	Predicated	Foreign Intelligence
1	59A	Obtain publicly available information Taking a UCE to attend a religious service	None Required Not Permitted	None Required SSA Approval	None Required SSA Approval
2	59B	Physical surveillance of person or group (Consult the DIOG for handheld photo and video surveillance with no reasonable expectation of privacy)	[Redacted] consult DIOG for requirements	None Required	None Required
		[Redacted]	[Redacted]	ASAC Approval	ASAC Approval
3	59C	Access and examine FBI and other Department of Justice (DOJ) records, and obtain information from any FBI or other DOJ personnel	None Required	None Required	None Required
4	59D	Access and examine records maintained by, and request information from, other federal, state, local, or tribal, or foreign government entities or agencies	None (Unless such approval is required by MOU or other agreements)	None (Unless such approval is required by MOU or other agreements)	None (Unless such approval is required by MOU or other agreements)
5	59E	Use online services and resources (whether nonprofit or commercial)	None Required	None Required	None Required
6	59F	Interview or request information from members of the public and private entities	None Required except for contact with represented persons, members of U.S. Congress, or their staffs, White House personnel, or other substantive division requirements	None Required except for contact with represented persons, members of U.S. Congress, or their staffs, White House personnel, or other substantive division requirements	None Required except for contact with represented persons, members of U.S. Congress, or their staffs, White House personnel, or other substantive division requirements
7	59G	Accept information voluntarily provided by governmental or private entities	None Required	None Required	None Required
8	59H	Use and recruit human source Taking a CHS to attend a religious service	None Required (utilize [Redacted]) SAC Approval	None Required (utilize Data) SSA Approval	None Required (utilize Data) SSA Approval
9	5.9	Federal Grand Jury subpoenas for telephone or electronic mail subscriber information	US Attorney Office Approval (Type 1 and 2 Assessments Only)	US Attorney Office Approval	Not Permitted
10	59C	Pattern Based Data Mining	SORC	SORC	SORC

b2
b7E



Investigative Methods/Approvals Chart

		Assessments	Predicated	Foreign Intelligence
11	11.3	Mail covers		
12	11.4	Physical searches of personal or real property where a warrant or court order is not legally required because there is no reasonable expectation of privacy (e.g. [redacted])		
13	11.5	Consensual monitoring of communications, including consensual computer monitoring	Not Permitted	CDC or OGC Review SSA Approval
14	11.5	Consensual monitoring of communications, including consensual computer monitoring, with a sensitive monitoring circumstance	Not Permitted	CDC or OGC Review, SAC Approval, DOJ Criminal or DOJ NSD Approval
15	11.6	Use of closed-circuit television, direction finders, and other monitoring devices		
16	11.7	Polygraph examinations		
17	11.8	Undercover operations, Group II		
18	11.8	Undercover operations, Group I		
19	11.9	Compulsory process as authorized by law, Federal Grand Jury and trial subpoenas		
20	11.9	Administrative Subpoenas: Drugs		
		Administrative Subpoenas: Sexual Exploitation	Not Permitted	
		Administrative Subpoenas: Healthcare Fraud		
21	11.9	National Security Letters		
22	11.10	Accessing stored wire and electronic communications and transactional records	Not Permitted	Statute/Court Order, Consult DIOG
				Not Permitted
23	11.11	Use of pen registers and trap and trace devices	Not Permitted	FISA Court or District Court Order
24	11.12	Electronic surveillance		Only Available for Non-USPER by FISA Court order
25	11.13	Physical searches, where there is reasonable expectation of privacy, including mail openings		
26	11.14	Acquisition of foreign intelligence information in conformity with Title VII of the Foreign Intelligence Surveillance Act		

b2
b7E

UNCLASSIFIED//FOUO



FEDERAL BUREAU OF INVESTIGATION

OVERALL CLASSIFICATION:

FBIHQ DIOG Training Session A



FEDERAL
BUREAU OF
INVESTIGATION

UNCLASSIFIED//FOUO



UNCLASSIFIED//FOUO

Course Overview

Overall Training Objective:

Provide an instructional foundation on the DIOG and then apply the knowledge gained by using hypothetical examples and scenarios. Upon completing this course of instruction you should have a firm grasp of the concepts and principles underpinning the DIOG.

UNCLASSIFIED//FOUO

2



UNCLASSIFIED//FCUO

Course Overview

Participation Standards:

Questions are welcome; however, if your question is about a specific set of facts that may divert the training objective, please direct your question to one of the Training team members at a break for a response.

During the scenario exercises, participants will be called upon to provide their response to particular facts or circumstances. Each Unit/Section should select a representative to speak for the Unit/Section and rotate that responsibility among the group. The scenarios are meant to prompt discussion, but the presenters must keep the scenario moving forward. Please understand that everyone may not be able to voice their perspective in the group setting. Keep in mind there may be several avenues to reach the same justified conclusion. You may use your handouts and training aids to inform your decision.

UNCLASSIFIED//FCUO

3



UNCLASSIFIED//FOUO

Course Overview

Course Completion:

- You must complete the entire mandatory 16.5 hours of training. You must score an 80% or higher to pass. You will be notified of your score via e-mail. If you do not pass the first time, you will be permitted to take the test again.
- Please annotate on the attendance sheet your presence at the training if you pre-registered. If you did not pre-register, please print your name, division, and the items requested on the attendance roster.
- After the course is complete, you will be receiving a survey e-mail containing questions that will test your knowledge and understanding of the material presented. The test is open book.

UNCLASSIFIED//FOUO



UNCLASSIFIED//FOUO

AGG-Dom: Overview

- Provides ability to FBI authorities to be more proactive and preventative, and the flexibility to deal with complex threats that do not fall neatly into individual programs
- Provides clarity and improves compliance by combining several sets of guidelines into one consistent set of guidelines
- Removes discrepancies, sets uniform rules for criminal, national security, and foreign intelligence collection cases. Each program will have a program-specific policy guide (PG)

UNCLASSIFIED//FOUO

5



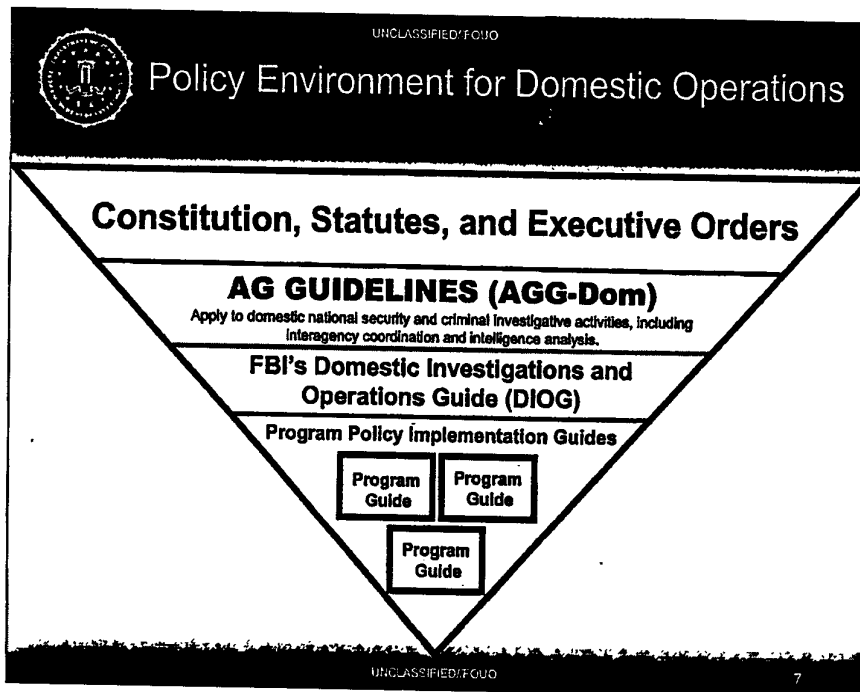
UNCLASSIFIED//FOUO

AGG-Dom: Overview

- Reduces reporting requirements, particularly in the national security area
- Recognizes Special Events and Domain Management as part of the FBI's mission
- Recognizes the FBI's obligation to provide investigative assistance and joint operational support to other agencies, including the U.S. intelligence community
- Creates a new category outside of predicated investigations named "Assessments"

UNCLASSIFIED//FOUO

6



Teaching Point:

FBIHQ Division Program Policy Implementation Guides (PG):

- Cannot be less restrictive than the DIOG
- Must comply with the policy contained in the DIOG
- Requests for program policy deviations from the DIOG must be reviewed by the OGC and approved by the Deputy Director



UNCLASSIFIED//FCUO

DIOG Section 1: Scope & Purpose

- **DIOG applies to all investigative and intelligence collection activities conducted by the FBI**
 - within the United States
 - in the United States territories
 - outside the territories of all countries
- **DIOG does not apply to investigative and intelligence collection activities of the FBI in foreign countries**
 - governed by AGGs for Extraterritorial FBI Operations (national security and criminal).

UNCLASSIFIED//FCUO

8



UNCLASSIFIED//FOUO

DIOG Section 1: Scope & Purpose

- The primary purpose of the AGG-DOM and the DIOG is to standardize policy so that criminal, national security and foreign intelligence investigative activities are performed in a legal and consistent manner
- The DIOG replaces numerous FBI manuals, electronic communications, letterhead memoranda and other policy documents. The DIOG is located on the Corporate policy Office (CPO) Policy and Guidance Library web site
- The changes implemented by the DIOG better equip you to protect the people of the United States against crime and threats to the national security
- The DIOG stresses the importance of oversight and self-regulation to ensure compliance

UNCLASSIFIED//FOUO

9



UNCLASSIFIED//FOUO

DIOG Section 2: General Authorities & Principles

- **The AGG-Dom replaces six guidelines:**
 - The Attorney General's Guidelines on General Crimes, Racketeering Enterprise and Terrorism Enterprise Investigations (May 30, 2002)
 - The Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection (October 31, 2003) *
 - The Attorney General's Supplemental Guidelines for Collection, Retention, and Dissemination of Foreign Intelligence (November 29, 2006)

UNCLASSIFIED//FOUO

10



UNCLASSIFIED//FOUO

DIOG Section 2: General Authorities & Principles

- **The AGG-Dom also replaces:**
 - The Attorney General Procedure for Reporting and Use of Information Concerning Violations of Law and Authorization for Participation in Otherwise Illegal Activity in FBI Foreign Intelligence, Counterintelligence or International Terrorism: Intelligence Investigations (August 8, 1988) *
 - The Attorney General's Guidelines for Reporting on Civil Disorders and Demonstrations Involving a Federal Interest (April 5, 1976)
 - The Attorney General's Procedures for Lawful, Warrantless Monitoring of Verbal Communications (May 30, 2002) (only portion applicable to FBI)

UNCLASSIFIED//FOUO

11



UNCLASSIFIED//FOUO

DIOG Section 2: General Authorities & Principles

Note: Regarding Extraterritorial FBI's Operations, the AGG-Dom did not repeal or supersede certain portions of the prior guidelines (marked * in prior slides). These national security extraterritorial portions continue to remain in effect pending the approval of new Attorney General's Guidelines for Extraterritorial FBI Operations for both national security and criminal investigations. Additionally, the classified Attorney General Guidelines for Extraterritorial FBI Operations and Criminal Investigations (1993) continue to remain in effect pending approval of the new guidelines.

UNCLASSIFIED//FOUO

12



UNCLASSIFIED//FOUO

DIOG Section 2: General Authorities & Principles

The FBI is authorized to:

- Conduct investigations and collect evidence (criminal and national security) and collect foreign intelligence (AGG-Dom, Part II)
- Provide investigative assistance to federal, state, local, tribal, and foreign agencies (AGG-Dom, Part III) and (DIOG Section 12)
- Collect information necessary for and conduct intelligence analysis & planning (AGG-Dom, Part II & IV) and (DIOG Section 15)
- Retain and share information (AGG-Dom, Part VI) and (DIOG Section 14)

UNCLASSIFIED//FOUO

10



UNCLASSIFIED//FOUO

DIOG Section 2: General Authorities & Principles

The word "Assessment" has two distinct meanings:

- The AGG-Dom authorizes as an investigative activity an "assessment" which requires an authorized purpose and objective as discussed in DIOG Section 5.
- The U.S. intelligence community uses the word "assessment" to describe written intelligence products as discussed in DIOG Section 15.7.B.

UNCLASSIFIED//FOUO

14



UNCLASSIFIED//FOUO

DIOG Section 2: General Authorities & Principles

- **The FBI is an intelligence agency as well as a law enforcement agency**
- **The FBI is authorized to engage in intelligence analysis and planning, using all lawful sources of information:**
 - development of overviews and analysis
 - research and analysis to produce reports and assessments
 - operate intelligence systems that facilitate and support investigations through ongoing compilation and analysis of data and information

UNCLASSIFIED//FOUO

15



UNCLASSIFIED//FOUO

DIOG Section 2: General Authorities & Principles

- **The FBI is the “lead federal agency” in the following areas:**
 - Federal Crimes of Terrorism (listed in DIOG Section 2.4.C)
 - Other non-Terrorism federal crimes (listed in DIOG Section 2.4.D)
 - Counterintelligence and Espionage (listed in DIOG Section 2.4.F)
 - Criminal Investigations (some listed in DIOG Section 2.4.G; see also CID PGs)

UNCLASSIFIED//FOUO

16



UNCLASSIFIED//FOUO

DIOG Section 2: General Authorities & Principles

Departures from the AGG – Dom:

In Advance: FBI Director, Deputy Director, or EAD (NSB or Criminal Cyber Response and Services Branch) must approve with notice to the General Counsel.

In Emergency: Approving authority who authorizes the departure must give notice as soon thereafter as practical to Director, Deputy Director or EAD with notice to General Counsel – OGC must keep records of all departures to advise DOJ, as required.

UNCLASSIFIED//FOUO

17



UNCLASSIFIED//FCUO

DIOG Section 2: General Authorities & Principles

Departures from the DIOG:

In Advance: Appropriate substantive AD or DAD must approve with notice to the General Counsel or appropriate Deputy General Counsel (DGC).

In Emergency: Approving authority who authorizes the departure must give notice as soon thereafter as practical; SAC or HQ Section Chief must provide written notice to appropriate substantive AD and the General Counsel.

UNCLASSIFIED//FCUO

18



UNCLASSIFIED//FOUO

DIOG Section 2: General Authorities & Principles

The AGG-Dom and DIOG apply to all FBI domestic investigations and operations conducted by "FBI employees" – defined as:

- applicable support personnel
- intelligence analysts
- special agents
- task force officers (TFO)
- detailees
- FBI contractors
- confidential human sources (CHS)

UNCLASSIFIED//FOUO

19



UNCLASSIFIED//FOUO

DIOG Section 2: General Authorities & Principles

Authorities of an FBI Special Agent:

1. Investigate violations of the laws, including the criminal drug laws, of the United States (21 U.S.C. § 871; 28 U.S.C. §§ 533, 534 and 535; 28 C.F.R. § 0.85)
2. Collect evidence in cases in which the United States is or may be a party in interest (28 C.F.R. § 0.85 [a]) as redelegated through exercise of the authority contained in 28 C.F.R. § 0.138 to direct personnel in the FBI
3. Make arrests (18 U.S.C. §§ 3052 and 3062)
4. Serve and execute arrest warrants and seize property under warrant; issue and/or serve administrative subpoenas; serve subpoenas issued by other proper authority; and make civil investigative demands (18 U.S.C. §§ 3052, 3107; 21 U.S.C. § 876; 15 U.S.C. § 1312)

UNCLASSIFIED//FOUO

20



UNCLASSIFIED//FCUO

DIOG Section 2: General Authorities & Principles

Authorities of an FBI Special Agent (cont.):

5. Carry firearms (18 U.S.C. § 3052)
6. Administer oaths to witnesses attending to testify or depose in the course of investigations of frauds on or attempts to defraud the United States or irregularities or misconduct of employees or agents of the United States (5 U.S.C. § 303)
7. Seize property subject to seizure under the criminal and civil forfeiture laws of the United States (e.g., 18 U.S.C. §§ 981 and 982)
8. Perform other duties imposed by law

UNCLASSIFIED//FCUO

21



UNCLASSIFIED//FOUO

DIOG Section 2: General Authorities & Principles

The AGG-Dom did not limit other authorized FBI activities, such as:

- Conducting background checks and inquires concerning applicants and employees under federal personnel security programs
- Maintenance and operation of national criminal records systems and preparation of national crime statistics
- Forensic assistance and administration functions of the FBI Laboratory

UNCLASSIFIED//FOUO

22



UNCLASSIFIED//FOUO

DIOG Section 3: FBI's Core Values

The FBI's Core Values are:

- Rigorous obedience to the U.S. Constitution
- Respect for the dignity of all those we protect
- Compassion
- Fairness
- Uncompromising personal integrity and institutional integrity
- Accountability by accepting responsibility for our actions and decisions and their consequences
- Leadership, by example, both personal and professional

UNCLASSIFIED//FOUO

23

Teaching Points: DIOG Section 3.1:

1. Core values must be fully understood, practice, shared, vigorously defended and preserved.
2. By observing core values – FBI will achieve a high level of excellence in performing both our national security and criminal missions.
3. Information for reporting violations is available from the Office of Integrity and Compliance (OIC).



UNCLASSIFIED//FOUO

DIOG Section 3: Compliance

Everyone's Responsibility:

- To learn and understand the laws, rules and regulations that govern their activities
- To fully comply with all laws, rules and regulations governing investigations, operations, programs and activities
- To report to proper authority any known or suspected failures to adhere to the law, rules or regulations

UNCLASSIFIED//FOUO

24

Teaching Point: DIOG Section 3.1:

1. DIOG compliance applies to all FBI employees, task force officers, contractor's etc.
2. May not disregard the law, rule, etc. for sake of expediency.
3. Information for reporting.



UNCLASSIFIED//FCUO

DIOG Section 3: Deputy Director Roles and Responsibilities

DIOG Section 3.2:

- DD is the proponent of the DIOG and subordinate implementing procedural directives and specific policy implementation guides (PGs)
- DD has oversight of DIOG compliance, monitoring and auditing processes
- DD has responsibility for DIOG training
- DD, through the Corporate Policy Office (CPO), will ensure the DIOG is updated one year from implementation, and every three years thereafter

UNCLASSIFIED//FCUO

25

Teaching Point: DD, through the CPO, will review the Program Guides (PGs) for all divisions to ensure compliance with DIOG standards.



UNCLASSIFIED//FOUO

DIOG Section 3: Special Agent, Intelligence Analyst, Task Force Officer, FBI Contractor, and Others - Roles and Responsibilities

DIOG Section 3.3:

- Comply with AGG-Dom and DIOG standards for initiation, conducting, and closing investigative activity; collection activity; or use of an investigative method
- Obtain training on DIOG standards relevant to their position and perform activities consistent with those standards
- Ensure all investigative activity complies with all laws and policy
- Identify victims, offer FBI assistance, and furnish information to the FBI Victim Specialist

UNCLASSIFIED//FOUO

26

Teaching Point:

1. Laws/policy include the Constitution, federal law, Executive Orders, Presidential Directives, AGG-Dom, other AGGs, Treaties, MOAs/MOUs, DIOG and other policy. When in doubt – consult their Supervisor, the CDC or OGC.
2. Victims include those who have suffered direct physical, emotional, or financial harm as a result of the commission of federal crimes.



UNCLASSIFIED//FOUO

DIOG Section 3: Special Agent, Intelligence Analyst, Task Force Officer, FBI Contractor, and Others - Roles and Responsibilities

(Continued – DIOG Section 3.3)

- Ensure civil liberties and privacy are protected throughout the assessment or investigative process
- Conduct no investigative activity solely on the basis of activities protected by the 1st Amendment or solely on the basis of race, ethnicity, national origin or religion of the subject
- Report non-compliance to the proper authority

UNCLASSIFIED//FOUO

27



UNCLASSIFIED//FOUO

DIOG Section 3: Supervisor Roles and Responsibilities

DIOG Section 3.4.A – Supervisor Defined:

- Field Office or FBIHQ personnel, including: SIA, SSA, SSRA, UC, ASAC, ASC, SAC, DAD, AD, ADIC, and EAD

UNCLASSIFIED//FOUO

28



UNCLASSIFIED//FOUO

DIOG Section 3: Supervisor Roles and Responsibilities

DIOG Section 3.4.B - Supervisor Responsibilities:

- Determine whether the DIOG standards are satisfied for initiating, approving, conducting and closing an investigative activity, collection activity, or investigative method
- Ensure all investigative activity complies with all laws and policy
- Obtain training on DIOG standards relevant to their position and conform their decisions to those standards
- Ensure civil liberties and privacy are protected throughout the assessment or investigative process

UNCLASSIFIED//FOUO

29



UNCLASSIFIED//FOUO

DIOG Section 3: Supervisor Roles and Responsibilities

Continued DIOG Section 3.4.B - Supervisor Responsibilities:

- If encountering a practice that does not comply with the law, rules, or regulations, the supervisor must:
 - 1. report that compliance concern to the proper authority
 - 2. take action to maintain compliance, when necessary
- Ensure no retaliation or adverse action is taken against persons who raise compliance concerns

UNCLASSIFIED//FOUO

30

Teaching Points:

1. Should report non-compliance to immediate Supervisor and/or OIC.
2. OIC non-retaliation policy located in the CPO policy and guidance library.



UNCLASSIFIED//FCUO

DIOG Section 3: Supervisor Roles and Responsibilities

DIOG Section 3.4.C - Supervisory Delegation:

- Any DIOG requirement imposed on a Supervisor may be delegated/performed by a designated Acting, Primary, or Secondary Relief supervisor as indicated below, unless specified otherwise by federal statute, EO, PD, AGG, FBI Policy or any other regulation.
 - Supervisor may delegate authority to a supervisor one level junior to himself/herself (e.g. SAC to ASAC; or SC to Assistant/SC)
 - Must identify the task delegated
 - Must identify the supervisory position given approval authority
 - Must be in writing
 - Must be retained appropriately
 - Higher level Supervisors in the same chain-of-command as the original supervisor may approve a particular activity without written delegation documentation

UNCLASSIFIED//FCUO

31

Teaching Points: Question – Can SSA or SIA delegate? No, but an appropriately designated Acting or Relief Supervisor can assume the responsibilities in the absence of the SSA.

DIOG 3.4 C



UNCLASSIFIED//FOUO

DIOG Section 3: Supervisor Roles and Responsibilities

DIOG Section 3.4.D - Investigative File Reviews:

- Conducted by full-time supervisors or primary relief supervisors with subordinates
 - (other relief supervisors must have written SAC authority to conduct)
- Conducted with all Agents, Resident Agents, TFOs, analysts, detailees, and FBI contractors, as appropriate
- Conducted in-person or by telephone when necessary
- Conducted in private
- Documented/noted on ACS ICMC report, FD-71 or Guardian
- Conducted at least every 60 days for Probationary Agents, recommended every 30 days

UNCLASSIFIED//FOUO

32

Teaching Points: ACS Investigative Case management Case Review report.



UNCLASSIFIED//FOUO

DIOG Section 3: Supervisor Roles and Responsibilities

Assessment Justification/File Reviews:

- Conducted for every 30 day period for Type 1 and 2 Assessments
 - (with 10 additional days to complete and document)
- Conducted for every 90 day period for Type 3, 4, and 6 Assessments
 - (with 30 additional days to complete and document)
- Supervisor Must:
 - Evaluate progress made toward the achievement of authorized purpose and objective
 - Ensure activities that occurred during prior period were appropriate
 - Determine whether it is reasonably likely that information may be obtained that is relevant to the authorized objective – thus warranting an extension for another 30/90 day period
 - Determine whether adequate predication has been developed to open a predicated investigation
 - Determine whether the assessment should be terminated

UNCLASSIFIED//FOUO

33

Teaching Points: DIOG Section 5 details file review requirements.



UNCLASSIFIED//FOUO

DIOG Section 3: Supervisor Roles and Responsibilities

Predicated (Preliminary and Full) Investigation File Reviews:

- Conducted for every 90 day period
 - (with 30 additional days to complete and document)
- Supervisor Must:
 - Evaluate progress made toward the achievement of authorized purpose and objective
 - Ensure activities that occurred during prior period were appropriate
 - Determine whether it is reasonably likely that information may be obtained that is relevant to the authorized objective – thus warranting an extension for another 90 day period
 - Determine whether adequate predication has been developed to open/or continues to justify a predicated investigation

UNCLASSIFIED//FOUO

34

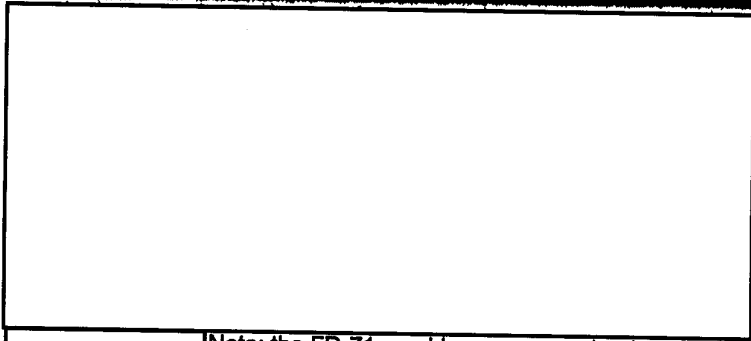
Teaching Points: Probationary Agent File reviews conducted at least every 60 days, recommend 30 days



UNCLASSIFIED//FOUO

DIOG Section 3: Unaddressed Work

-
-
-
-



Note: the FD-71 provides a new mechanism to assign an Assessment to an electronic Unaddressed Work File in the appropriate classification

UNCLASSIFIED//FOUO

35

b2
b7E



UNCLASSIFIED//FOUO

DIOG Section 3: CDC's Role and Responsibilities

CDC's Role and Responsibilities:

1. Must review all Assessments, Preliminary Investigations (PI) and Full Investigations (FI) that involve a "Sensitive Investigative Matter" (SIM)
2. Must review particular investigative methods as mandated by DIOG Section 5 and 11
3. Requirements imposed on the CDC may be performed by an Associate Division Counsel, Legal Advisor, or designated Acting CDC. All delegations must be in writing and retained appropriately.

UNCLASSIFIED//FOUO

36



UNCLASSIFIED//FOUO

DIOG Section 3: CDC Roles and Responsibilities

CDC Determinations:

The primary purpose of the CDC's review is to ensure the legality of the actions proposed. In this context, the review includes a determination that the:

- Investigative activity is not legally objectionable (can be overruled by OGC)
 - Activity is not based solely on the exercise of 1st Amendment rights or on the race, ethnicity, national origin or religion of the subject
- The investigation is founded upon an "authorized purpose" (Assessments) or have adequate factual predication (Preliminary and Full)
- Advise as to the "wisdom" of the proposed action

UNCLASSIFIED//FOUO

37



UNCLASSIFIED//FCUO

DIOG Section 3: CDC Roles and Responsibilities

Continued: CDC Determinations

The CDC's determination is based on facts known at the time of the review and recommendation.

The CDC may require additional reviews or provide guidance as to monitoring the results of investigative activity to ensure that the authorized purpose and/or factual predication remain intact after additional facts are developed.

UNCLASSIFIED//FCUO

38



UNCLASSIFIED//FOUO

DIOG Section 3: OGC Roles and Responsibilities

OGC Role: In coordination with the DOJ NSD, the OGC is responsible for conducting regular reviews of all aspects of FBI national security and foreign intelligence activities.

The primary purpose of the OGC's review is to ensure the legality of the actions proposed. These reviews, conducted in the field offices and in HQ Units, broadly examine such activities for compliance with the AGG-Dom and other requirements. In this context, the review includes a determination that the:

- Investigative activity is not legally objectionable (Activity is not based solely on the exercise of 1st Amendment rights or on the race, ethnicity, national origin or religion of the subject)
- The investigation is founded upon an "authorized purpose" (Assessments) or have adequate factual predication (Preliminary and Full) and meets the standards in the DIOG
- Advise as to the "wisdom" of the proposed action

UNCLASSIFIED//FOUO

39



UNCLASSIFIED//FOUO

DIOG Section 3: OGC Roles and Responsibilities

Continued: OGC Determinations

- The OGC's determination above is based on facts known at the time of the review and recommendation.
- The OGC may require additional reviews or provide guidance as to monitoring the results of investigative activity to ensure that the authorized purpose and/or factual predication remain in tact after facts are developed

UNCLASSIFIED//FOUO

40



UNCLASSIFIED//FOUO

DIOG Section 3: Other Roles and Responsibilities

CPO = Corporate Policy Office: Oversight and Implementation of the DIOG; Report compliance risks to OIC (DIOG Section 3.7)

OIC = Office of Integrity and Compliance: Identify compliance risk areas, adequacy of policy and training programs, monitor DIOG compliance (DIOG Section 3.8)

DCO = Division Compliance Officer: One identified in each Field Office to assist the OIC to identify potential non-compliance risk areas and report them to proper authority and OIC (DIOG Section 3.10)

PM = Program Manager: HQ entity that identifies, prioritizes, and analyzes compliance risks and takes appropriate corrective action (DIOG Section 3.9)

UNCLASSIFIED//FOUO

41



UNCLASSIFIED//FOUO

DIOG Section 4: Privacy and Civil Liberties, and Least Intrusive Methods

- Responsibility to protect the American public, not only from crime and terrorism, but also from incursions into their constitutional rights; accordingly, all investigative activities must fully adhere to the Constitution and the principles of civil liberty and privacy.
- Provisions of the AGG-Dom, other AG guidelines, and oversight from DOJ components, are designed to ensure FBI's activities are lawful, appropriate, and ethical, as well as effective in protecting civil liberties and privacy.
- DOJ and FBI's Inspection Division, Office of Integrity and Compliance, the OGC, other Bureau components, and **you** share responsibility for ensuring the FBI meets these goals.

UNCLASSIFIED//FOUO

42

Teaching Point:

The FBI is a very important agency with dedicated, highly professional, greatly disciplined Government servants. These words, uttered in 1975 by then Attorney General Levi, are just as true today – if not more so – than they were 34 years ago. But when these words were spoken, it was in the context of Senate hearings on the intelligence function of the FBI and the substantial concerns expressed by a parade of witnesses that for the purpose of protecting the national security and preventing violence, the Bureau was engaging in activities that “tread[] on forbidden ground.”

Fashioning investigative activities that navigate between Constitutional requirements and the imperatives of protecting the nation is often a difficult balancing act and one of the hardest issues that an agent or analyst can face is whether and under what circumstances a particular investigative activity is appropriate. The rewards when we find the right balance often go unnoticed by the general public, but the criticism when we don't can be heard far and wide.

The Attorney General Guidelines for Domestic Activities and the implementing Domestic Investigations Operations Guide are built on a history of attempting to fashion the proper balance between investigating crimes and collecting intelligence while protecting the civil liberties of our people. You are sitting here today because it is your job to help educate your colleagues on how to strike the right balance.



UNCLASSIFIED//FOUO

DIOG Section 4: Privacy and Civil Liberties, and Least Intrusive Methods

- No investigation or assessment can be commenced based solely on race, ethnicity, national origin, religion of the subject or the exercise of First Amendment rights.
- Corollary to this AGG requirement is the Privacy Act, which states that each agency that maintains a system of records shall "maintain no record describing how any individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute or by the individual about whom the record is maintained or **unless pertinent to and within the scope of an authorized law enforcement activity.** 5 U.S.C. 552a(e)(7).

UNCLASSIFIED//FOUO

43

Teaching Point:

The first two conditions in the Privacy Act are fairly simply and not typical. If Congress says we can collect and maintain records about how an individual exercises First Amendment rights or if the subject of the record consents, there's no problem – and any resultant records would not be based solely on First Amendment activities.

The purpose of (e)(7) of the Privacy Act, as articulated in the limited legislative history that we have, is to prevent the "collection of protected information not immediately needed, about law-abiding Americans, on the off-chance that Government or the particular agency might possibly have to deal with them in the future." The Act does not define an "authorized law enforcement activity," but the courts have been generous in finding a law enforcement purpose for FBI activities.



UNCLASSIFIED//FCUO

DIOG Section 4 Scenario

-

- **What can you do with this information?**

-

-

-


UNCLASSIFIED//FCUO

44

b2
b7E

Questions continue on next slide

UNCLASSIFIED//FOUO



DIOG Section 4 Scenario

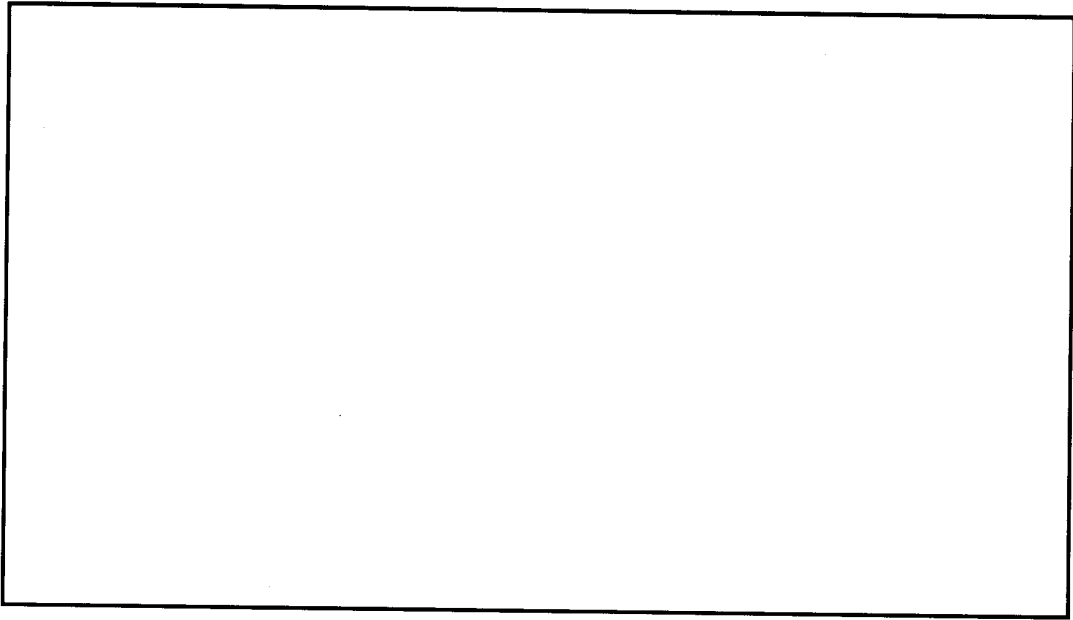
- [Redacted]
- [Redacted]

UNCLASSIFIED//FOUO 45

b2
b7E

Teaching Point:

These are difficult issues, but it is important to understand not only what is permissible, but how to document what action is taken.



b2
b7E



UNCLASSIFIED//FOUO

DIOG Section 4: Privacy and Civil Liberties, and Least Intrusive Methods

FIRST AMENDMENT RIGHTS:

Individuals or groups who communicate with each other or with members of the public in any form in pursuit of social or political causes—such as opposing war or foreign policy, protesting government actions, promoting certain religious beliefs, championing particular local, national, or international causes, or a change in government through non-criminal means, and actively recruit others to join their causes—have a fundamental constitutional right to do so. An assessment may not be initiated based solely on the exercise of these First Amendment rights. If, however, a group exercising its First Amendment rights also threatens or advocates violence or destruction of property, an assessment would be appropriate

UNCLASSIFIED//FOUO

46



UNCLASSIFIED//FOUO

DIOG Section 4: Privacy and Civil Liberties, and Least Intrusive Methods

FIRST AMENDMENT RIGHTS (cont.):

- No investigative activity, including assessments, may be taken solely on the basis of activities that are protected by the First Amendment or on the race, ethnicity, national origin or religion of the subject.
- If an assessment or predicated investigation touches on or is partially motivated by First Amendment activities, race, ethnicity, national origin or religion, it is particularly important to identify and document the basis for the assessment with clarity

UNCLASSIFIED//FOUO

47



UNCLASSIFIED//FOUO

DIOG Section 4: Privacy and Civil Liberties, and Least Intrusive Methods

All activities must be consistent with the Attorney General's 2003 Guidance Regarding the Use of Race by Federal Law Enforcement Agencies (forbids the use of racial profiling and requires activities involving the investigation or prevention of threats to the national security to comply with the Constitution and laws of the United States)

The DIOG stresses several points in each section:

- No investigation or assessment can be commenced based solely on race, ethnicity, national origin, religion, or exercise of First Amendment rights
- The FBI must use the least intrusive method that is feasible under the circumstances
- In connection with Foreign Intelligence collection, agents must operate openly and consensually with U.S. Persons, to the extent practicable
- All investigative activities must have an "authorized purpose"

UNCLASSIFIED//FCUO

48



UNCLASSIFIED//FCUO

DIOG Section 4: Use of Race or Ethnicity

DIOG Guidance on use of Race or Ethnicity

As to individuals:

1. Permits the consideration of ethnic and racial identity information based on specific reporting;
2. The race or ethnicity of suspected members, associates, or supporters of an ethnic-based gang or criminal enterprise may be collected when gathering information about or investigating the organization; or
3. Ethnicity may be considered in evaluating whether a subject is—or is not—a possible associate of a criminal or terrorist group that is known to be comprised of members of the same ethnic grouping—as long as it is not the dominant factor for focusing on a particular person

UNCLASSIFIED//FCUO

49



UNCLASSIFIED//FOUO

DIOG Section 4: Use of Race or Ethnicity

DIOG Guidance on use of Race or Ethnicity

As to a community:

1. Collecting and analyzing demographics – if these locations will reasonably aid the analysis of potential threats and vulnerabilities, and, overall, assist domain awareness
2. Geo-Mapping ethnic/racial demographics – if properly collected
3. General ethnic/racial behavior – cannot be collected, unless it bears a rational relationship to a valid investigative or analytical need
4. Specific and relevant ethnic behavior
5. Exploitive ethnic behavior – by criminal or terrorist groups

UNCLASSIFIED//FOUO

50

Teaching Point:

Specific and relevant ethnic behavior: Intelligence analysis or investigative experience may show that individuals associated with an ethnic based terrorist group or criminal organization conduct activities in certain ways. For example, they may conduct their finances using certain systems, work in certain jobs, come from certain parts of the country that has links to terrorist activities. These are characteristics that can be used when investigating the group or assessing whether there is a terrorist or criminal presence.

Exploitive ethnic behavior: We can collect information that is behavioral or culturally oriented about ethnic or racial communities that is reasonably likely to be exploited by terrorist or criminal groups who hide within those communities in order to engage in their illegal or illicit activities undetected. For example, a cultural tradition of using informal money transfer systems to move money overseas may be exploited by criminal organizations or terrorists.



UNCLASSIFIED//FOUO

DIOG Section 4: Least Intrusive Investigative Method

The AGG-DOM and the DIOG require that the “least intrusive” means or method be considered and, if operationally sound and effective, used to obtain intelligence or evidence in lieu of a more intrusive method

UNCLASSIFIED//FOUO

51

Teaching Point: there is a component of efficiency in being “effective”.

In some instances, a more intrusive method, i.e. use of a CHS, may be more operationally sound and effective for resolving an outstanding investigative need, than a less intrusive method such as acquiring financial records or business records. The totality of the circumstances surrounding the investigative activity plays an important role in considering the use of the least intrusive alternative for obtaining intelligence or evidence. It is a balancing test.



UNCLASSIFIED//FOUO

DIOG Section 4: Privacy and Civil Liberties, and Least Intrusive Methods.

**By emphasizing the use of less intrusive
means, employees will be able to balance:**

Our need for evidence/intelligence

vs.

**Mitigating potential negative impact on the privacy and civil
liberties of people/public**

UNCLASSIFIED//FOUO

52



UNCLASSIFIED//FOUO

DIOG Section 4: Privacy and Civil Liberties, and Least Intrusive Methods

Primary factor in determining "intrusiveness":

- The degree of procedural protection that the law and the AGG-DOM provide for the use of the particular method.
 - Examples of "more intrusive" methods: Search Warrants, wiretaps, UCOs
 - Examples of "less intrusive" methods: checks of government databases, state or local criminal record checks, commercial databases, interviews

UNCLASSIFIED//FOUO

53



UNCLASSIFIED//FCJO

DIOG Section 4: Privacy and Civil Liberties, and Least Intrusive Methods

Items to consider when determining the relative intrusiveness of an investigative method:

- Is method permitted prior to the initiation of an assessment?
- Is the method relevant to the assessment or investigation?
- Will the information collected or obtained likely further the investigative objective?
- What alternatives exist for gathering the same information?
- Are those alternatives relatively less intrusive?
- What time span is involved in using the investigative method (days, weeks, months)?
- What confidence level is associated with the information gathered using the investigative method?
- Will the method resolve a pending investigative issue quickly?

UNCLASSIFIED//FCJO

54



UNCLASSIFIED//FOUO

DIOG Section 4: Least Intrusive Investigative Method

Factors to Determine "Intrusiveness":

1. Nature of the information sought
2. Scope of the information sought
3. Scope of the use of the investigative method
4. Source of the information sought
5. Risk of public exposure

UNCLASSIFIED//FOUO

55



DIOP Section 5 & 11: Investigative Methods

Authorial Note: This table for Assessments and Pretextual Investigations indicates methods used under a particular operational activity; Section 11 indicates methods of e-vo.

Assessments
Pretextual
Investigations
Field
Investigations

Obtain publicly available information

Access and examine FBI and other DOJ records, and obtain information from any FBI or DOJ personnel

Access and examine records maintained by, and request information from, other federal, state, local, tribal, or foreign governmental entities or agencies

Use online services and resources (whether nonprofit or commercial)

Use and recruit human sources in conformity with AG Guidelines Regarding the Use of FBI Confidential Human Sources

Interview or request information from members of the public and private entities [includes pretextual interviews]

Accept information voluntarily provided by governmental or private entities

Engage in observation or surveillance not requiring a court order

Mail covers

Physical searches of personal or real property where a warrant or court order is not legally required because there is no reasonable expectation of privacy (e.g., trash covers)

Consensual monitoring of communications, including consensual computer monitoring, is subject to legal review by the CDC or the FBI OGC. Where a sensitive monitoring circumstance is involved, monitoring must be approved by the Criminal Division or, if the investigation concerns foreign intelligence or a threat to the national security, by the National Security Division

Use of closed-circuit television, direction finders, and other monitoring devices, subject to legal review by the CDC or FBI OGC

Polygraph examinations

Undercover operations

Compulsory process as authorized by law, including Federal Grand Jury and other subpoenas and National Security Letters (Federal Grand Jury subpoenas for telephone and electronic mail subscriber records can be used during type 1 and 2 Assessments only)

Accessing stored wire and electronic communications and transactional records

Use of pen registers and trap and trace devices

Electronic surveillance

Foreign intelligence collection under Title VII of FISA

Physical searches, including mail openings, where a warrant or court order is legally required because there is an expectation of privacy



UNCLASSIFIED//FOUO

Investigative Methods/Approvals Chart

Authorized Method and DIOG Reference*	Approval Levels for Assessments and Predicted Investigations		
	Assessments	Predicted	Foreign Intelligence
1. 5.8A Obtain publicly available information	None Required	None Required	None Required
Testing a VICE to attend a religious service	Not Permitted	SSA Approval	SSA Approval
2. 5.9B Physical surveillance of a person or group (Consult the DIOG for hand-held photo and video surveillance with no reasonable expectation of privacy)	DIOG for requirements	None Required	None Required
		ASAC Approval	ASAC Approval
	ASAC Approval	ASAC Approval	ASAC Approval
3. 5.9C Access and examine FBI and other Department of Justice (DOJ) records, and obtain information from any FBI or other DOJ personnel	None Required	None Required	None Required
4. 5.9D Access and examine records maintained by, and request information from, other federal, state, local, or tribal, or foreign governmental entities or agencies	None (Unless such approval is required by MOU or other agreements)	None (Unless such approval is required by MOU or other agreements)	None (Unless such approval is required by MOU or other agreements)
5. 5.9E Use online services and resources (whether nonprofit or commercial)	None Required	None Required	None Required
6. 5.9F Interview or request information from members of the public and private entities	None Required except for contact with represented persons, members of U.S. Congress, or their staffs, White House personnel, or other substantive division requirements	None Required except for contact with represented persons, members of U.S. Congress, or their staffs, White House personnel, or other substantive division requirements	None Required except for contact with represented persons, members of U.S. Congress, or their staffs, White House personnel, or other substantive division requirements
7. 5.9G Accept information voluntarily provided by governmental or private entities	None Required	None Required	None Required
8. 5.9H Use and recruit human sources	None Required (unless [redacted])	None Required (unless Delta)	None Required (unless Delta)
Testing a CHS to attend a religious service	SAC Approval	SSA Approval	SSA Approval
9. 5.9I Federal Grand Jury subpoenas for telephone or electronic mail subscriber information	US Attorney Office Approval (Type 1 and 2 Assessments Only)	US Attorney Office Approval	Not Permitted
10. 5.9C Pattern Based Data Mining	SORC	SORC	SORC

b2
b7E

UNCLASSIFIED//FOUO

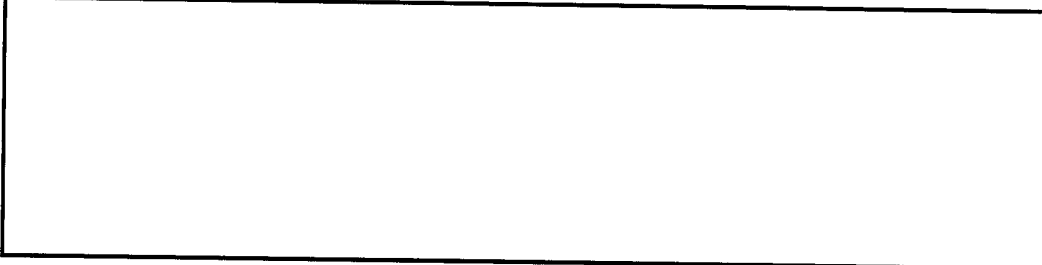
As of May 19, 2009

57

Teaching Points:

- Obtain Publicly Available Information:** Supervisory approval is not required for use of this method, except as to information gathered at a religious service. Notwithstanding any other policy, testing a CHS or VICE to attend a religious service during a predicted investigation, whether open to the public or not, requires SSA approval. Testing a CHS to attend a religious service, whether open to the public or not, during an assessment requires SAC approval.
 - Errors in observation or surveillance not requiring a court order:** Use of mechanical devices operated by a user (e.g., binoculars; hand-held cameras; radiation, chemical or biological detectors) is authorized in physical surveillance provided the device is not used to collect information in which a person has a reasonable expectation of privacy (e.g., equipment such as a parabolic microphone or other listening device that would intercept a private conversation or thermal imaging a home is not permitted.)
- Physical Surveillance:** For assessments, surveillance begins as stated in the plan at the initiation of surveillance. Requires SSA or SIA approval. SSA or SIA authorized to approve physical surveillance requests in incremental phases. **For predicted investigations:** No limitation on use. FBI employee cannot submit multiple requests for one time approval. No limitation on use of fixed or moving physical surveillance. For predicted investigations, no limitation on use.
- ASAC can delegate approval to SSA or SIA. Must be in writing and appropriately filed.
- ASAC can delegate approval to SSA or SIA. Must be in writing and appropriately filed.
- Access and Examine FBI and other DOJ Records, and Obtain Information from any FBI or other DOJ Personnel:** Supervisory approval is not required to use this method during assessments or predicted investigations, except that if the use of records constitutes pattern-based data mining under the Federal Data Mining Reporting Act of 2007, it must be reviewed by the SORC and the FBI must report the pattern-based data mining to Congress.
- Pattern-Based Data Mining Defined:** Use of one or more data bases to search for persons who fit a set of group characteristics or patterns of behavior (e.g., the known characteristics of a particular terrorist organization).
- Use Online Services and Resources (whether non-profit or commercial):** Subscribing to or purchasing any new service must be done pursuant to FBI contracting procedures.
 - Interview Defined:** Questioning of an individual (to include the subject) designed to gather information from the person being interviewed that is accurate, pertinent to, and within the scope of an authorized assessment or predicted investigation.
- In normal course of interview, FBI should divulge employee's affiliation with FBI and true purpose of interview. If person being interviewed expresses desire not to provide information, FBI employee may not state or imply in any way that the interviewee is compelled to provide information or that adverse consequences may follow. If interviewee indicates he or she wishes to consult an attorney, the interview must immediately stop.
- Custodial Interviews:** Miranda warnings are required to be given prior to custodial interviews if the subject is significantly restricted in his/her freedom of action to a degree normally associated with arrest. See FBI Legal Handbook for Special Agents.
- Interviews that require supervisory approval:**
- (i) contact with represented persons requires CDC review.
 - (ii) Members of U.S. Congress and Staff: Generally, FBI employees may take information received just as they would from other sources, and they may act upon it accordingly. However, prior CDC review, SAC and appropriate FBIHQ AD approval and prior notice to the AD Office of Congressional Affairs are required if FBI employee seeks to establish a formal relationship or interview a member of Congress or Congressional staff in connection with a foreign counterintelligence and/or public corruption matter.
 - (iii) White House Personnel: CDC review and SAC approval is required before initiating contact with White House personnel. CDC review, SAC approval and appropriate FBIHQ Section Chief approval must be obtained prior to conducting an interview of a member of the White House.

b2
b7E



- Accept Information Voluntarily Provided by Governmental or Private Entities:** Voluntarily provided information includes, but is not limited to: oral as well as documentary evidence and physical evidence such as: a computer hard drive or other electronic media that contains information, paper documents containing information, or physical objects (e.g., handgun or narcotics). FBI employee may not request nor knowingly accept information where disclosure would be prohibited by federal law (e.g., communications records).
- Access and Examine Records Maintained by, and Request Information From, Other Federal, State, Local, Tribal, or Foreign Governmental Entities or Agencies:** When requesting information using this authority, care must be taken to ensure the entity concerned understands that it is not compelled to provide such information or create a new record.
- Grand Jury Subpoenas for Telephone or Electronic Mail Subscriber Information:** Used only during a type 1 or 2 assessment. [redacted] Guardian



UNCLASSIFIED//FOUO

Investigative Methods/Approvals Chart

Authoritative Method and DIOG Reference	Assessments	Approval Levels for Administrative and Professional Investigations	
		Domestic	Foreign Intelligence
11 11.2 Mail covers			
12 11.4 Physical searches of personal or real property where a warrant or court order is not legally required (except from the reasonable expectation of privacy (e.g. [redacted]))			
13 11.6 Consensual monitoring of communications, including consensual computer monitoring	Not Permitted	CDC or OIG Review SSA Approval	CDC or OIG Review SSA Approval
14 11.8 Consensual monitoring of communications, including consensual computer monitoring, with a sensitive monitoring circumstance	Not Permitted	CDC or OIG Review, SAC Approval, DOJ Chief or DOJ HSD Approval	CDC or OIG Review, SAC Approval, DOJ Chief or DOJ HSD Approval
15 11.8 Use of closed-circuit television, direction finders, and other monitoring devices			
16 11.7 Polygraph examinations	Not Permitted	SSA Approval	SSA Approval
17 11.9 Undercover operations, Group II		CDC Review, SAC or ADAC with delegated authority; National Security cases also require HSD and NSLACB	CDC Review, SAC or ASAC with delegated authority; HSB-Unit/ACB Approval
18 11.8 Undercover operations, Group I		CDC review, SAC, and AD and OIG/IC or UIC/IC (SAD/IC or/and cases)	CDC review, SAC and AD and UIC/IC (SAD/IC or/and cases)
19 11.9 Compulsory process as authorized by law; Federal Grand Jury and trial subpoenas		US Attorney's Office Approval	
20 11.9 Administrative Subpoenas: Drugs		SAC, ASAC, SSA/A, or Drug Squad SSA	
Administrative Subpoenas: Sexual Exploitation	Not Permitted		Not Permitted
Administrative Subpoenas: Healthcare Fraud		U.S. Attorney's Office Approval	
21 11.9 National Security Letters	Not Permitted	Field Office, CDC Review, ADIC or SAC Approval, HQ, NSLB Review, DD or EAD-HSB or AD & DADs, CT/CD/CY or CC or Deputy OC-NSLB Approval	Not Permitted
22 11.10 Accessing stored wire and electronic communications and transaction records	Not Permitted	Stable/Cloud Order, Consent DIOG	Not Permitted
23 11.11 Use of pen registers and trap and trace devices	Not Permitted	FISA Court or District Court Order	Only Available if Authorized by FISA Court Order
24 11.12 Electronic surveillance			
28 11.13 Physical searches, where there is reasonable expectation of privacy, including mail openings			
29 11.14 Accession of foreign intelligence information in conformity with Title VII of the Foreign Intelligence Surveillance Act		FISA Court Order	FISA Court Order

UNCLASSIFIED//FOUO

As of May 19, 2009

58

b2
b7E

Teaching Points:

- 1. Mail Covers:** The DIOG currently states that for national security mail covers, "after being approved by the SSA, the Field Office must transmit the mail cover letter request by EC, with the draft letter as an attachment, to the National Security Law Branch (NSLB) for legal review and concurrence. Upon review and concurrence, the NSLB must transmit the letter request for signature to the EAD, National Security Branch, or, in his or her absence, to the Director.
- 2. Consensual Monitoring:** [redacted] Field Office must ensure that the individual who approves OIA is so authorized. For example, if the SAC has delegated authority to approve OIA for consensual monitoring to the SSA, upon CDC review, the SSA can approve the consensual monitoring and OIA. If OIA authority was not delegated to SSA, appropriate supervisory authority must expressly approve OIA.
- 3. Administrative Subpoenas:** Within the FBI, the authority to issue administrative subpoenas is limited to those positions holding the delegated authority from the Attorney General; that authority may not be redelegated. [redacted]

b2
b7E

Three Types of Administrative Subpoenas Authorized: (i) drug program investigations; (ii) child sexual exploitation and abuse investigations; (iii) health care fraud investigations.

- 4. National Security Letters:** Authority to sign NSLs has been delegated to the Deputy Director, EAD and Assistant EAD for NSB; ADs and all DADs for CT/CD/Cyber; General Counsel; DGC for NSLB; ADICs in NY, DC and LA; and all SACs. Every NSL must be reviewed and approved by a CDC or NSLB attorney.

UNCLASSIFIED//FOUO



FEDERAL BUREAU OF INVESTIGATION

OVERALL CLASSIFICATION:
UNCLASSIFIED

FBIHQ DIOG Training Session A



UNCLASSIFIED//FOUO



FEDERAL
BUREAU OF
INVESTIGATION



Course Overview

Overall Training Objective:

Provide an instructional foundation on the DIOG and then apply the knowledge gained by using hypothetical examples and scenarios. Upon completing this course of instruction you should have a firm grasp of the concepts and principles underpinning the DIOG.



UNCLASSIFIED//FOUO

Course Overview

Participation Standards:

Questions are welcome; however, if your question is about a specific set of facts that may divert the training objective, please direct your question to one of the Training team members at a break for a response.

During the scenario exercises, participants will be called upon to provide their response to particular facts or circumstances. Each Unit/Section should select a representative to speak for the Unit/Section and rotate that responsibility among the group. The scenarios are meant to prompt discussion, but the presenters must keep the scenario moving forward. Please understand that everyone may not be able to voice their perspective in the group setting. Keep in mind there may be several avenues to reach the same justified conclusion. You may use your handouts and training aids to inform your decision.

UNCLASSIFIED//FOUO

3



UNCLASSIFIED//FOUO

Course Overview

Course Completion:

- You must complete the entire mandatory 16.5 hours of training. You must score an 80% or higher to pass. You will be notified of your score via e-mail. If you do not pass the first time, you will be permitted to take the test again.
- Please annotate on the attendance sheet your presence at the training if you pre-registered. If you did not pre-register, please print your name, division, and the items requested on the attendance roster.
- After the course is complete, you will be receiving a survey e-mail containing questions that will test your knowledge and understanding of the material presented. The test is open book.

UNCLASSIFIED//FOUO

4



UNCLASSIFIED//FOUO

AGG-Dom: Overview

- Provides ability to FBI authorities to be more proactive and preventative, and the flexibility to deal with complex threats that do not fall neatly into individual programs
- Provides clarity and improves compliance by combining several sets of guidelines into one consistent set of guidelines

UNCLASSIFIED//FOUO

5

Teaching Point: Removes discrepancies, sets uniform rules for criminal, national security, and foreign intelligence collection cases. Each program will have a program-specific policy guide (PG)



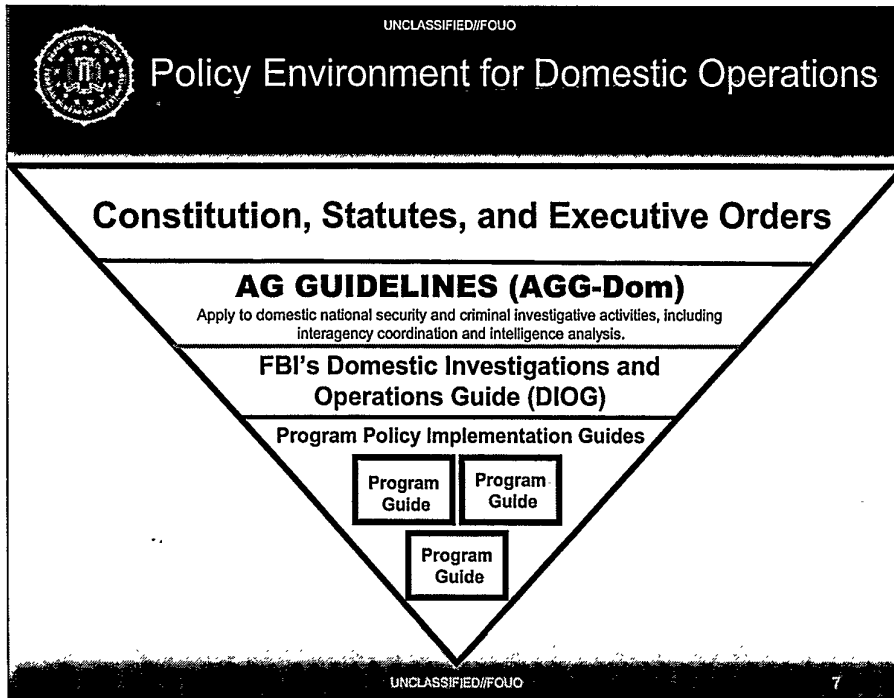
UNCLASSIFIED//FOUO

AGG-Dom: Overview

- Reduces reporting requirements, particularly in the national security area
- Recognizes Special Events and Domain Management as part of the FBI's mission
- Recognizes the FBI's obligation to provide investigative assistance and joint operational support to other agencies, including the U.S. intelligence community
- Creates a new category outside of predicated investigations named "Assessments"

UNCLASSIFIED//FOUO

6



Teaching Point:

FBIHQ Division Program Policy Implementation Guides (PG):

- Cannot be less restrictive than the DIOG
- Must comply with the policy contained in the DIOG
- Requests for program policy deviations from the DIOG must be reviewed by the OGC and approved by the Deputy Director



UNCLASSIFIED//FOUO

DIOG: Table of Contents

1. Scope and Purpose	10. Sensitive Investigative Matter
2. General Authorities and Principles	11. Investigative Methods
3. Core Values, Roles and Responsibilities	12. Assistance to Other Agencies
4. Privacy and Civil Liberties, and Least Intrusive Methods	13. Extraterritorial Provisions
5. Assessments	14. Retention and Sharing of Information
6. Preliminary Investigations	15. Intelligence Analysis and Planning
7. Full Investigations	16. Undisclosed Participation
8. Enterprise Investigations	17. Otherwise Illegal Activity
9. Foreign Intelligence	Appendices

UNCLASSIFIED//FOUO

8



UNCLASSIFIED//FOUO

DIOG Section 1: Scope & Purpose

- **DIOG applies to all investigative and intelligence collection activities conducted by the FBI**
 - within the United States
 - in the United States territories
 - outside the territories of all countries
- **DIOG does not apply to investigative and intelligence collection activities of the FBI in foreign countries**
 - governed by AGGs for Extraterritorial FBI Operations (national security and criminal)

UNCLASSIFIED//FOUO

9



UNCLASSIFIED//FOUO

DIOG Section 1: Scope & Purpose

- The primary purpose of the AGG-DOM and the DIOG is to standardize policy so that criminal, national security and foreign intelligence investigative activities are performed in a legal and consistent manner
- The DIOG replaces numerous FBI manuals, electronic communications, letterhead memoranda and other policy documents. The DIOG is located on the Corporate policy Office (CPO) Policy and Guidance Library web site
- The changes implemented by the DIOG better equip you to protect the people of the United States against crime and threats to the national security
- The DIOG stresses the importance of oversight and self-regulation to ensure compliance

UNCLASSIFIED//FOUO

10



UNCLASSIFIED//FOUO

DIOG Section 2: General Authorities & Principles

- **The AGG-Dom replaces six guidelines:**
 - The Attorney General's Guidelines on General Crimes, Racketeering Enterprise and Terrorism Enterprise Investigations (May 30, 2002)
 - The Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection (October 31, 2003) *
 - The Attorney General's Supplemental Guidelines for Collection, Retention, and Dissemination of Foreign Intelligence (November 29, 2006)

UNCLASSIFIED//FOUO

11



UNCLASSIFIED//FOUO

DIOG Section 2: General Authorities & Principles

- **The AGG-Dom also replaces:**
 - The Attorney General Procedure for Reporting and Use of Information Concerning Violations of Law and Authorization for Participation in Otherwise Illegal Activity in FBI Foreign Intelligence, Counterintelligence or International Terrorism Intelligence Investigations (August 8, 1988) *
 - The Attorney General's Guidelines for Reporting on Civil Disorders and Demonstrations Involving a Federal Interest (April 5, 1976)
 - The Attorney General's Procedures for Lawful, Warrantless Monitoring of Verbal Communications (May 30, 2002) (only portion applicable to FBI)

UNCLASSIFIED//FOUO

12



UNCLASSIFIED//FOUO

DIOG Section 2: General Authorities & Principles

Note: Regarding Extraterritorial FBI's Operations, the AGG-Dom did not repeal or supersede certain portions of the prior guidelines (marked * in prior slides). These national security extraterritorial portions continue to remain in effect pending the approval of new Attorney General's Guidelines for Extraterritorial FBI Operations for both national security and criminal investigations. Additionally, the classified Attorney General Guidelines for Extraterritorial FBI Operations and Criminal Investigations (1993) continue to remain in effect pending approval of the new guidelines.

UNCLASSIFIED//FOUO

13



UNCLASSIFIED//FOUO

Comparison of Prior and New Attorney General Guidelines

General Comparison

Prior AGG

Investigative Guidelines and Compliance Rules

- The six guidelines governing investigative and intelligence gathering replaced/superseded by the new AGG:
 - The Attorney General's Guidelines on General Crimes, Racketeering Enterprise and Terrorism Enterprise Investigations;
 - The Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection
 - The Attorney General's Supplemental Guidelines for Collection, Retention, and Dissemination of Foreign Intelligence
 - The Attorney General Procedure for Reporting and Use of Information Concerning Violations of Law and Authorization for Participation in Otherwise Illegal Activity in FBI Foreign Intelligence, Counterintelligence or International Terrorist Intelligence Investigations
 - The Attorney General's Guidelines for Reporting on Civil Disorders and Demonstrations Involving a Federal Interest
 - The Attorney General's Procedures for Lawful, Warrantless Monitoring of Verbal Communications (superseded, as to the FBI)
- Numerous and different guidelines used for compliance
- Different rules for national security and criminal investigations

New AGG

Investigative Guidelines and Compliance Rules

- The Attorney General's Guidelines (AGG) for Domestic FBI Operations govern all FBI investigative and intelligence gathering activities conducted in the United States or outside the territories of all other countries replaces five guidelines and supersedes one
- One standardized guideline used for compliance
- One set of rules for national security and criminal investigations

UNCLASSIFIED//FOUO

14



UNCLASSIFIED//FOUO

Comparison of Prior and New Attorney General Guidelines

Assessments

Prior AGG (Threat Assessments)

Authorized Methods

- Obtain publicly available information
- Access and examine FBI/DOJ records, and obtain information from any FBI/DOJ personnel
- Check other federal, state, and local records
- Use online services and resources
- Interview previously established Human Sources (not including new tasking of such sources)
- Interview or request information from members of the public and private entities (other than pretext interviews or requests)
- Accept voluntarily information

Reporting Requirements

- None

New AGG (Assessments)

Authorized Methods

- Obtain publicly available information
- Access and examine FBI and other DOJ records, and obtain information from any FBI or DOJ personnel
- Access and examine records maintained by, and request information from, other federal, state, local, tribal, or foreign government or agencies
- Use online services and resources
- Use and recruit human sources in conformity with AG Guidelines Regarding the Use of FBI Confidential Human Sources
- Interview or request information from members of the public and private entities
- Accept information voluntarily provided by governmental or private entities
- Engage in observation or surveillance not requiring a court order
- Federal Grand Jury subpoenas for telephone and electronic mail - subscriber records only

Reporting Requirements

- None

UNCLASSIFIED//FOUO

15



UNCLASSIFIED//FOUO

Comparison of Prior and New Attorney General Guidelines

Preliminary Investigations

Prior AGG

Authorized Methods

- All Threat Assessment techniques
- Interviews (including pretext) of subject and others
- Recruitment of new human sources & tasking of existing sources
- Inquiry of foreign law enforcement, intelligence, or security agencies
- Mail covers
- Consensual monitoring of communications
- Closed circuit TV, direction finders, and monitoring devices
- Undercover operations
- Physical, photo, and video surveillance
- [REDACTED]
- Polygraph examinations
- National Security Letters
- Accessing stored wire/electronic communications
- Pen registers/Trap & Trace
- Obtain business records
- Grand Jury subpoenas

Reporting Requirements

- Field notification of Initiation to FBIHQ (10 Days)
- FBIHQ notification to DOJ-OI of Initiation (10 Days)
- FBIHQ notify DAG if Initiation is disapproved

New AGG

Authorized Methods

- All Assessment Methods
- Mail covers
- Physical searches of personal or real property where a warrant or court order is not legally required because there is no reasonable expectation of privacy
- Consensual monitoring of communications (including consensual computer monitoring)
- Closed circuit TV, direction finders, and monitoring devices
- Polygraph examinations
- Undercover operations
- Compulsory process as authorized by law; Federal Grand Jury and other subpoenas and National Security Letters
- Accessing store wire and electronic communications and transactional records
- Use of pen registers and trap and trace devices

Reporting Requirements

- Only if sensitive investigative matter - Notify FBIHQ and DOJ/U.S. Attorney - Notify NSD if sensitive matter is a national security threat (NLT 30 Days)
- FBIHQ notify the DAG if Initiation is disapproved based on insufficient predication for national security matters

b2
b7E

UNCLASSIFIED//FOUO

16



UNCLASSIFIED//FOUO

Comparison of Prior and New Attorney General Guidelines

Full Investigations

Prior AGG

Authorized Methods

- All Threat Assessment techniques
- All preliminary investigation techniques
- Electronic Surveillance
- Physical searches and Mail openings

Reporting Requirements

- Field notification of initiation to FBIHQ (10 Days)
- FBIHQ notification to DOJ-OI of initiation (10 Days)
- FBIHQ notify DAG if initiation is disapproved
- Annual summary submitted to DOJ-OI

New AGG

Authorized Methods

- All Assessment Methods
- All Preliminary Investigation Methods
- Electronic Surveillance
- Foreign Intelligence collection under Title VII of FISA
- Physical searches and Mail openings

Reporting Requirements

- Notify FBIHQ and DOJ/U.S. Attorney sensitive investigative matter - Notify NSD if sensitive matter is a national security threat (NLT 30 Days)
- FBIHQ notification to DOJ-NSD (NLT 30 Days) only if:
 - Initiation on U.S. person relating to a national security threat
 - Initiation based on foreign intelligence requirement
- FBIHQ notify the DAG if initiation is disapproved based on insufficient predication for national security matters

UNCLASSIFIED//FOUO

17



UNCLASSIFIED//FOUO

DIOG Section 2: General Authorities & Principles

The FBI is authorized to:

- Conduct investigations and collect evidence (criminal and national security) and collect foreign intelligence (AGG-Dom, Part II)
- Provide investigative assistance to federal, state, local, tribal, and foreign agencies (AGG-Dom, Part III) and (DIOG Section 12)
- Collect information necessary for and conduct intelligence analysis & planning (AGG-Dom, Part II & IV) and (DIOG Section 15)
- Retain and share information (AGG-Dom, Part VI) and (DIOG Section 14)

UNCLASSIFIED//FOUO

18



DIOG Section 2: General Authorities & Principles

The word "Assessment" has two distinct meanings:

- The AGG-Dom authorizes as an investigative activity an "assessment" which requires an authorized purpose and objective as discussed in DIOG Section 5.
- The U.S. intelligence community uses the word "assessment" to describe written intelligence products as discussed in DIOG Section 15.7.B.



UNCLASSIFIED//FOUO

DIOG Section 2: General Authorities & Principles

- **The FBI is an intelligence agency as well as a law enforcement agency**
- **The FBI is authorized to engage in intelligence analysis and planning, using all lawful sources of information:**
 - development of overviews and analysis
 - research and analysis to produce reports and assessments
 - operate intelligence systems that facilitate and support investigations through ongoing compilation and analysis of data and information

UNCLASSIFIED//FOUO

20



UNCLASSIFIED//FOUO

DIOG Section 2: General Authorities & Principles

- **The FBI is the “lead federal agency” in the following areas:**
 - Federal Crimes of Terrorism (listed in DIOG Section 2.4.C)
 - Other non-Terrorism federal crimes (listed in DIOG Section 2.4.D)
 - Counterintelligence and Espionage (listed in DIOG Section 2.4.F)
 - Criminal Investigations (some listed in DIOG Section 2.4.G; see also CID PGs)

UNCLASSIFIED//FOUO

21



UNCLASSIFIED//FOUO

DIOG Section 2: General Authorities & Principles

Departures from the AGG – Dom:

In Advance: FBI Director, Deputy Director, or EAD (NSB or Criminal Cyber Response and Services Branch) must approve with notice to the General Counsel.

In Emergency: Approving authority who authorizes the departure must give notice as soon thereafter as practical to Director, Deputy Director or EAD with notice to General Counsel – OGC must keep records of all departures to advise DOJ, as required.

UNCLASSIFIED//FOUO

22



UNCLASSIFIED//FOUO

DIOG Section 2: General Authorities & Principles

Departures from the DIOG:

In Advance: Appropriate substantive AD or DAD must approve with notice to the General Counsel or appropriate Deputy General Counsel (DGC).

In Emergency: Approving authority who authorizes the departure must give notice as soon thereafter as practical; SAC or HQ Section Chief must provide written notice to appropriate substantive AD and the General Counsel.

UNCLASSIFIED//FOUO

23



UNCLASSIFIED//FOUO

DIOG Section 2: General Authorities & Principles

The AGG-Dom and DIOG apply to all FBI domestic investigations and operations conducted by “FBI employees” – defined as:

- applicable support personnel
- intelligence analysts
- special agents
- task force officers (TFO)
- detailees
- FBI contractors
- confidential human sources (CHS)

UNCLASSIFIED//FOUO

24



UNCLASSIFIED//FOUO

DIOG Section 2: General Authorities & Principles

FBIHQ Division Program Policy Implementation Guides (PG):

- Cannot be less restrictive than the DIOG
- Must comply with the policy contained in the DIOG
 - requests for program policy deviations from the DIOG must be reviewed by the OGC and approved by the Deputy Director

UNCLASSIFIED//FOUO

25



UNCLASSIFIED//FOUO

DIOG Section 2: General Authorities & Principles

Authorities of an FBI Special Agent:

1. Investigate violations of the laws, including the criminal drug laws, of the United States (21 U.S.C. § 871; 28 U.S.C. §§ 533, 534 and 535; 28 C.F.R. § 0.85)
2. Collect evidence in cases in which the United States is or may be a party in interest (28 C.F.R. § 0.85 [a]) as redelegated through exercise of the authority contained in 28 C.F.R. § 0.138 to direct personnel in the FBI
3. Make arrests (18 U.S.C. §§ 3052 and 3062)
4. Serve and execute arrest warrants and seize property under warrant; issue and/or serve administrative subpoenas; serve subpoenas issued by other proper authority; and make civil investigative demands (18 U.S.C. §§ 3052, 3107; 21 U.S.C. § 876; 15 U.S.C. § 1312)

UNCLASSIFIED//FOUO

26



UNCLASSIFIED//FOUO

DIOG Section 2: General Authorities & Principles

Authorities of an FBI Special Agent (cont.):

5. Carry firearms (18 U.S.C. § 3052)
6. Administer oaths to witnesses attending to testify or depose in the course of investigations of frauds on or attempts to defraud the United States or irregularities or misconduct of employees or agents of the United States (5 U.S.C. § 303)
7. Seize property subject to seizure under the criminal and civil forfeiture laws of the United States (e.g., 18 U.S.C. §§ 981 and 982)
8. Perform other duties imposed by law

UNCLASSIFIED//FOUO

27



UNCLASSIFIED//FOUO

DIOG Section 2: General Authorities & Principles

The AGG-Dom did not limit other authorized FBI activities, such as:

- Conducting background checks and inquires concerning applicants and employees under federal personnel security programs
- Maintenance and operation of national criminal records systems and preparation of national crime statistics
- Forensic assistance and administration functions of the FBI Laboratory

UNCLASSIFIED//FOUO

28



UNCLASSIFIED//FOUO

DIOG Section 3: FBI's Core Values

The FBI's Core Values are:

- Rigorous obedience to the U.S. Constitution
- Respect for the dignity of all those we protect
- Compassion
- Fairness
- Uncompromising personal integrity and institutional integrity
- Accountability by accepting responsibility for our actions and decisions and their consequences
- Leadership, by example, both personal and professional

UNCLASSIFIED//FOUO

29

Teaching Points: DIOG Section 3.1:

1. Core values must be fully understood, practice, shared, vigorously defended and preserved.
2. By observing core values – FBI will achieve a high level of excellence in performing both our national security and criminal missions.
3. Information for reporting violations is available from the Office of Integrity and Compliance (OIC).



UNCLASSIFIED//FOUO

DIOG Section 3: Compliance

Everyone's Responsibility:

- To learn and understand the laws, rules and regulations that govern their activities
- To fully comply with all laws, rules and regulations governing investigations, operations, programs and activities
- To report to proper authority any known or suspected failures to adhere to the law, rules or regulations

UNCLASSIFIED//FOUO

30

Teaching Point: DIOG Section 3.1:

1. DIOG compliance applies to all FBI employees, task force officers, contractor's etc.
2. May not disregard the law, rule, etc. for sake of expediency.
3. Information for reporting.



UNCLASSIFIED//FOUO

DIOG Section 3: Deputy Director Roles and Responsibilities

DIOG Section 3.2:

- DD is the proponent of the DIOG and subordinate implementing procedural directives and specific policy implementation guides (PGs)
- DD has oversight of DIOG compliance, monitoring and auditing processes
- DD has responsibility for DIOG training
- DD, through the Corporate Policy Office (CPO), will ensure the DIOG is updated one year from implementation, and every three years thereafter

UNCLASSIFIED//FOUO

31

Teaching Point: DD, through the CPO, will review the Program Guides (PGs) for all divisions to ensure compliance with DIOG standards.



UNCLASSIFIED//FOUO

DIOG Section 3: Special Agent, Intelligence Analyst, Task Force Officer, FBI Contractor, and Others - Roles and Responsibilities

DIOG Section 3.3:

- Comply with AGG-Dom and DIOG standards for initiation, conducting, and closing investigative activity; collection activity; or use of an investigative method
- Obtain training on DIOG standards relevant to their position and perform activities consistent with those standards
- Ensure all investigative activity complies with all laws and policy
- Identify victims, offer FBI assistance, and furnish information to the FBI Victim Specialist

UNCLASSIFIED//FOUO

32

Teaching Point:

1. Laws/policy include the Constitution, federal law, Executive Orders, Presidential Directives, AGG-Dom, other AGGs, Treaties, MOAs/MOUs, DIOG and other policy. When in doubt – consult their Supervisor, the CDC or OGC.
2. Victims include those who have suffered direct physical, emotional, or financial harm as a result of the commission of federal crimes.



UNCLASSIFIED//FOUO

DIOG Section 3: Special Agent, Intelligence Analyst, Task Force Officer, FBI Contractor, and Others - Roles and Responsibilities

(Continued – DIOG Section 3.3)

- Ensure civil liberties and privacy are protected throughout the assessment or investigative process
- Conduct no investigative activity solely on the basis of activities protected by the 1st Amendment or solely on the basis of race, ethnicity, national origin or religion of the subject
- Report non-compliance to the proper authority

UNCLASSIFIED//FOUO

33



UNCLASSIFIED//FOUO

DIOG Section 3: Supervisor Roles and Responsibilities

DIOG Section 3.4.A – Supervisor Defined:

- Field Office or FBIHQ personnel, including: SIA, SSA, SSRA, UC, ASAC, ASC, SAC, DAD, AD, ADIC, and EAD

UNCLASSIFIED//FOUO

34



UNCLASSIFIED//FOUO

DIOG Section 3: Supervisor Roles and Responsibilities

DIOG Section 3.4.B - Supervisor Responsibilities:

- Determine whether the DIOG standards are satisfied for initiating, approving, conducting and closing an investigative activity, collection activity, or investigative method
- Ensure all investigative activity complies with all laws and policy
- Obtain training on DIOG standards relevant to their position and conform their decisions to those standards
- Ensure civil liberties and privacy are protected throughout the assessment or investigative process

UNCLASSIFIED//FOUO

35



UNCLASSIFIED//FOUO

DIOG Section 3: Supervisor Roles and Responsibilities

Continued DIOG Section 3.4.B - Supervisor Responsibilities:

- If encountering a practice that does not comply with the law, rules, or regulations, the supervisor must:
 - 1. report that compliance concern to the proper authority
 - 2. take action to maintain compliance, when necessary
- Ensure no retaliation or adverse action is taken against persons who raise compliance concerns

UNCLASSIFIED//FOUO

36

Teaching Points:

1. Should report non-compliance to immediate Supervisor and/or OIC.
2. OIC non-retaliation policy located in the CPO policy and guidance library.



UNCLASSIFIED//FOUO

DIOG Section 3: Supervisor Roles and Responsibilities

DIOG Section 3.4.C - Supervisory Delegation:

- Any DIOG requirement imposed on a Supervisor may be delegated/performed by a designated Acting, Primary, or Secondary Relief supervisor as indicated below, unless specified otherwise by federal statute, EO, PD, AGG, FBI Policy or any other regulation.
 - Supervisor may delegate authority to a supervisor one level junior to himself/herself (e.g. SAC to ASAC; or SC to Assistant/SC)
 - Must identify the task delegated
 - Must identify the supervisory position given approval authority
 - Must be in writing
 - Must be retained appropriately
 - Higher level Supervisors in the same chain-of-command as the original supervisor may approve a particular activity without written delegation documentation

UNCLASSIFIED//FOUO

37

Teaching Points: Question – Can SSA or SIA delegate? No, but an appropriately designated Acting or Relief Supervisor can assume the responsibilities in the absence of the SSA.

DIOG 3.4 C



UNCLASSIFIED//FOUO

DIOG Section 3: Supervisor Roles and Responsibilities

DIOG Section 3.4.D - Investigative File Reviews:

- Conducted by full-time supervisors or primary relief supervisors with subordinates
 - (other relief supervisors must have written SAC authority to conduct)
- Conducted with all Agents, Resident Agents, TFOs, analysts, detailees, and FBI contractors, as appropriate
- Conducted in-person or by telephone when necessary
- Conducted in private
- Documented/noted on ACS ICMC report, FD-71 or Guardian
- Conducted at least every 60 days for Probationary Agents, recommended every 30 days

UNCLASSIFIED//FOUO

38

Teaching Points: ACS Investigative Case management Case Review report.



UNCLASSIFIED//FOUO

DIOG Section 3: Supervisor Roles and Responsibilities

Assessment Justification/File Reviews:

- Conducted for every 30 day period for Type 1 and 2 Assessments
 - (with 10 additional days to complete and document)
- Conducted for every 90 day period for Type 3, 4, and 6 Assessments
 - (with 30 additional days to complete and document)
- Supervisor Must:
 - Evaluate progress made toward the achievement of authorized purpose and objective
 - Ensure activities that occurred during prior period were appropriate
 - Determine whether it is reasonably likely that information may be obtained that is relevant to the authorized objective – thus warranting an extension for another 30/90 day period
 - Determine whether adequate predication has been developed to open a predicated investigation
 - Determine whether the assessment should be terminated

UNCLASSIFIED//FOUO

39

Teaching Points: DIOG Section 5 details file review requirements.



UNCLASSIFIED//FOUO

DIOG Section 3: Supervisor Roles and Responsibilities

Predicated (Preliminary and Full) Investigation File Reviews:

- Conducted for every 90 day period
 - (with 30 additional days to complete and document)
- Supervisor Must:
 - Evaluate progress made toward the achievement of authorized purpose and objective
 - Ensure activities that occurred during prior period were appropriate
 - Determine whether it is reasonably likely that information may be obtained that is relevant to the authorized objective – thus warranting an extension for another 90 day period
 - Determine whether adequate predication has been developed to open/or continues to justify a predicated investigation

UNCLASSIFIED//FOUO

40

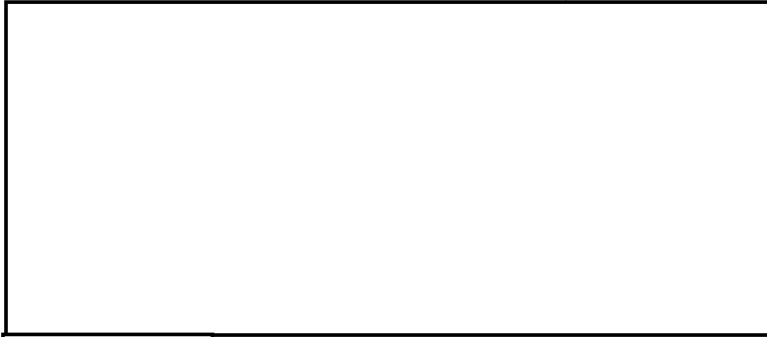
Teaching Points: Probationary Agent File reviews conducted at least every 60 days, recommend 30 days



UNCLASSIFIED//FOUO

DIOG Section 3: Unaddressed Work

-
-
-
-



Note: the FD-71 provides a new mechanism to assign an Assessment to an electronic Unaddressed Work File in the appropriate classification

b2
b7E

UNCLASSIFIED//FOUO

41



UNCLASSIFIED//FOUO

DIOG Section 3: CDC's Role and Responsibilities

CDC's Role and Responsibilities:

1. Must review all Assessments, Preliminary Investigations (PI) and Full Investigations (FI) that involve a "Sensitive Investigative Matter" (SIM)
2. Must review particular investigative methods as mandated by DIOG Section 5 and 11
3. Requirements imposed on the CDC may be performed by an Associate Division Counsel, Legal Advisor, or designated Acting CDC. All delegations must be in writing and retained appropriately.

UNCLASSIFIED//FOUO

42



UNCLASSIFIED//FOUO

DIOG Section 3: CDC Roles and Responsibilities

CDC Determinations:

The primary purpose of the CDC's review is to ensure the legality of the actions proposed. In this context, the review includes a determination that the:

- Investigative activity is not legally objectionable (can be overruled by OGC)
 - Activity is not based solely on the exercise of 1st Amendment rights or on the race, ethnicity, national origin or religion of the subject
- The investigation is founded upon an "authorized purpose" (Assessments) or have adequate factual predication (Preliminary and Full)
- Advise as to the "wisdom" of the proposed action

UNCLASSIFIED//FOUO

43



UNCLASSIFIED//FOUO

DIOG Section 3: CDC Roles and Responsibilities

Continued: CDC Determinations

The CDC's determination is based on facts known at the time of the review and recommendation.

The CDC may require additional reviews or provide guidance as to monitoring the results of investigative activity to ensure that the authorized purpose and/or factual predication remain intact after additional facts are developed.

UNCLASSIFIED//FOUO

44



UNCLASSIFIED//FOUO

DIOG Section 3: OGC Roles and Responsibilities

OGC Role: In coordination with the DOJ NSD, the OGC is responsible for conducting regular reviews of all aspects of FBI national security and foreign intelligence activities.

The primary purpose of the OGC's review is to ensure the legality of the actions proposed. These reviews, conducted in the field offices and in HQ Units, broadly examine such activities for compliance with the AGG-Dom and other requirements. In this context, the review includes a determination that the:

- Investigative activity is not legally objectionable (Activity is not based solely on the exercise of 1st Amendment rights or on the race, ethnicity, national origin or religion of the subject)
- The investigation is founded upon an "authorized purpose" (Assessments) or have adequate factual predication (Preliminary and Full) and meets the standards in the DIOG
- Advise as to the "wisdom" of the proposed action

UNCLASSIFIED//FOUO

45



UNCLASSIFIED//FOUO

DIOG Section 3: OGC Roles and Responsibilities

Continued: OGC Determinations

- The OGC's determination above is based on facts known at the time of the review and recommendation.
- The OGC may require additional reviews or provide guidance as to monitoring the results of investigative activity to ensure that the authorized purpose and/or factual predication remain in tact after facts are developed

UNCLASSIFIED//FOUO

46



UNCLASSIFIED//FOUO

DIOG Section 3: Other Roles and Responsibilities

CPO = Corporate Policy Office: Oversight and Implementation of the DIOG; Report compliance risks to OIC (DIOG Section 3.7)

OIC = Office of Integrity and Compliance: Identify compliance risk areas, adequacy of policy and training programs, monitor DIOG compliance (DIOG Section 3.8)

DCO = Division Compliance Officer: One identified in each Field Office to assist the OIC to identify potential non-compliance risk areas and report them to proper authority and OIC (DIOG Section 3.10)

PM = Program Manager: HQ entity that identifies, prioritizes, and analyzes compliance risks and takes appropriate corrective action (DIOG Section 3.9)

UNCLASSIFIED//FOUO

47



UNCLASSIFIED//FOUO

DIOG Section 4: Privacy and Civil Liberties, and Least Intrusive Methods

- Responsibility to protect the American public, not only from crime and terrorism, but also from incursions into their constitutional rights; accordingly, all investigative activities must fully adhere to the Constitution and the principles of civil liberty and privacy.
- Provisions of the AGG-Dom, other AG guidelines, and oversight from DOJ components, are designed to ensure FBI's activities are lawful, appropriate, and ethical, as well as effective in protecting civil liberties and privacy.
- DOJ and FBI's Inspection Division, Office of Integrity and Compliance, the OGC, other Bureau components, and **you** share responsibility for ensuring the FBI meets these goals.

UNCLASSIFIED//FOUO

48

Teaching Point:

The FBI is a very important agency with dedicated, highly professional, greatly disciplined Government servants. These words, uttered in 1975 by then Attorney General Levi, are just as true today – if not more so – than they were 34 years ago. But when these words were spoken, it was in the context of Senate hearings on the intelligence function of the FBI and the substantial concerns expressed by a parade of witnesses that for the purpose of protecting the national security and preventing violence, the Bureau was engaging in activities that “tread[] on forbidden ground.”

Fashioning investigative activities that navigate between Constitutional requirements and the imperatives of protecting the nation is often a difficult balancing act and one of the hardest issues that an agent or analyst can face is whether and under what circumstances a particular investigative activity is appropriate. The rewards when we find the right balance often go unnoticed by the general public, but the criticism when we don't can be heard far and wide.

The Attorney General Guidelines for Domestic Activities and the implementing Domestic Investigations Operations Guide are built on a history of attempting to fashion the proper balance between investigating crimes and collecting intelligence while protecting the civil liberties of our people. You are sitting here today because it is your job to help educate your colleagues on how to strike the right balance.



UNCLASSIFIED//FOUO

DIOG Section 4: Privacy and Civil Liberties, and Least Intrusive Methods

- No investigation or assessment can be commenced based solely on race, ethnicity, national origin, religion of the subject or the exercise of First Amendment rights.
- Corollary to this AGG requirement is the Privacy Act, which states that each agency that maintains a system of records shall “maintain no record describing how any individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute or by the individual about whom the record is maintained or **unless pertinent to and within the scope of an authorized law enforcement activity.** 5 U.S.C. 552a(e)(7).

UNCLASSIFIED//FOUO

49

Teaching Point:

The first two conditions in the Privacy Act are fairly simple and not typical. If Congress says we can collect and maintain records about how an individual exercises First Amendment rights or if the subject of the record consents, there's no problem – and any resultant records would not be based solely on First Amendment activities.

The purpose of (e)(7) of the Privacy Act, as articulated in the limited legislative history that we have, is to prevent the “collection of protected information not immediately needed, about law-abiding Americans, on the off-chance that Government or the particular agency might possibly have to deal with them in the future.” The Act does not define an “authorized law enforcement activity,” but the courts have been generous in finding a law enforcement purpose for FBI activities.



UNCLASSIFIED//FOUO

DIOG Section 4: Privacy and Civil Liberties, and Least Intrusive Methods

- The test is whether the collection of information is relevant to a law enforcement activity.
- Consider the following cases:
 - Patterson v. FBI, 893 F.2d 595 (3d Cir. 1990).
 - Bassiouni v. FBI, 436 F.3d 712 (7th Cir. 2006).

UNCLASSIFIED//FOUO

50

Teaching Point:

Cases interpreting this section of the Privacy Act have approved:

1. The first cases involved the FBI's maintenance of records describing a 6th grader's letters, written as part of a school project, to a large number of foreign embassies. The return address on the letters was his father's business and the resultant records not only examined the company, but also the 6th grader. The court found that maintenance of records about the 6th grader was relevant to a law enforcement activity. Interestingly, the investigation in this case was undertaken pursuant to the then existing AG Guidelines.
2. In the second case, we argued that the plaintiff's records were relevant to current FBI "investigative interests" because the investigation of terrorism is a top FBI priority and the records concerned the plaintiff's contacts with, and activities concerning, the Middle East. The court agreed. We also argued that we needed to keep the records for contextual reasons, if we received new information about the plaintiff, and also to evaluate the credibility and veracity of FBI sources. The court found all these reasons for maintenance of the records persuasive and consistent with an authorized law enforcement activity.



UNCLASSIFIED//FOUO

DIOG Section 4: Privacy and Civil Liberties, and Least Intrusive Methods

- The AGG-Dom says that any activity undertaken pursuant to the Guidelines is an authorized law enforcement activity for purposes of the Privacy Act.
- Is this enough?

UNCLASSIFIED//FOUO

51

Teaching Point:

b2
b7E



UNCLASSIFIED//FOUO

DIOG Section 4 Scenario

-

- What can you do with this information?

-

-

-


UNCLASSIFIED//FOUO

52

b2
b7E

Questions continue on next slide

UNCLASSIFIED//FOUO



DIOG Section 4 Scenario

-
-

UNCLASSIFIED//FOUO 53

b2
b7E

Teaching Point:

These are difficult issues, but it is important to understand not only what is permissible, but how to document what action is taken.

b2
b7E



UNCLASSIFIED//FOUO

DIOG Section 4: Privacy and Civil Liberties, and Least Intrusive Methods

FIRST AMENDMENT RIGHTS:

Individuals or groups who communicate with each other or with members of the public in any form in pursuit of social or political causes—such as opposing war or foreign policy, protesting government actions, promoting certain religious beliefs, championing particular local, national, or international causes, or a change in government through non-criminal means, and actively recruit others to join their causes—have a fundamental constitutional right to do so. An assessment may not be initiated based solely on the exercise of these First Amendment rights. If, however, a group exercising its First Amendment rights also threatens or advocates violence or destruction of property, an assessment would be appropriate

UNCLASSIFIED//FOUO

54



UNCLASSIFIED//FOUO

DIOG Section 4: Privacy and Civil Liberties, and Least Intrusive Methods

FIRST AMENDMENT RIGHTS (cont.):

- No investigative activity, including assessments, may be taken solely on the basis of activities that are protected by the First Amendment or on the race, ethnicity, national origin or religion of the subject.
- If an assessment or predicated investigation touches on or is partially motivated by First Amendment activities, race, ethnicity, national origin or religion, it is particularly important to identify and document the basis for the assessment with clarity

UNCLASSIFIED//FOUO

55



UNCLASSIFIED//FOUO

DIOG Section 4: Privacy and Civil Liberties, and Least Intrusive Methods

All activities must be consistent with the Attorney General's 2003 Guidance Regarding the Use of Race by Federal Law Enforcement Agencies (forbids the use of racial profiling and requires activities involving the investigation or prevention of threats to the national security to comply with the Constitution and laws of the United States)

The DIOG stresses several points in each section:

- No investigation or assessment can be commenced based solely on race, ethnicity, national origin, religion, or exercise of First Amendment rights
- The FBI must use the least intrusive method that is feasible under the circumstances
- In connection with Foreign Intelligence collection, agents must operate openly and consensually with U.S. Persons, to the extent practicable
- All investigative activities must have an "authorized purpose"

UNCLASSIFIED//FOUO

56



UNCLASSIFIED//FOUO

DIOG Section 4: Use of Race or Ethnicity

DIOG Guidance on use of Race or Ethnicity

As to individuals:

1. Permits the consideration of ethnic and racial identity information based on specific reporting;
2. The race or ethnicity of suspected members, associates, or supporters of an ethnic-based gang or criminal enterprise may be collected when gathering information about or investigating the organization; or
3. Ethnicity may be considered in evaluating whether a subject is—or is not—a possible associate of a criminal or terrorist group that is known to be comprised of members of the same ethnic grouping—as long as it is not the dominant factor for focusing on a particular person

UNCLASSIFIED//FOUO

57



UNCLASSIFIED//FOUO

DIOG Section 4: Use of Race or Ethnicity

DIOG Guidance on use of Race or Ethnicity

As to a community:

1. Collecting and analyzing demographics – if these locations will reasonably aid the analysis of potential threats and vulnerabilities, and, overall, assist domain awareness
2. Geo-Mapping ethnic/racial demographics – if properly collected
3. General ethnic/racial behavior – cannot be collected, unless it bears a rational relationship to a valid investigative or analytical need
4. Specific and relevant ethnic behavior
5. Exploitive ethnic behavior – by criminal or terrorist groups

UNCLASSIFIED//FOUO

58



UNCLASSIFIED//FOUO

DIOG Section 4: Least Intrusive Investigative Method

The AGG-DOM and the DIOG require that the “least intrusive” means or method be considered and, if operationally sound and effective, used to obtain intelligence or evidence in lieu of a more intrusive method

UNCLASSIFIED//FOUO

59

Teaching Point: There is a component of efficiency in being “effective”.

In some instances, a more intrusive method, i.e. use of a CHS, may be more operationally sound and effective for resolving an outstanding investigative need, than a less intrusive method such as acquiring financial records or business records. The totality of the circumstances surrounding the investigative activity plays an important role in considering the use of the least intrusive alternative for obtaining intelligence or evidence. It is a balancing test.



UNCLASSIFIED//FOUO

DIOG Section 4: Privacy and Civil Liberties, and Least Intrusive Methods

By emphasizing the use of less intrusive
means, employees will be able to balance:

Our need for evidence/intelligence

vs.

Mitigating potential negative impact on the privacy and civil
liberties of people/public

UNCLASSIFIED//FOUO

60



UNCLASSIFIED//FOUO

DIOG Section 4: Privacy and Civil Liberties, and Least Intrusive Methods

Primary factor in determining “intrusiveness”:

- The degree of procedural protection that the law and the AGG-DOM provide for the use of the particular method.
 - Examples of “more intrusive” methods: Search Warrants, wiretaps, UCOs
 - Examples of “less intrusive” methods: checks of government databases, state or local criminal record checks, commercial databases, interviews

UNCLASSIFIED//FOUO

61



UNCLASSIFIED//FOUO

DIOG Section 4: Privacy and Civil Liberties, and Least Intrusive Methods

Items to consider when determining the relative intrusiveness of an investigative method:

- Is method permitted prior to the initiation of an assessment?
- Is the method relevant to the assessment or investigation?
- Will the information collected or obtained likely further the investigative objective?
- What alternatives exist for gathering the same information?
- Are those alternatives relatively less intrusive?
- What time span is involved in using the investigative method (days, weeks, months)?
- What confidence level is associated with the information gathered using the investigative method?
- Will the method resolve a pending investigative issue quickly?

UNCLASSIFIED//FOUO

62



DIOG Section 4: Least Intrusive Investigative Method

Factors to Determine "Intrusiveness":

1. Nature of the information sought
2. Scope of the information sought
3. Scope of the use of the investigative method
4. Source of the information sought
5. Risk of public exposure



DIOG Section 5 & 11: Investigative Methods

Authorized Methods for Assessments and Predicated Investigations
Red indicates methods not allowed under a particular operational activity; Green indicates methods allowed.

	Assessments	Preliminary Investigations	Full Investigations
Obtain publicly available information			
Access and examine FBI and other DOJ records, and obtain information from any FBI or DOJ personnel			
Access and examine records maintained by, and request information from, other federal, state, local, tribal, or foreign governmental entities or agencies			
Use online services and resources (whether nonprofit or commercial)			
Use and recruit human sources in conformity with AG Guidelines Regarding the Use of FBI Confidential Human Sources			
Interview or request information from members of the public and private entities (includes pretextual interviews)			
Accept information voluntarily provided by governmental or private entities			
Engage in observation or surveillance not requiring a court order			
Mail covers			
Physical searches of personal or real property where a warrant or court order is not legally required because there is no reasonable expectation of privacy (e.g., trash covers)			
Consensual monitoring of communications, including consensual computer monitoring, is subject to legal review by the CDC or the FBI OGC. Where a sensitive monitoring circumstance is involved, monitoring must be approved by the Criminal Division or, if the investigation concerns foreign intelligence or a threat to the national security, by the National Security Division			
Use of closed-circuit television, direction finders, and other monitoring devices, subject to legal review by the CDC or FBI OGC			
Polygraph examinations			
Undercover operations			
Compulsory process as authorized by law, including Federal Grand Jury and other subpoenas and National Security Letters (Federal Grand Jury subpoenas for telephone and electronic mail subscriber records can be used during type 1 and 2 Assessments only)			
Accessing stored wire and electronic communications and transactional records			
Use of pen registers and trap and trace devices			
Electronic surveillance			
Foreign intelligence collection under Title VII of FISA			
Physical searches, including mail openings, where a warrant or court order is legally required because there is an expectation of privacy.			



Investigative Methods/Approvals Chart

Authorized Method and DIOG Reference*	Approval Levels for Assessments and Predicated Investigations		
	Assessments	Predicated	Foreign Intelligence
1 5.9A Obtain publicly available information	None Required	None Required	None Required
Tasking a UCE to attend a religious service	Not Permitted	SSA Approval	SSA Approval
2 5.9B Physical surveillance of a person or group (Consult the DIOG for handheld photo and video surveillance with no reasonable expectation of privacy)	DIOG for requirements	None Required	None Required
	ASAC Approval	ASAC Approval	ASAC Approval
3 5.9C Access and examine FBI and other Department of Justice (DOJ) records, and obtain information from any FBI or other DOJ personnel	None Required	None Required	None Required
4 5.9D Access and examine records maintained by, and request information from, other federal, state, local, or tribal, or foreign governmental entities or agencies	None (Unless such approval is required by MOU or other agreements)	None (Unless such approval is required by MOU or other agreements)	None (Unless such approval is required by MOU or other agreements)
5 5.9E Use online services and resources (whether nonprofit or commercial)	None Required	None Required	None Required
6 5.9F Interview or request information from members of the public and private entities	None Required except for contact with represented persons, members of U.S. Congress, or their staffs, White House personnel, or other substantive division requirements	None Required except for contact with represented persons, members of U.S. Congress, or their staffs, White House personnel, or other substantive division requirements	None Required except for contact with represented persons, members of U.S. Congress, or their staffs, White House personnel, or other substantive division requirements
7 5.9G Accept information voluntarily provided by governmental or private entities	None Required	None Required	None Required
8 5.9H Use and recruit human sources	None Required (utilize [redacted])	None Required (utilize Delta)	None Required (utilize Delta)
Tasking a CHS to attend a religious service	SAC Approval	SSA Approval	SSA Approval
9 5.9I Federal Grand Jury subpoenas for telephone or electronic mail subscriber information	US Attorney Office Approval (Type 1 and 2 Assessments Only)	US Attorney Office Approval	Not Permitted
10 5.9C Pattern Based Data Mining	SORC	SORC	SORC

b2
b7E

Teaching Points:


- Obtain Publicly Available Information:** Supervisory approval is not required for use of this method, except as to information gathered at a religious service. Notwithstanding any other policy, tasking a CHS or UCE to attend a religious service during a predicated investigation, whether open to the public or not, requires SSA approval. Tasking a CHS to attend a religious service, whether open to the public or not, during an assessment requires SAC approval.
 - Engage in observation or surveillance not requiring a court order:** Use of mechanical devices operated by a user (e.g., binoculars; hand-held cameras; radiation, chemical or biological detectors) is authorized in physical surveillance provided the device is not used to collect information in which a person has a reasonable expectation of privacy (e.g., equipment such as a parabolic microphone or other listening device that would intercept a private conversation or thermal imaging a home is not permitted).
- Physical Surveillance: For assessments:** [redacted] surveillance begins as stated in the plan at the initiation of surveillance. Requires SSA or SIA approval. SSA or SIA authorized to approve physical surveillance requests in incremental periods. [redacted] FBI employee cannot submit multiple requests for one time approval. No limitation on use of fixed or moving physical surveillance. For predicated investigations: no limitation on use. [redacted] ASAC can delegate approval to SSA or SIA. Must be in writing and appropriately filed.
- Access and Examine FBI and other DOJ Records, and Obtain Information from any FBI or other DOJ Personnel:** Supervisory approval is not required to use this method during assessments or predicated investigations, except that if the use of records constitutes pattern-based data mining under the Federal Data Mining Reporting Act of 2007, it must be reviewed by the SORC and the FBI must report the pattern-based data mining to Congress.
 - Pattern-Based Data Mining Defined:** Use of one or more data bases to search for persons who fit a set of group characteristics or patterns of behavior (e.g., the known characteristics of a particular terrorist organization).
 - Use Online Services and Resources (whether non-profit or commercial):** Subscribing to or purchasing any new service must be done pursuant to FBI contracting procedures.
 - Interview Defined:** Questioning of an individual (to include the subject) designed to gather information from the person being interviewed that is accurate, pertinent to, and within the scope of an authorized assessment or predicated investigation.
- In normal course of interview, FBI should divulge employee's affiliation with FBI and true purpose of interview. If person being interviewed expresses desire not to provide information, FBI employee may not state or imply in any way that the interviewee is compelled to provide information or that adverse consequences may follow. If interviewee indicates he or she wishes to consult an attorney, the interview must immediately stop.
- Custodial Interviews:** Miranda warnings are required to be given prior to custodial interviews if the subject is significantly restricted in his/her freedom of action to a degree normally associated with arrest. See FBI Legal Handbook for Special Agents.
- Interviews that require supervisory approval:**
- contact with represented persons requires CDC review.
 - Members of U.S. Congress and Staff: Generally, FBI employees may take information received just as they would from other sources, and they may act upon it accordingly. However, prior CDC review, SAC and appropriate FBIHQ AD approval and prior notice to the AD Office of Congressional Affairs are required if FBI employee seeks to establish a formal relationship or interview a member of Congress or Congressional staff in connection with a foreign counterintelligence and/or public corruption matter.
 - White House Personnel: CDC review and SAC approval is required before initiating contact with White House personnel. CDC review, SAC approval and appropriate FBIHQ Section Chief approval must be obtained prior to conducting an interview of a member of the White House.

b2
b7E



- Accept Information Voluntarily Provided By Governmental or Private Entities:** Voluntarily provided information includes, but is not limited to: oral as well as documentary evidence and physical evidence such as: a computer hard drive or other electronic media that contains information, paper documents containing information, or physical objects (e.g., handgun or narcotics). FBI employee may not request nor knowingly accept information where disclosure would be prohibited by federal law (e.g., communications records).
- Access and Examine Records Maintained by, and Request Information From, Other Federal, State, Local, Tribal, or Foreign Governmental Entities or Agencies:** When requesting information using this authority, care must be taken to ensure the entity concerned understands that it is not compelled to provide such information or create a new record.
- Grand Jury Subpoenas for Telephone or Electronic Mail Subscriber Information:** Used only during a type 1 or 2 assessment. [redacted] Guardian [redacted]

UNCLASSIFIED//FOUO



Investigative Methods/Approvals Chart

Authorized Method and DIOG Reference*		Approval Levels for Assessments and Predicated Investigations		
		Assessments*	Predicated	Foreign Intelligence
11	11.3 Mail covers	Not Permitted		
12	11.4 Physical searches of personal or real property where a warrant or court order is not legally required because there is no reasonable expectation of privacy (e.g. [redacted])	[redacted]	[redacted]	[redacted]
13	11.5 Consensual monitoring of communications, including consensual computer monitoring	Not Permitted	CDC or OIG Review SSA Approval	CDC or OIG Review SSA Approval
14	11.5 Consensual monitoring of communications, including consensual computer monitoring, with a sensitive monitoring circumstance	Not Permitted	CDC or OIG Review, SAC Approval, DOJ Criminal or DOJ NSD Approval	CDC or OIG Review, SAC Approval, DOJ Criminal or DOJ NSD Approval
15	11.6 Use of closed-circuit television, direction finders, and other monitoring devices	Not Permitted	[redacted]	[redacted]
16	11.7 Polygraph examinations	Not Permitted	SSA Approval	SSA Approval
17	11.8 Undercover operations, Group II	[redacted]	CDC Review, SAC or ASAC with delegated authority; National Security cases also require NSD and UACB	CDC Review, SAC or ASAC with delegated authority; NSB-UH/UACB Approval
18	11.8 Undercover operations, Group I	Not Permitted	CDC review, SAC, and AD and GUORC or UGRG (EAD/DIO certain cases) Approval	CDC review, SAC and AD and UGRG (EAD/DIO certain cases) Approval
19	11.9 Compulsory process as authorized by law, Federal Grand Jury and trial subpoenas	[redacted]	US Attorney's Office Approval	[redacted]
20	11.9 Administrative Subpoenas, Drugs	Not Permitted	SAC, ASAC, SSRA, or Drug Squad SSA	Not Permitted
	11.9 Administrative Subpoenas, Sexual Exploitation		U.S. Attorney's Office Approval	
	11.9 Administrative Subpoenas, Healthcare Fraud		Field Office, CDC Review, ADIC or SAC Approval, HQ, NSLB Review, DD or EAD-NSB or AD & DADs CT/CD/Cyber or GC or Deputy GC-NSLB Approval	
21	11.9 National Security Letters	Not Permitted	Field Office, CDC Review, ADIC or SAC Approval, HQ, NSLB Review, DD or EAD-NSB or AD & DADs CT/CD/Cyber or GC or Deputy GC-NSLB Approval	Not Permitted
22	11.10 Accessing stored wire and electronic communications and transaction records	Not Permitted	Subpoena/Court Order, Consult DIOG	Not Permitted
23	11.11 Use of pen registers and trap and trace devices	Not Permitted	FISA Court or District Court Order	Only Available for Non-US/SPER by FISA Court order
24	11.12 Electronic surveillance	Not Permitted	[redacted]	[redacted]
25	11.13 Physical searches, where there is reasonable expectation of privacy, including mail openings	[redacted]	[redacted]	[redacted]
26	11.14 Acquisition of foreign intelligence information in conformity with Title VII of the Foreign Intelligence Surveillance Act	[redacted]	FISA Court Order	FISA Court order

UNCLASSIFIED//FOUO As of May 19, 2009 66

b2
b7E

Teaching Points:

1. **Mail Covers:** The DIOG currently states that for national security mail covers, "after being approved by the SSA, the Field Office must transmit the mail cover letter request by EC, with the draft letter as an attachment, to the National Security Law Branch (NSLB) for legal review and concurrence. Upon review and concurrence, the NSLB must transmit the letter request for signature to the EAD, National Security Branch, or, in his or her absence, to the Director.

2. **Consensual Monitoring:** [redacted] Field Office must ensure that the individual who approves OIA is so authorized. For example, if the SAC has delegated authority to approve OIA for consensual monitoring to the SSA, upon CDC review, the SSA can approve the consensual monitoring and OIA. If OIA authority was not delegated to SSA, appropriate supervisory authority must expressly approve OIA.

b2
b7E

3. **Administrative Subpoenas:** Within the FBI, the authority to issue administrative subpoenas is limited to those positions holding the delegated authority from the Attorney General; that authority may not be redelegated. [redacted]

[redacted]

Three Types of Administrative Subpoenas Authorized: (i) drug program investigations; (ii) child sexual exploitation and abuse investigations; (iii) health care fraud investigations.

4. **National Security Letters:** Authority to sign NSLs has been delegated to the Deputy Director, EAD and Assistant EAD for NSB; ADs and all DADs for CT/CD/Cyber; General Counsel; DGC for NSLB; ADICs in NY, DC and LA; and all SACs. Every NSL must be reviewed and approved by a CDC or NSLB attorney.

UNCLASSIFIED//FOUO

DIOG Training

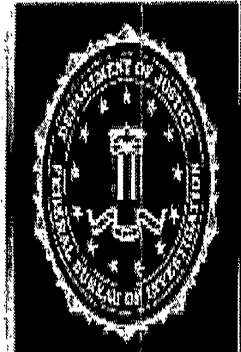
FEDERAL BUREAU OF INVESTIGATION

OVERALL CLASSIFICATION:

UNCLASSIFIED

Session C – Quantico

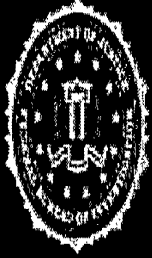
Privacy, Civil Liberties, Strategic Analysis
& Intel Collection, and PFI Full
Investigations



FEDERAL
BUREAU OF
INVESTIGATION

UNCLASSIFIED//FOUO

UNCLASSIFIED//FOUO



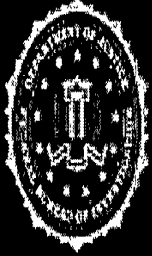
DIOG Sections 4, 9, 15

SSA ...

Division ...

– (Tel Number)

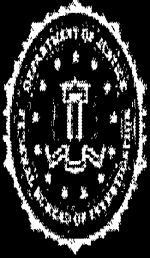
UNCLASSIFIED//FOUO



Course Overview

Overall Training Objective:

Provide an instructional foundation on the DIOG and then apply the knowledge gained by using hypothetical examples and scenarios. Upon completing this course of instruction you should have a firm grasp of the concepts and principles underpinning the DIOG.

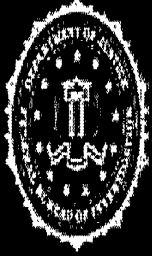


Course Overview

Participation Standards:

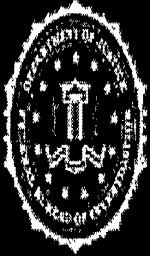
Questions are welcome; however, if your question is about a specific set of facts that may divert the training objective, please direct your question to one of the Training team members at a break for a response.

During the scenario exercises, participants will be called upon to provide their response to particular facts or circumstances. Each Unit/Section should select a representative to speak for the Unit/Section and rotate that responsibility among the group. The scenarios are meant to prompt discussion, but the presenters must keep the scenario moving forward. Please understand that everyone may not be able to voice their perspective in the group setting. Keep in mind there may be several avenues to reach the same justified conclusion. You may use your handouts and training aids to inform your decision.



DIOG Section 1: Scope & Purpose

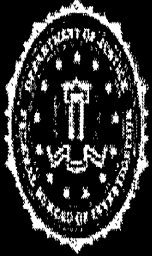
- **DIOG applies to all investigative and intelligence collection activities conducted by the FBI**
 - within the United States
 - in the United States territories
 - outside the territories of all countries
- **DIOG does not apply to investigative and intelligence collection activities of the FBI in foreign countries**
 - governed by AGGs for Extraterritorial FBI Operations (national security and criminal)



DIOG Section 1: Scope & Purpose

In addition to this policy document, each FBIHQ substantive Division has a Policy Implementation Guide (PG) that supplements the DIOG.

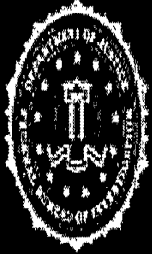
As a result, numerous FBI manuals, electronic communications, letterhead memoranda, and other policy documents are incorporated into the DIOG and Division PGs, thus, consolidating FBI policy guidance.



DIOG Overview

The AGG-Dom replaces the following six guidelines:

- The Attorney General's Guidelines on General Crimes, Racketeering Enterprise and Terrorism Enterprise Investigations (May 30, 2002)
- The Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection (October 31, 2003)
- The Attorney General's Supplemental Guidelines for Collection, Retention, and Dissemination of Foreign Intelligence (November 29, 2006)
- The Attorney General Procedure for Reporting and Use of Information Concerning Violations of Law and Authorization for Participation in Otherwise Illegal Activity in FBI Foreign Intelligence, Counterintelligence or International Terrorism Intelligence Investigations (August 8, 1988).
- The Attorney General's Guidelines for Reporting on Civil Disorders and Demonstrations Involving a Federal Interest (April 5, 1976)
- The Attorney General's Procedures for Lawful, Warrantless Monitoring of Verbal Communications (May 30, 2002) [only portion applicable to FBI repealed]



Policy Environment for Domestic Operations

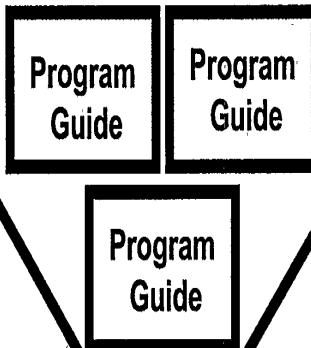
Constitution, Statutes, and Executive Orders

AG GUIDELINES (AGG-Dom)

Apply to domestic national security and criminal investigative activities, including interagency coordination and intelligence analysis.

FBI's Domestic Investigations and Operations Guide (DIOG)

Program Policy Implementation Guides

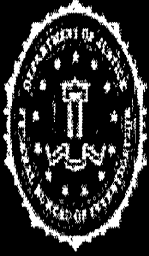




DIOG:

Table of Contents

1. Scope and Purpose	10. Sensitive Investigative Matter
2. General Authorities and Principles	11. Investigative Methods
3. Core Values, Roles and Responsibilities	12. Assistance to Other Agencies
4. Privacy and Civil Liberties, and Least Intrusive Methods	13. Extraterritorial Provisions
5. Assessments	14. Retention and Sharing of Information
6. Preliminary Investigations	15. Intelligence Analysis and Planning
7. Full Investigations	16. Undisclosed Participation
8. Enterprise Investigations	17. Otherwise Illegal Activity
9. Foreign Intelligence	Appendices



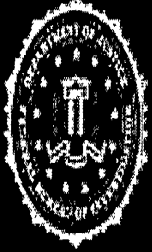
DIOG Overview

The Test...

50 questions

- **Multiple Choice**
- **True/False**

**** Max 20 mins each question***

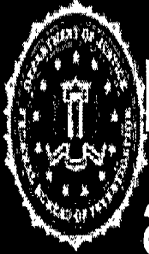


DIOG Overview

Taking the test...

- Access to testing site
- Materials
 - DIOG
 - Charts
 - PowerPoint slides
 - Notes

**** Max 20 mins each question***

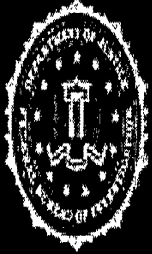


DIOG Section 4: Privacy and Civil Liberties, and Least Intrusive Methods

- **15.1. Overview**

The AGG-Dom provide specific guidance and authorization for intelligence analysis and planning. This authority enables the FBI to identify and understand trends, causes, and potential indicia of criminal activity and other threats to the United States that would not be apparent from the investigation of discrete matters alone. By means of intelligence analysis and planning, the FBI can more effectively discover criminal threats, threats to the national security, and other matters of national intelligence interest, and can provide the critical support needed for the effective discharge of its investigative responsibilities and other authorized activities.

(AGGDom, Part IV)



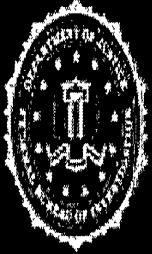
DIOG Section 4: Privacy and Civil Liberties, and Least Intrusive Methods

- Responsibility to protect the American public, not only from crime and terrorism, but also from incursions into their constitutional rights; accordingly, all investigative activities must fully adhere to the Constitution and the principles of civil liberty and privacy.
- Provisions of the AGG-Dom, other AG guidelines, and oversight from DOJ components, are designed to ensure FBI's activities are lawful, appropriate, and ethical, as well as effective in protecting civil liberties and privacy.
- DOJ and FBI's Inspection Division, Office of Integrity and Compliance, the OGC, other Bureau components, and **you** share responsibility for ensuring the FBI meets these goals.



DIOG Section 4: Privacy and Civil Liberties, and Least Intrusive Methods

- No investigation or assessment can be commenced based solely on race, ethnicity, national origin, religion of the subject or the exercise of First Amendment rights.
- Corollary to this AGG requirement is the Privacy Act, which states that each agency that maintains a system of records shall “maintain no record describing how any individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute or by the individual about whom the record is maintained or **unless pertinent to and within the scope of an authorized law enforcement activity.** 5 U.S.C. 552a(e)(7).



DIOG Section 4 Scenario

- [Empty rectangular box for notes]

b2
b7E

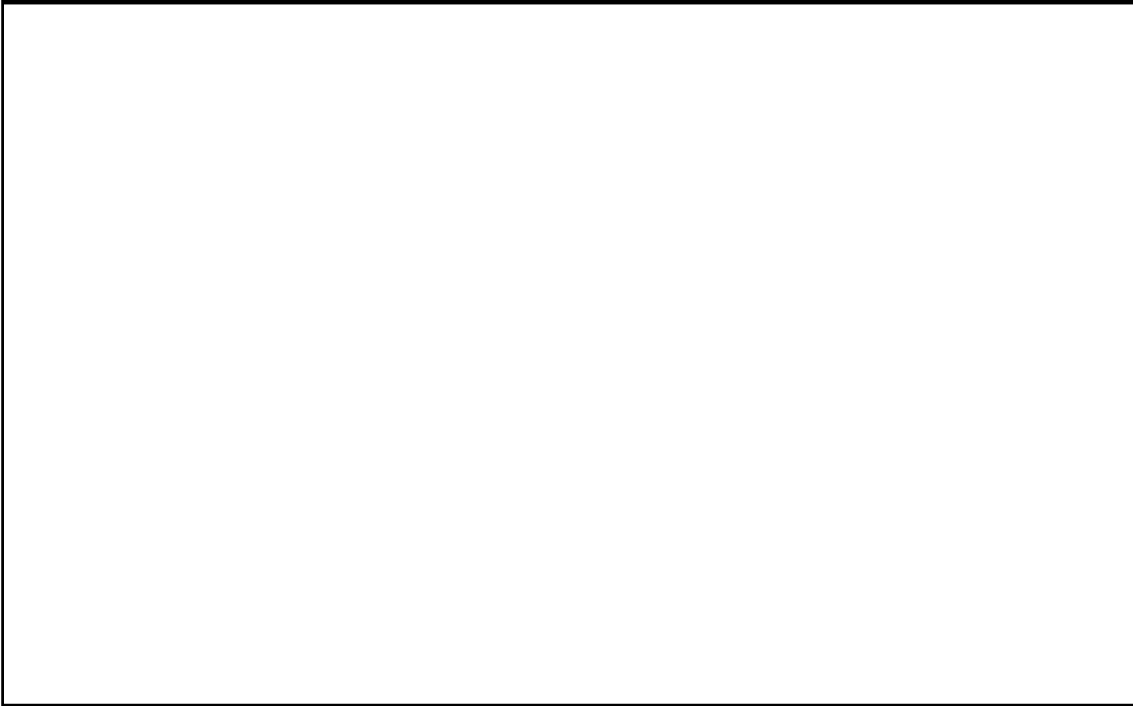
- What can you do with this information?

- [Empty rectangular box for notes]
- [Empty rectangular box for notes]
- [Empty rectangular box for notes]

UNCLASSIFIED//FOUO



DIOG Section 4 Scenario



b2
b7E

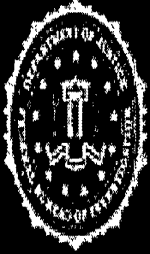
UNCLASSIFIED//FOUO



DIOG Section 4: Privacy and Civil Liberties, and Least Intrusive Methods

FIRST AMENDMENT RIGHTS:

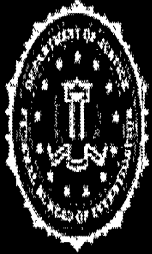
Individuals or groups who communicate with each other or with members of the public in any form in pursuit of social or political causes—such as opposing war or foreign policy, protesting government actions, promoting certain religious beliefs, championing particular local, national, or international causes, or a change in government through non-criminal means, and actively recruit others to join their causes—have a fundamental constitutional right to do so. An assessment may not be initiated based solely on the exercise of these First Amendment rights. If, however, a group exercising its First Amendment rights also threatens or advocates violence or destruction of property, an assessment would be appropriate



DIOG Section 4: Privacy and Civil Liberties, and Least Intrusive Methods

FIRST AMENDMENT RIGHTS (cont.):

- No investigative activity, including assessments, may be taken solely on the basis of activities that are protected by the First Amendment or on the race, ethnicity, national origin or religion of the subject.
- If an assessment or predicated investigation touches on or is partially motivated by First Amendment activities, race, ethnicity, national origin or religion, it is particularly important to identify and document the basis for the assessment with clarity



DIOG Section 4: Privacy and Civil Liberties, and Least Intrusive Methods

All activities must be consistent with the Attorney General's 2003 Guidance Regarding the Use of Race by Federal Law Enforcement Agencies (forbids the use of racial profiling and requires activities involving the investigation or prevention of threats to the national security to comply with the Constitution and laws of the United States)

The DIOG stresses several points in each section:

- No investigation or assessment can be commenced based solely on race, ethnicity, national origin, religion, or exercise of First Amendment rights
- The FBI must use the least intrusive method that is feasible under the circumstances
- In connection with Foreign Intelligence collection, agents must operate openly and consensually with U.S. Persons, to the extent practicable
- All investigative activities must have an "authorized purpose"

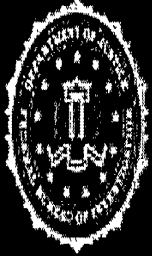


DIOG Section 4: Use of Race or Ethnicity

DIOG Guidance on use of Race or Ethnicity

As to individuals:

1. Permits the consideration of ethnic and racial identity information based on specific reporting;
2. The race or ethnicity of suspected members, associates, or supporters of an ethnic-based gang or criminal enterprise may be collected when gathering information about or investigating the organization; or
3. Ethnicity may be considered in evaluating whether a subject is—or is not—a possible associate of a criminal or terrorist group that is known to be comprised of members of the same ethnic grouping—as long as it is not the dominant factor for focusing on a particular person

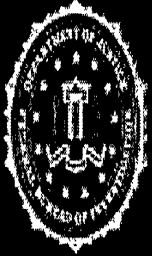


DIOG Section 4: Use of Race or Ethnicity

DIOG Guidance on use of Race or Ethnicity

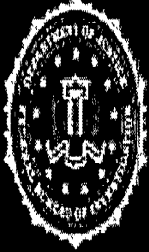
As to a community:

1. Collecting and analyzing demographics – if these locations will reasonably aid the analysis of potential threats and vulnerabilities, and, overall, assist domain awareness
2. Geo-Mapping ethnic/racial demographics – if properly collected
3. General ethnic/racial behavior – cannot be collected, unless it bears a rational relationship to a valid investigative or analytical need
4. Specific and relevant ethnic behavior
5. Exploitive ethnic behavior – by criminal or terrorist groups



DIOG Section 4: Least Intrusive Investigative Method

The AGG-DOM and the DIOG require that the “least intrusive” means or method be considered and, if operationally sound and effective, used to obtain intelligence or evidence in lieu of a more intrusive method



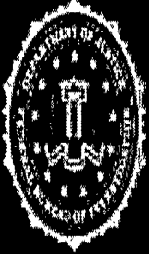
DIOG Section 4: Privacy and Civil Liberties, and Least Intrusive Methods

By emphasizing the use of less intrusive means, employees will be able to balance:

Our need for evidence/intelligence

VS.

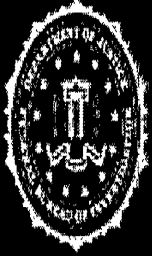
Mitigating potential negative impact on the privacy and civil liberties of people/public



DIOG Section 4: Privacy and Civil Liberties, and Least Intrusive Methods

Primary factor in determining “intrusiveness”:

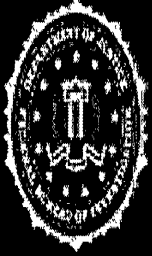
- The degree of procedural protection that the law and the AGG-DOM provide for the use of the particular method.
 - Examples of “more intrusive” methods: Search Warrants, wiretaps, UCOs
 - Examples of “less intrusive” methods: checks of government databases, state or local criminal record checks, commercial databases, interviews



DIOG Section 4: Privacy and Civil Liberties, and Least Intrusive Methods

Items to consider when determining the relative intrusiveness of an investigative method:

- Is method permitted prior to the initiation of an assessment?
- Is the method relevant to the assessment or investigation?
- Will the information collected or obtained likely further the investigative objective?
- What alternatives exist for gathering the same information?
- Are those alternatives relatively less intrusive?
- What time span is involved in using the investigative method (days, weeks, months)?
- What confidence level is associated with the information gathered using the investigative method?
- Will the method resolve a pending investigative issue quickly?



DIOG Section 4: Least Intrusive Investigative Method

Factors to Determine “Intrusiveness”:

1. Nature of the information sought
2. Scope of the information sought
3. Scope of the use of the investigative method
4. Source of the information sought
5. Risk of public exposure

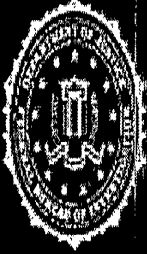


DIOG Section 5 & 11: Investigative Methods

Authorized Methods for Assessments and Predicated Investigations

Red indicates methods not allowed under a particular operational activity; Green indicates methods allowed.

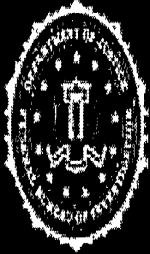
	Assessments	Preliminary Investigations	Full Investigations
Obtain publicly available information			
Access and examine FBI and other DOJ records, and obtain information from any FBI or DOJ personnel			
Access and examine records maintained by, and request information from, other federal, state, local, tribal, or foreign governmental entities or agencies			
Use online services and resources (whether nonprofit or commercial)			
Use and recruit human sources in conformity with AG Guidelines Regarding the Use of FBI Confidential Human Sources			
Interview or request information from members of the public and private entities [includes pretextual interviews]			
Accept information voluntarily provided by governmental or private entities			
Engage in observation or surveillance not requiring a court order			
Mail covers			
Physical searches of personal or real property where a warrant or court order is not legally required because there is no reasonable expectation of privacy (e.g., trash covers)			
Consensual monitoring of communications, including consensual computer monitoring, is subject to legal review by the CDC or the FBI OGC. Where a sensitive monitoring circumstance is involved, monitoring must be approved by the Criminal Division or, if the investigation concerns foreign intelligence or a threat to the national security, by the National Security Division			
Use of closed-circuit television, direction finders, and other monitoring devices, subject to legal review by the CDC or FBI OGC			
Polygraph examinations			
Undercover operations			
Compulsory process as authorized by law, including Federal Grand Jury and other subpoenas and National Security Letters (Federal Grand Jury subpoenas for telephone and electronic mail subscriber records can be used during type 1 and 2 Assessments only)			
Accessing stored wire and electronic communications and transactional records			
Use of pen registers and trap and trace devices			
Electronic surveillance			
Foreign Intelligence collection under Title VII of FISA			
Physical searches, including mail openings, where a warrant or court order is legally required because there is an expectation of privacy			



Investigative Methods/Approvals Chart

Authorized Method and DIOG Reference*		Approval Levels for Assessments and Predicated Investigations			
		Assessments	Predicated	Foreign Intelligence	
1	5.9A	Obtain publicly available information	None Required	None Required	None Required
		Tasking a UCE to attend a religious service	Not Permitted	SSA Approval	SSA Approval
2	5.9B	Physical surveillance of a person or group (Consult the DIOG for handheld photo and video surveillance with no reasonable expectation of privacy)	[Redacted] consult DIOG for requirements	None Required	None Required
		[Redacted]	[Redacted]	ASAC Approval	ASAC Approval
		[Redacted]	[Redacted]	ASAC Approval	ASAC Approval
3	5.9C	Access and examine FBI and other Department of Justice (DOJ) records, and obtain information from any FBI or other DOJ personnel	None Required	None Required	None Required
4	5.9D	Access and examine records maintained by, and request information from, other federal, state, local, or tribal, or foreign governmental entities or agencies	None (Unless such approval is required by MOU or other agreements)	None (Unless such approval is required by MOU or other agreements)	None (Unless such approval is required by MOU or other agreements)
5	5.9E	Use online services and resources (whether nonprofit or commercial)	None Required	None Required	None Required
6	5.9F	Interview or request information from members of the public and private entities	None Required except for contact with represented persons; members of U.S. Congress, or their staffs, White House personnel, or other substantive division requirements	None Required except for contact with represented persons; members of U.S. Congress, or their staffs, White House personnel, or other substantive division requirements	None Required except for contact with represented persons; members of U.S. Congress, or their staffs, White House personnel, or other substantive division requirements
7	5.9G	Accept information voluntarily provided by governmental or private entities	None Required	None Required	None Required
8	5.9H	Use and recruit human sources	None Required (utilize [Redacted])	None Required (utilize Delta)	None Required (utilize Delta)
		Tasking a CHS to attend a religious service	SAC Approval	SSA Approval	SSA Approval
9	5.9I	Federal Grand Jury subpoenas for telephone or electronic mail subscriber information	US Attorney Office Approval (Type 1 and 2 Assessments Only)	US Attorney Office Approval	Not Permitted
10	5.9C	Pattern Based Data Mining	SORC	SORC	SORC

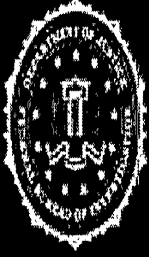
b2
b7E



Investigative Methods/Approvals Chart

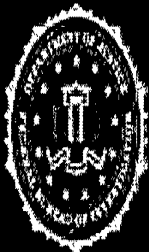
Authorized Method and DIOG Reference*		Approval Levels for Assessments and Predicated Investigations		
		Assessments	Predicated	Foreign Intelligence
11	11.3	Mail covers	[]	[]
12	11.4	Physical searches of personal or real property where a warrant or court order is not legally required because there is no reasonable expectation of privacy (e.g. [])	[]	[]
13	11.5	Consensual monitoring of communications, including consensual computer monitoring	Not Permitted	CDC or OGC Review SSA Approval
14	11.5	Consensual monitoring of communications, including consensual computer monitoring, with a sensitive monitoring circumstance	Not Permitted	CDC or OGC Review, SAC Approval, DOJ Criminal or DOJ NSD Approval
15	11.6	Use of closed-circuit television, direction finders, and other monitoring devices	[]	[]
16	11.7	Polygraph examinations	[]	SSA Approval
17	11.8	Undercover operations, Group II	[]	CDC Review, SAC or ASAC with delegated authority; National Security cases also require NSD unit UACB
18	11.8	Undercover operations, Group I	[]	CDC review, SAC, and AD and CUORC or UCRC (EAD/DD certain cases) Approval
19	11.9	Compulsory process as authorized by law; Federal Grand Jury and trial subpoenas	[]	US Attorney's Office Approval
20	11.9	Administrative Subpoenas: Drugs	Not Permitted	SAC, ASAC, SSRA, or Drug Squad SSA
		Administrative Subpoenas: Sexual Exploitation		[]
		Administrative Subpoenas: Healthcare Fraud		U.S. Attorney's Office Approval
21	11.9	National Security Letters	Not Permitted	Field Office: CDC Review, ADIC or SAC Approval.
				HQ: NSLB Review; DD or EAD-NSB or AD & DADs CT/CD/CyD or GC or Deputy GC-NSLB Approval
22	11.10	Accessing stored wire and electronic communications and transactional records	Not Permitted	Statute/Court Order, Consult DIOG
23	11.11	Use of pen registers and trap and trace devices	Not Permitted	FISA Court or District Court Order
24	11.12	Electronic surveillance	[]	[]
25	11.13	Physical searches, where there is reasonable expectation of privacy, including mail openings	[]	[]
26	11.14	Acquisition of foreign intelligence information in conformity with Title VII of the Foreign Intelligence Surveillance Act	[]	FISA Court Order

b2
b7E



DIOG Section 15: Intelligence Analysis and Planning

- **Overview:** Authority for planning and developing intelligence analysis to support the intelligence functions and missions of the FBI is incorporated in AGG-Dom, Part IV. This section elaborates upon the means by which the investigative assessments outlined in AGG-Dom, Part II are authorized for the FBI to undertake in executing its mission to discover and avert criminal threats and threats to US national security
- The term “assessment” as used within the DOJ to describe aspects of investigative activity should not be confused with the intelligence community use of the same word to describe intelligence analysis products such as an intelligence assessment



DIOG Section 15: Intelligence Analysis and Planning

- Strategic Planning and Analysis: The FBI is authorized to develop overviews and analysis of threats to and vulnerabilities of the United States and its interests in areas relative to the FBI's responsibilities. The FBI employs the following methodologies to identify, target and assess these threats:
 - Domain Management
 - Collection Management
 - Written Intelligence Products
 - Geospatial Intelligence (GEOINT)



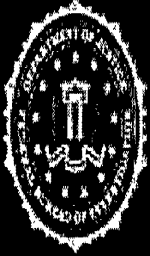
DIOG Section 15: Intelligence Analysis and Planning

- **Domain Management** (cont.): Domain Management is undertaken at the Field Office and national levels. All National Domain Assessments must be coordinated in advance with the Directorate of Intelligence. All information collected for Domain Management must be documented in



- **Collection Management:** A formal business process through which Intelligence Information Needs and Intelligence Gaps (e.g., unknowns) are expressed as Intelligence Collection Requirements (questions or statements requesting information), prioritized in a comprehensive, dynamic Intelligence Collection Plan.

b2
b7E



DIOG Section 15: Intelligence Analysis and Planning

Written Intelligence Products: The FBI produces written intelligence products which represent the results of collection efforts in the field (raw intelligence) and analytic judgments made from the compilation and synthesis of relevant raw intelligence (finished intelligence).

US Person Information: Information regarding US persons is not to be included in intelligence products if the pertinent intelligence can be conveyed without including identifying information. An exception would be if the context for usage is publicly accessible information, i.e., the white powder anthrax letter addressed to Senator Tom Daschle in October 2001.



DIOG Section 15: Intelligence Analysis and Planning

- **Raw Intelligence:** This represents information collected from sources which is generally considered to be unvetted or not confirmed by other reporting means. Such reporting information is typically captured in Intelligence Information Reports (IIRs), FD 302s and ECs.
- **Finished Intelligence:** Such reports represent judgments made by intelligence analysts in the field or at FBIHQ regarding the synthesis of multiple, relevant raw intelligence source reports which indicate probable intent or action by threat actors of either a criminal or national security nature. FBI finished intelligence products used are the Intelligence Bulletin (IB), Intelligence Assessment (IA) and Special Event Threat Assessment (SETA). Domain Assessments and briefings can also represent finished intelligence products.



DIOG Section 15: Intelligence Analysis and Planning

Intelligence Systems: The FBI is authorized to operate intelligence, identification, tracking and information systems in support of authorized investigative activities or for such other additional purposes as may be legally authorized, such as intelligence tracking systems related to terrorists, gangs, or organized crime groups.

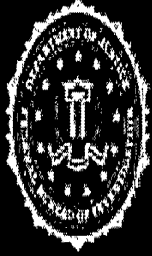
Information is shared both internally within the FBI and externally to LE orUSIC partners as appropriate based on the classification and handling instructions established by the managers of the programs which have created these files or reports. Common information platforms used for sharing and receiving intelligence products are Law Enforcement Online (LEO), Intellink (both Secret and Top Secret for theUSIC) and [redacted] for the counter-terrorism community.

b2
b7E



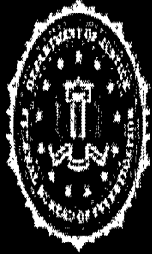
DIOG Section 15: Intelligence Analysis and Planning

Geospatial Intelligence (GEOINT) is the exploitation and analysis of imagery and geospatial information to describe, assess and visually depict physical features and geographically- referenced activities on the Earth. **Mapping** is an activity under GEOINT and may be used in assessments (Domain Management; Collection Management) and predicated investigations



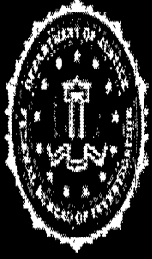
DIOG Section 9: Foreign Intelligence

Investigation	Predication	Duration	Documentation	Approval	Justification Review	SIM	Responsible Entity
PFI Full	Investigation may obtain foreign intelligence that is responsive to a foreign intelligence requirement	Until the requirement is met; No time limit	EC	Prior D/CMS notice to DOJ/NSO within 30 days	Every 90 days; if probationary employee, every 60 days	CDC Review, SAC Approval; Section Chief approval	FIG



DIOG Section 9: Foreign Intelligence

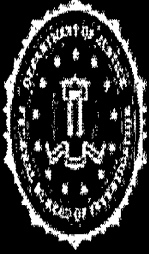
- **Foreign Intelligence** is “information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorists.”
- A **Foreign Intelligence Requirement** is a collection requirement issued by USIC and accepted by the FBI DI. Foreign Intelligence Requirements from the USIC fall into two categories which are
 - **FBI Requirements** are those that address national security issues that are within the FBI’s core national security mission
 - **Positive Foreign Intelligence Requirements** are those that address the military, economic and foreign relations concerns of foreign governments, which are within FBI’s responsibility as part of the USIC but are not directly related to national security concerns



DIOG Section 9: Foreign Intelligence

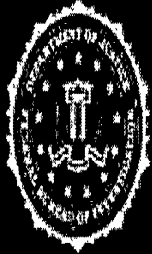
- Requirements in the first category that are accepted by the DI as "FBI Requirements" will be worked within a properly authorized Type 3 Assessment or incidental to a predicated case worked by a substantive squad.
- Foreign Intelligence Requirements that fall into the second category will be worked exclusively under [redacted] and will be referred to as "Positive Foreign Intelligence" Requirements.

b2
b7E



DIOG Section 9: Positive Foreign Intelligence

- Positive Foreign intelligence (PFI) collection in the FBI is a requirements-based activity
- Under the AGG-Dom, there are two categories of “authorized activity” under which PFI may be collected:
 - a (non-predicated) **Assessment** relating to “a matter of foreign intelligence interest” responsive to FI requirements
 - a **Full Investigation** predicated on an FI requirement
 - *Both must be requirements-based and approved by FBIHQ DI*
- In collecting FI, the FBI will generally be guided by nationally-determined intelligence requirements, including the National Intelligence Priorities Framework and the National HUMINT Collection Directives, or any successor directives issued under the authority of the Director of National Intelligence



PFI Full Investigations

- Used when a collection capability (source) is established or positively identified.
- PFI requirement must have been accepted by the FBI as the agency with “primary” collection responsibility.
- The authorized purpose must be documented in the opening EC
- Must be approved in advance by DI, CMS, CPMU - Files opened by the Field Office.
- Sensitive PFI matters require field office CDC review, SAC approval & CMS Section Chief approval.
- Unique PFI file number for each DI, CMS, CPMU approved PFI requirement.
- Approval EC from CPMU will contain explicit directions regarding the approved PFI investigation title, requirement, etc.
- No duration limit for PFI full investigations.

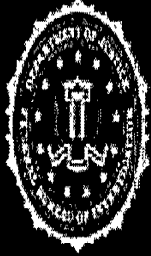
b2
b7E



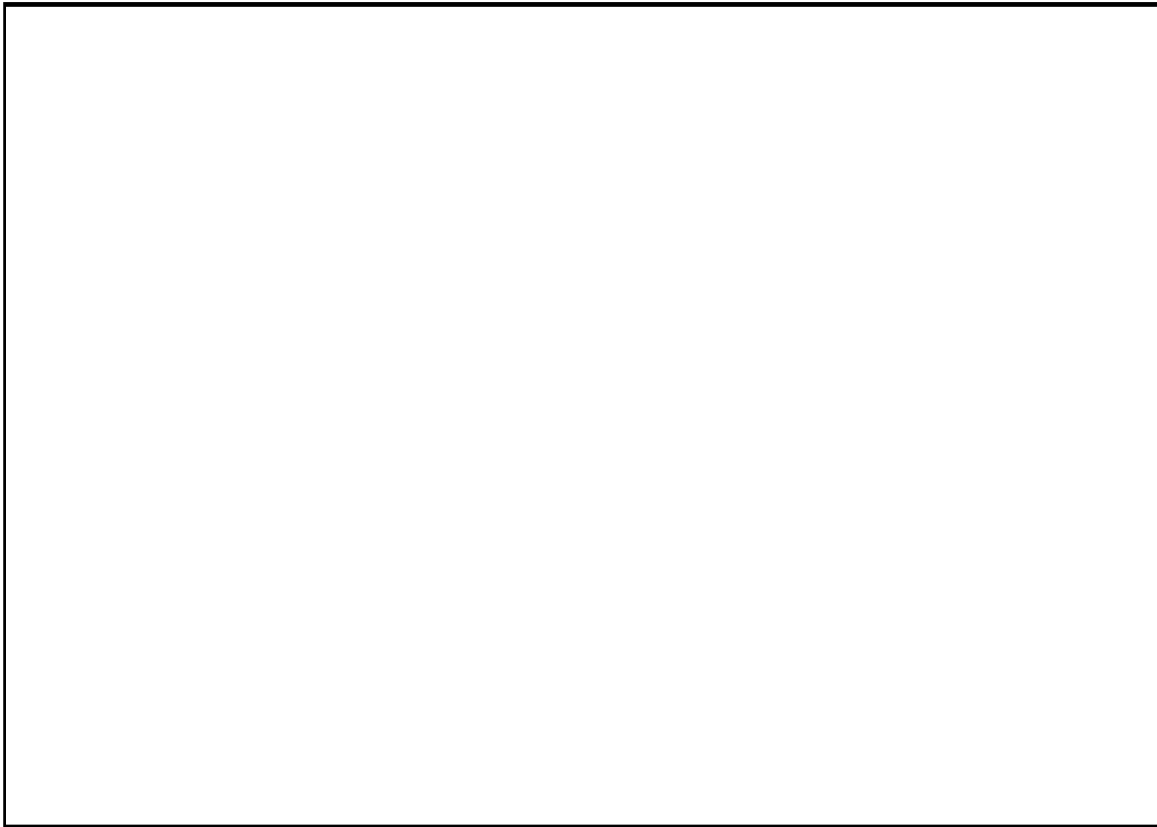
Privacy Act / USPER Considerations

- PFI is not about people – it is about a foreign power's capabilities, intentions or activities...
 - Avoid identifying individuals (USPERS) in PFI files unless ID is essential to satisfy the collection requirement.
 - If you must ID U.S. persons (covered by the Privacy Act) limit any/all identifying info to basic identifiers.
 - If you must ID U.S. persons (covered by the Privacy Act) do not index the person in ACS.
 - Utilize or a Type 5 assessment to record information about prospective or potential sources, etc.

b2
b7E

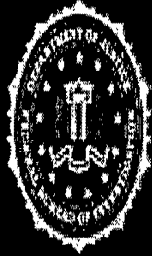


DIOG Section 9: Example

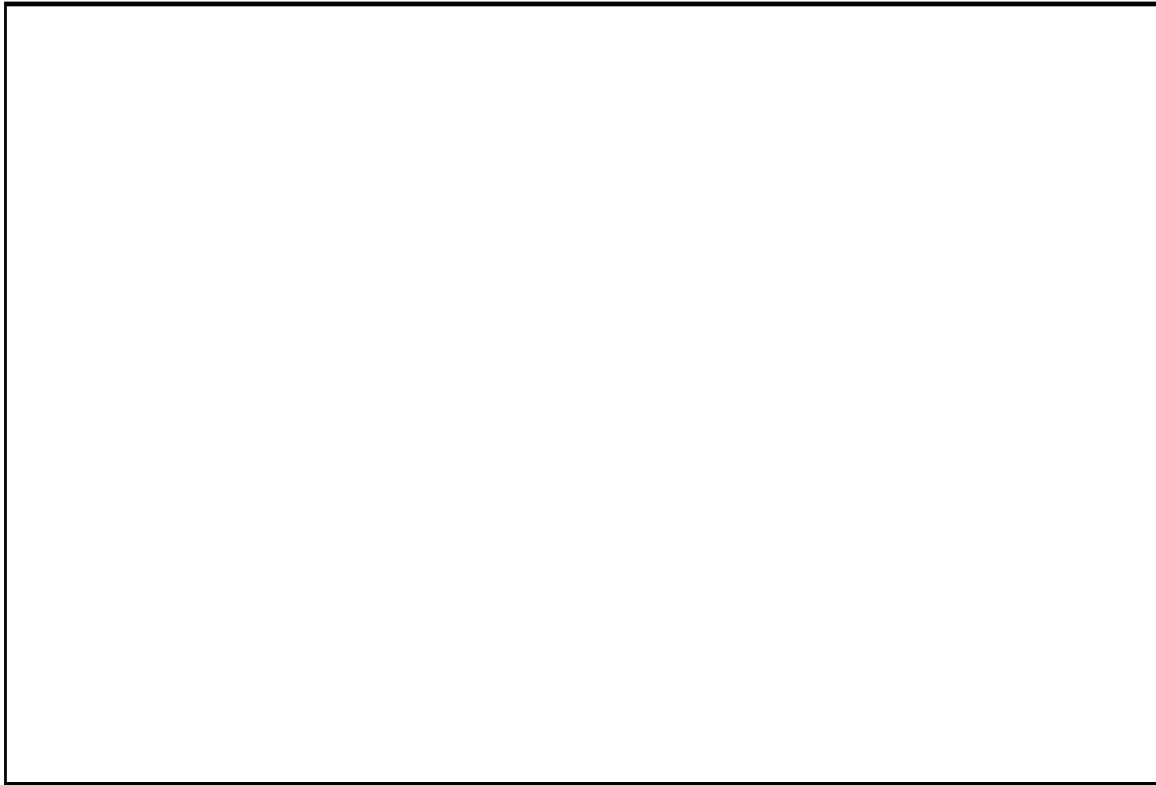


- Should Indianapolis open a PFI Assessment?

b2
b7E

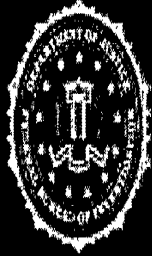


DIOG Section 9: Example



b2
b7E

UNCLASSIFIED//FOUO




FBIHQ DIOG Training

Thank you...

SSA

UNCLASSIFIED//FOUO


UNCLASSIFIED//FOUO



FEDERAL BUREAU OF INVESTIGATION

OVERALL CLASSIFICATION:
UNCLASSIFIED


FBIHQ DIOG Training Session A



FEDERAL
BUREAU OF
INVESTIGATION

UNCLASSIFIED//FOUO

UNCLASSIFIED//FOUO



Course Overview

Overall Training Objective:

Provide an instructional foundation on the DIOG and then apply the knowledge gained by using hypothetical examples and scenarios. Upon completing this course of instruction you should have a firm grasp of the concepts and principles underpinning the DIOG.

UNCLASSIFIED//FOUO 2



UNCLASSIFIED//FOUO

Course Overview

Participation Standards:

Questions are welcome; however, if your question is about a specific set of facts that may divert the training objective, please direct your question to one of the Training team members at a break for a response.

During the scenario exercises, participants will be called upon to provide their response to particular facts or circumstances. Each Unit/Section should select a representative to speak for the Unit/Section and rotate that responsibility among the group. The scenarios are meant to prompt discussion, but the presenters must keep the scenario moving forward. Please understand that everyone may not be able to voice their perspective in the group setting. Keep in mind there may be several avenues to reach the same justified conclusion. You may use your handouts and training aids to inform your decision.

UNCLASSIFIED//FOUO

3



UNCLASSIFIED//FOUO

Course Overview

Course Completion:

- You must complete the entire mandatory 16.5 hours of training. You must score an 80% or higher to pass. You will be notified of your score via e-mail. If you do not pass the first time, you will be permitted to take the test again.
- Please annotate on the attendance sheet your presence at the training if you pre-registered. If you did not pre-register, please print your name, division, and the items requested on the attendance roster.
- After the course is complete, you will be receiving a survey e-mail containing questions that will test your knowledge and understanding of the material presented. The test is open book.

UNCLASSIFIED//FOUO

4



UNCLASSIFIED//FOUO

AGG-Dom: Overview

- Provides ability to FBI authorities to be more proactive and preventative, and the flexibility to deal with complex threats that do not fall neatly into individual programs
- Provides clarity and improves compliance by combining several sets of guidelines into one consistent set of guidelines
- Removes discrepancies, sets uniform rules for criminal, national security, and foreign intelligence collection cases. Each program will have a program-specific policy guide (PG)

UNCLASSIFIED//FOUO

5



UNCLASSIFIED//FOUO

AGG-Dom: Overview

- Reduces reporting requirements, particularly in the national security area
- Recognizes Special Events and Domain Management as part of the FBI's mission
- Recognizes the FBI's obligation to provide investigative assistance and joint operational support to other agencies, including the U.S. intelligence community
- Creates a new category outside of predicated investigations named "Assessments"

UNCLASSIFIED//FOUO

6



UNCLASSIFIED//FOUO

Policy Environment for Domestic Operations

Constitution, Statutes, and Executive Orders

AG GUIDELINES (AGG-Dom)

Apply to domestic national security and criminal investigative activities, including interagency coordination and intelligence analysis.

FBI's Domestic Investigations and Operations Guide (DIOG)

Program Policy Implementation Guides

Program Guide

Program Guide

Program Guide

UNCLASSIFIED//FOUO

7



UNCLASSIFIED//FOUO

DIOG Section 1: Scope & Purpose

- **DIOG applies to all investigative and intelligence collection activities conducted by the FBI**
 - within the United States
 - in the United States territories
 - outside the territories of all countries
- **DIOG does not apply to investigative and intelligence collection activities of the FBI in foreign countries**
 - governed by AGGs for Extraterritorial FBI Operations (national security and criminal)

UNCLASSIFIED//FOUO

8



UNCLASSIFIED//FOUO

DIOG Section 1: Scope & Purpose

- The primary purpose of the AGG-DOM and the DIOG is to standardize policy so that criminal, national security and foreign intelligence investigative activities are performed in a legal and consistent manner
- The DIOG replaces numerous FBI manuals, electronic communications, letterhead memoranda and other policy documents. The DIOG is located on the Corporate Policy Office (CPO) Policy and Guidance Library web site
- The changes implemented by the DIOG better equip you to protect the people of the United States against crime and threats to the national security
- The DIOG stresses the importance of oversight and self-regulation to ensure compliance

UNCLASSIFIED//FOUO

9



UNCLASSIFIED//FOUO

DIOG Section 2: General Authorities & Principles

- **The AGG-Dom replaces six guidelines:**
 - The Attorney General's Guidelines on General Crimes, Racketeering Enterprise and Terrorism Enterprise Investigations (May 30, 2002)
 - The Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection (October 31, 2003) *
 - The Attorney General's Supplemental Guidelines for Collection, Retention, and Dissemination of Foreign Intelligence (November 29, 2006)

UNCLASSIFIED//FOUO

10



UNCLASSIFIED//FOUO

DIOG Section 2: General Authorities & Principles

- **The AGG-Dom also replaces:**
 - The Attorney General Procedure for Reporting and Use of Information Concerning Violations of Law and Authorization for Participation in Otherwise Illegal Activity in FBI Foreign Intelligence, Counterintelligence or International Terrorism Intelligence Investigations (August 8, 1988) *
 - The Attorney General's Guidelines for Reporting on Civil Disorders and Demonstrations Involving a Federal Interest (April 5, 1976)
 - The Attorney General's Procedures for Lawful, Warrantless Monitoring of Verbal Communications (May 30, 2002) (only portion applicable to FBI)

UNCLASSIFIED//FOUO

11



UNCLASSIFIED//FOUO

DIOG Section 2: General Authorities & Principles

Note: Regarding Extraterritorial FBI's Operations, the AGG-Dom did not repeal or supersede certain portions of the prior guidelines (marked * in prior slides). These national security extraterritorial portions continue to remain in effect pending the approval of new Attorney General's Guidelines for Extraterritorial FBI Operations for both national security and criminal investigations. Additionally, the classified Attorney General Guidelines for Extraterritorial FBI Operations and Criminal Investigations (1993) continue to remain in effect pending approval of the new guidelines.

UNCLASSIFIED//FOUO

12



UNCLASSIFIED//FOUO

DIOG Section 2: General Authorities & Principles

The FBI is authorized to:

- Conduct investigations and collect evidence (criminal and national security) and collect foreign intelligence (AGG-Dom, Part II)
- Provide investigative assistance to federal, state, local, tribal, and foreign agencies (AGG-Dom, Part III) and (DIOG Section 12)
- Collect information necessary for and conduct intelligence analysis & planning (AGG-Dom, Part II & IV) and (DIOG Section 15)
- Retain and share information (AGG-Dom, Part VI) and (DIOG Section 14)

UNCLASSIFIED//FOUO

13



UNCLASSIFIED//FOUO

DIOG Section 2: General Authorities & Principles

The word "Assessment" has two distinct meanings:

- The AGG-Dom authorizes as an investigative activity an "assessment" which requires an authorized purpose and objective as discussed in DIOG Section 5.
- The U.S. intelligence community uses the word "assessment" to describe written intelligence products as discussed in DIOG Section 15.7.B.

UNCLASSIFIED//FOUO

14



UNCLASSIFIED//FOUO

DIOG Section 2: General Authorities & Principles

- **The FBI is an intelligence agency as well as a law enforcement agency**
- **The FBI is authorized to engage in intelligence analysis and planning, using all lawful sources of information:**
 - development of overviews and analysis
 - research and analysis to produce reports and assessments
 - operate intelligence systems that facilitate and support investigations through ongoing compilation and analysis of data and information

UNCLASSIFIED//FOUO

15



UNCLASSIFIED//FOUO

DIOG Section 2: General Authorities & Principles

- **The FBI is the “lead federal agency” in the following areas:**
 - Federal Crimes of Terrorism (listed in DIOG Section 2.4.C)
 - Other non-Terrorism federal crimes (listed in DIOG Section 2.4.D)
 - Counterintelligence and Espionage (listed in DIOG Section 2.4.F)
 - Criminal Investigations (some listed in DIOG Section 2.4.G; see also CID PGs)

UNCLASSIFIED//FOUO

16



UNCLASSIFIED//FOUO

DIOG Section 2: General Authorities & Principles

Departures from the AGG – Dom:

In Advance: FBI Director, Deputy Director, or EAD (NSB or Criminal Cyber Response and Services Branch) must approve with notice to the General Counsel.

In Emergency: Approving authority who authorizes the departure must give notice as soon thereafter as practical to Director, Deputy Director or EAD with notice to General Counsel – OGC must keep records of all departures to advise DOJ, as required.

UNCLASSIFIED//FOUO

17



UNCLASSIFIED//FOUO

DIOG Section 2: General Authorities & Principles

Departures from the DIOG:

In Advance: Appropriate substantive AD or DAD must approve with notice to the General Counsel or appropriate Deputy General Counsel (DGC).

In Emergency: Approving authority who authorizes the departure must give notice as soon thereafter as practical; SAC or HQ Section Chief must provide written notice to appropriate substantive AD and the General Counsel.

UNCLASSIFIED//FOUO

18



UNCLASSIFIED//FOUO

DIOG Section 2: General Authorities & Principles

The AGG-Dom and DIOG apply to all FBI domestic investigations and operations conducted by “FBI employees” – defined as:

- applicable support personnel
- intelligence analysts
- special agents
- task force officers (TFO)
- detailees
- FBI contractors
- confidential human sources (CHS)

UNCLASSIFIED//FOUO

19



UNCLASSIFIED//FOUO

DIOG Section 2: General Authorities & Principles

Authorities of an FBI Special Agent:

1. Investigate violations of the laws, including the criminal drug laws, of the United States (21 U.S.C. § 871; 28 U.S.C. §§ 533, 534 and 535; 28 C.F.R. § 0.85)
2. Collect evidence in cases in which the United States is or may be a party in interest (28 C.F.R. § 0.85 [a]) as redelegated through exercise of the authority contained in 28 C.F.R. § 0.138 to direct personnel in the FBI
3. Make arrests (18 U.S.C. §§ 3052 and 3062)
4. Serve and execute arrest warrants and seize property under warrant; issue and/or serve administrative subpoenas; serve subpoenas issued by other proper authority; and make civil investigative demands (18 U.S.C. §§ 3052, 3107; 21 U.S.C. § 876; 15 U.S.C. § 1312)

UNCLASSIFIED//FOUO

20



UNCLASSIFIED//FOUO

DIOG Section 2: General Authorities & Principles

Authorities of an FBI Special Agent (cont.):

5. Carry firearms (18 U.S.C. § 3052)
6. Administer oaths to witnesses attending to testify or depose in the course of investigations of frauds on or attempts to defraud the United States or irregularities or misconduct of employees or agents of the United States (5 U.S.C. § 303)
7. Seize property subject to seizure under the criminal and civil forfeiture laws of the United States (e.g., 18 U.S.C. §§ 981 and 982)
8. Perform other duties imposed by law

UNCLASSIFIED//FOUO

21



UNCLASSIFIED//FOUO

DIOG Section 2: General Authorities & Principles

The AGG-Dom did not limit other authorized FBI activities, such as:

- Conducting background checks and inquires concerning applicants and employees under federal personnel security programs
- Maintenance and operation of national criminal records systems and preparation of national crime statistics
- Forensic assistance and administration functions of the FBI Laboratory

UNCLASSIFIED//FOUO

22



UNCLASSIFIED//FOUO

DIOG Section 3: FBI's Core Values

The FBI's Core Values are:

- Rigorous obedience to the U.S. Constitution
- Respect for the dignity of all those we protect
- Compassion
- Fairness
- Uncompromising personal integrity and institutional integrity
- Accountability by accepting responsibility for our actions and decisions and their consequences
- Leadership, by example, both personal and professional

UNCLASSIFIED//FOUO

23



UNCLASSIFIED//FOUO

DIOG Section 3: Compliance

Everyone's Responsibility:

- To learn and understand the laws, rules and regulations that govern their activities
- To fully comply with all laws, rules and regulations governing investigations, operations, programs and activities
- To report to proper authority any known or suspected failures to adhere to the law, rules or regulations

UNCLASSIFIED//FOUO

24



UNCLASSIFIED//FOUO

DIOG Section 3: Deputy Director Roles and Responsibilities

DIOG Section 3.2:

- DD is the proponent of the DIOG and subordinate implementing procedural directives and specific policy implementation guides (PGs)
- DD has oversight of DIOG compliance, monitoring and auditing processes
- DD has responsibility for DIOG training
- DD, through the Corporate Policy Office (CPO), will ensure the DIOG is updated one year from implementation, and every three years thereafter

UNCLASSIFIED//FOUO

25



UNCLASSIFIED//FOUO

DIOG Section 3: Special Agent, Intelligence Analyst, Task Force Officer, FBI Contractor, and Others - Roles and Responsibilities

DIOG Section 3.3:

- Comply with AGG-Dom and DIOG standards for initiation, conducting, and closing investigative activity; collection activity; or use of an investigative method
- Obtain training on DIOG standards relevant to their position and perform activities consistent with those standards
- Ensure all investigative activity complies with all laws and policy
- Identify victims, offer FBI assistance, and furnish information to the FBI Victim Specialist

UNCLASSIFIED//FOUO

26



UNCLASSIFIED//FOUO

DIOG Section 3: Special Agent, Intelligence Analyst, Task Force Officer, FBI Contractor, and Others - Roles and Responsibilities

(Continued – DIOG Section 3.3)

- Ensure civil liberties and privacy are protected throughout the assessment or investigative process
- Conduct no investigative activity solely on the basis of activities protected by the 1st Amendment or solely on the basis of race, ethnicity, national origin or religion of the subject
- Report non-compliance to the proper authority

UNCLASSIFIED//FOUO

27



UNCLASSIFIED//FOUO

DIOG Section 3: Supervisor Roles and Responsibilities

DIOG Section 3.4.A – Supervisor Defined:

- Field Office or FBIHQ personnel, including: SIA, SSA, SSRA, UC, ASAC, ASC, SAC, DAD, AD, ADIC, and EAD

UNCLASSIFIED//FOUO

28



UNCLASSIFIED//FOUO

DIOG Section 3: Supervisor Roles and Responsibilities

DIOG Section 3.4.B - Supervisor Responsibilities:

- Determine whether the DIOG standards are satisfied for initiating, approving, conducting and closing an investigative activity, collection activity, or investigative method
- Ensure all investigative activity complies with all laws and policy
- Obtain training on DIOG standards relevant to their position and conform their decisions to those standards
- Ensure civil liberties and privacy are protected throughout the assessment or investigative process

UNCLASSIFIED//FOUO

29



UNCLASSIFIED//FOUO

DIOG Section 3: Supervisor Roles and Responsibilities

Continued DIOG Section 3.4.B - Supervisor Responsibilities:

- If encountering a practice that does not comply with the law, rules, or regulations, the supervisor must:
 - 1. report that compliance concern to the proper authority
 - 2. take action to maintain compliance, when necessary
- Ensure no retaliation or adverse action is taken against persons who raise compliance concerns

UNCLASSIFIED//FOUO

30



UNCLASSIFIED//FOUO

DIOG Section 3: Supervisor Roles and Responsibilities

DIOG Section 3.4.C - Supervisory Delegation:

- Any DIOG requirement imposed on a Supervisor may be delegated/performed by a designated Acting, Primary, or Secondary Relief supervisor as indicated below, unless specified otherwise by federal statute, EO, PD, AGG, FBI Policy or any other regulation.
 - Supervisor may delegate authority to a supervisor one level junior to himself/herself (e.g. SAC to ASAC; or SC to Assistant/SC)
 - Must identify the task delegated
 - Must identify the supervisory position given approval authority
 - Must be in writing
 - Must be retained appropriately
 - Higher level Supervisors in the same chain-of-command as the original supervisor may approve a particular activity without written delegation documentation

UNCLASSIFIED//FOUO

31



UNCLASSIFIED//FOUO

DIOG Section 3: Supervisor Roles and Responsibilities

DIOG Section 3.4.D - Investigative File Reviews:

- Conducted by full-time supervisors or primary relief supervisors with subordinates
 - (other relief supervisors must have written SAC authority to conduct)
- Conducted with all Agents, Resident Agents, TFOs, analysts, detailees, and FBI contractors, as appropriate
- Conducted in-person or by telephone when necessary
- Conducted in private
- Documented/noted on ACS ICMC report, FD-71 or Guardian
- Conducted at least every 60 days for Probationary Agents, recommended every 30 days

UNCLASSIFIED//FOUO

32



UNCLASSIFIED//FOUO

DIOG Section 3: Supervisor Roles and Responsibilities

Assessment Justification/File Reviews:

- Conducted for every 30 day period for Type 1 and 2 Assessments
 - (with 10 additional days to complete and document)
- Conducted for every 90 day period for Type 3, 4, and 6 Assessments
 - (with 30 additional days to complete and document)
- Supervisor Must:
 - Evaluate progress made toward the achievement of authorized purpose and objective
 - Ensure activities that occurred during prior period were appropriate
 - Determine whether it is reasonably likely that information may be obtained that is relevant to the authorized objective – thus warranting an extension for another 30/90 day period
 - Determine whether adequate predication has been developed to open a predicated investigation
 - Determine whether the assessment should be terminated

UNCLASSIFIED//FOUO

33



UNCLASSIFIED//FOUO

DIOG Section 3: Supervisor Roles and Responsibilities

Predicated (Preliminary and Full) Investigation File Reviews:

- Conducted for every 90 day period
 - (with 30 additional days to complete and document)
- Supervisor Must:
 - Evaluate progress made toward the achievement of authorized purpose and objective
 - Ensure activities that occurred during prior period were appropriate
 - Determine whether it is reasonably likely that information may be obtained that is relevant to the authorized objective – thus warranting an extension for another 90 day period
 - Determine whether adequate predication has been developed to open/or continues to justify a predicated investigation

UNCLASSIFIED//FOUO

34



UNCLASSIFIED//FOUO

DIOG Section 3: Unaddressed Work

-
-
-
-

Note: the FD-71 provides a new mechanism to assign an Assessment to an electronic Unaddressed Work File in the appropriate classification

b2
b7E

UNCLASSIFIED//FOUO

35



UNCLASSIFIED//FOUO

DIOG Section 3: CDC's Role and Responsibilities

CDC's Role and Responsibilities:

1. Must review all Assessments, Preliminary Investigations (PI) and Full Investigations (FI) that involve a "Sensitive Investigative Matter" (SIM)
2. Must review particular investigative methods as mandated by DIOG Section 5 and 11
3. Requirements imposed on the CDC may be performed by an Associate Division Counsel, Legal Advisor, or designated Acting CDC. All delegations must be in writing and retained appropriately.

UNCLASSIFIED//FOUO

36



UNCLASSIFIED//FOUO

DIOG Section 3: CDC Roles and Responsibilities

CDC Determinations:

The primary purpose of the CDC's review is to ensure the legality of the actions proposed. In this context, the review includes a determination that the:

- Investigative activity is not legally objectionable (can be overruled by OGC)
 - Activity is not based solely on the exercise of 1st Amendment rights or on the race, ethnicity, national origin or religion of the subject
- The investigation is founded upon an "authorized purpose" (Assessments) or have adequate factual predication (Preliminary and Full)
- Advise as to the "wisdom" of the proposed action

UNCLASSIFIED//FOUO

37



UNCLASSIFIED//FOUO

DIOG Section 3: CDC Roles and Responsibilities

Continued: CDC Determinations

The CDC's determination is based on facts known at the time of the review and recommendation.

The CDC may require additional reviews or provide guidance as to monitoring the results of investigative activity to ensure that the authorized purpose and/or factual predication remain intact after additional facts are developed.

UNCLASSIFIED//FOUO

38



UNCLASSIFIED//FOUO

DIOG Section 3: OGC Roles and Responsibilities

OGC Role: In coordination with the DOJ NSD, the OGC is responsible for conducting regular reviews of all aspects of FBI national security and foreign intelligence activities.

The primary purpose of the OGC's review is to ensure the legality of the actions proposed. These reviews, conducted in the field offices and in HQ Units, broadly examine such activities for compliance with the AGG-Dom and other requirements. In this context, the review includes a determination that the:

- Investigative activity is not legally objectionable (Activity is not based solely on the exercise of 1st Amendment rights or on the race, ethnicity, national origin or religion of the subject)
- The investigation is founded upon an "authorized purpose" (Assessments) or have adequate factual predication (Preliminary and Full) and meets the standards in the DIOG
- Advise as to the "wisdom" of the proposed action

UNCLASSIFIED//FOUO

39



UNCLASSIFIED//FOUO

DIOG Section 3: OGC Roles and Responsibilities

Continued: OGC Determinations

- The OGC's determination above is based on facts known at the time of the review and recommendation.
- The OGC may require additional reviews or provide guidance as to monitoring the results of investigative activity to ensure that the authorized purpose and/or factual predication remain in tact after facts are developed

UNCLASSIFIED//FOUO

40



UNCLASSIFIED//FOUO

DIOG Section 3: Other Roles and Responsibilities

CPO = Corporate Policy Office: Oversight and Implementation of the DIOG; Report compliance risks to OIC (DIOG Section 3.7)

OIC = Office of Integrity and Compliance: Identify compliance risk areas, adequacy of policy and training programs, monitor DIOG compliance (DIOG Section 3.8)

DCO = Division Compliance Officer: One identified in each Field Office to assist the OIC to identify potential non-compliance risk areas and report them to proper authority and OIC (DIOG Section 3.10)

PM = Program Manager: HQ entity that identifies, prioritizes, and analyzes compliance risks and takes appropriate corrective action (DIOG Section 3.9)

UNCLASSIFIED//FOUO

41



UNCLASSIFIED//FOUO

DIOG Section 4: Privacy and Civil Liberties, and Least Intrusive Methods

- Responsibility to protect the American public, not only from crime and terrorism, but also from incursions into their constitutional rights; accordingly, all investigative activities must fully adhere to the Constitution and the principles of civil liberty and privacy.
- Provisions of the AGG-Dom, other AG guidelines, and oversight from DOJ components, are designed to ensure FBI's activities are lawful, appropriate, and ethical, as well as effective in protecting civil liberties and privacy.
- DOJ and FBI's Inspection Division, Office of Integrity and Compliance, the OGC, other Bureau components, and **you** share responsibility for ensuring the FBI meets these goals.

UNCLASSIFIED//FOUO

42



UNCLASSIFIED//FOUO

DIOG Section 4: Privacy and Civil Liberties, and Least Intrusive Methods

- No investigation or assessment can be commenced based solely on race, ethnicity, national origin, religion of the subject or the exercise of First Amendment rights.
- Corollary to this AGG requirement is the Privacy Act, which states that each agency that maintains a system of records shall "maintain no record describing how any individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute or by the individual about whom the record is maintained or **unless pertinent to and within the scope of an authorized law enforcement activity.** 5 U.S.C. 552a(e)(7).

UNCLASSIFIED//FOUO

43



UNCLASSIFIED//FOUO

DIOG Section 4 Scenario

-
- What can you do with this information?
-
-
-

b2
b7E

UNCLASSIFIED//FOUO

44



UNCLASSIFIED//FOUO

DIOG Section 4 Scenario

-
-

b2
b7E

UNCLASSIFIED//FOUO

45



UNCLASSIFIED//FOUO

DIOG Section 4: Privacy and Civil Liberties, and Least Intrusive Methods

FIRST AMENDMENT RIGHTS:

Individuals or groups who communicate with each other or with members of the public in any form in pursuit of social or political causes—such as opposing war or foreign policy, protesting government actions, promoting certain religious beliefs, championing particular local, national, or international causes, or a change in government through non-criminal means, and actively recruit others to join their causes—have a fundamental constitutional right to do so. An assessment may not be initiated based solely on the exercise of these First Amendment rights. If, however, a group exercising its First Amendment rights also threatens or advocates violence or destruction of property, an assessment would be appropriate

UNCLASSIFIED//FOUO

46



UNCLASSIFIED//FOUO

DIOG Section 4: Privacy and Civil Liberties, and Least Intrusive Methods

FIRST AMENDMENT RIGHTS (cont.):

- No investigative activity, including assessments, may be taken solely on the basis of activities that are protected by the First Amendment or on the race, ethnicity, national origin or religion of the subject.
- If an assessment or predicated investigation touches on or is partially motivated by First Amendment activities, race, ethnicity, national origin or religion, it is particularly important to identify and document the basis for the assessment with clarity

UNCLASSIFIED//FOUO

47



UNCLASSIFIED//FOUO

DIOG Section 4: Privacy and Civil Liberties, and Least Intrusive Methods

All activities must be consistent with the Attorney General's 2003 Guidance Regarding the Use of Race by Federal Law Enforcement Agencies (forbids the use of racial profiling and requires activities involving the investigation or prevention of threats to the national security to comply with the Constitution and laws of the United States)

The DIOG stresses several points in each section:

- No investigation or assessment can be commenced based solely on race, ethnicity, national origin, religion, or exercise of First Amendment rights
- The FBI must use the least intrusive method that is feasible under the circumstances
- In connection with Foreign Intelligence collection, agents must operate openly and consensually with U.S. Persons, to the extent practicable
- All investigative activities must have an "authorized purpose"

UNCLASSIFIED//FOUO

48



UNCLASSIFIED//FOUO

DIOG Section 4: Use of Race or Ethnicity

DIOG Guidance on use of Race or Ethnicity

As to individuals:

1. Permits the consideration of ethnic and racial identity information based on specific reporting;
2. The race or ethnicity of suspected members, associates, or supporters of an ethnic-based gang or criminal enterprise may be collected when gathering information about or investigating the organization; or
3. Ethnicity may be considered in evaluating whether a subject is—or is not—a possible associate of a criminal or terrorist group that is known to be comprised of members of the same ethnic grouping—as long as it is not the dominant factor for focusing on a particular person

UNCLASSIFIED//FOUO

49



UNCLASSIFIED//FOUO

DIOG Section 4: Use of Race or Ethnicity

DIOG Guidance on use of Race or Ethnicity

As to a community:

1. Collecting and analyzing demographics – if these locations will reasonably aid the analysis of potential threats and vulnerabilities, and, overall, assist domain awareness
2. Geo-Mapping ethnic/racial demographics – if properly collected
3. General ethnic/racial behavior – cannot be collected, unless it bears a rational relationship to a valid investigative or analytical need
4. Specific and relevant ethnic behavior
5. Exploitive ethnic behavior – by criminal or terrorist groups

UNCLASSIFIED//FOUO

50



UNCLASSIFIED//FOUO

DIOG Section 4: Least Intrusive Investigative Method

The AGG-DOM and the DIOG require that the “least intrusive” means or method be considered and, if operationally sound and effective, used to obtain intelligence or evidence in lieu of a more intrusive method

UNCLASSIFIED//FOUO

51



UNCLASSIFIED//FOUO

DIOG Section 4: Privacy and Civil Liberties, and Least Intrusive Methods

By emphasizing the use of less intrusive means, employees will be able to balance:

Our need for evidence/intelligence

vs.

Mitigating potential negative impact on the privacy and civil liberties of people/public

UNCLASSIFIED//FOUO

52



UNCLASSIFIED//FOUO

DIOG Section 4: Privacy and Civil Liberties, and Least Intrusive Methods

Primary factor in determining “intrusiveness”:

- The degree of procedural protection that the law and the AGG-DOM provide for the use of the particular method.
 - Examples of “more intrusive” methods: Search Warrants, wiretaps, UCOs
 - Examples of “less intrusive” methods: checks of government databases, state or local criminal record checks, commercial databases, interviews

UNCLASSIFIED//FOUO

53



UNCLASSIFIED//FOUO

DIOG Section 4: Privacy and Civil Liberties, and Least Intrusive Methods

Items to consider when determining the relative intrusiveness of an investigative method:

- Is method permitted prior to the initiation of an assessment?
- Is the method relevant to the assessment or investigation?
- Will the information collected or obtained likely further the investigative objective?
- What alternatives exist for gathering the same information?
- Are those alternatives relatively less intrusive?
- What time span is involved in using the investigative method (days, weeks, months)?
- What confidence level is associated with the information gathered using the investigative method?
- Will the method resolve a pending investigative issue quickly?

UNCLASSIFIED//FOUO

54



UNCLASSIFIED//FOUO

DIOG Section 4: Least Intrusive Investigative Method

Factors to Determine "Intrusiveness":

1. Nature of the information sought
2. Scope of the information sought
3. Scope of the use of the investigative method
4. Source of the information sought
5. Risk of public exposure

UNCLASSIFIED//FOUO

55



UNCLASSIFIED//FOUO

As of February 20, 2009

DIOG Section 5 & 11: Investigative Methods

Authorized Methods for Assessments and Restricted Investigations

○ indicates methods used under a particular operational activity; □ indicates methods allowed.

	Assessments	Preliminary Investigations	Full Investigations
Obtain publicly available information	○	○	○
Access and examine FBI and other DOJ records, and obtain information from any FBI or DOJ personnel	○	○	○
Access and examine records maintained by, and request information from, other federal, state, local, tribal, or foreign governmental entities or agencies	○	○	○
Use online services and resources (whether nonprofit or commercial)	○	○	○
Use and recruit human sources in conformity with AG Guidelines Regarding the Use of FBI Confidential Human Sources	○	○	○
Interview or request information from members of the public and private entities [includes pretextual interviews]	○	○	○
Accept information voluntarily provided by governmental or private entities	○	○	○
Engage in observation or surveillance not requiring a court order	○	○	○
Mail covers	○	○	○
Physical searches of personal or real property where a warrant or court order is not legally required because there is no reasonable expectation of privacy (e.g., trash covers)	○	○	○
Consensual monitoring of communications, including consensual computer monitoring, is subject to legal review by the CDC or the FBI OGC. Where a sensitive monitoring circumstance is involved, monitoring must be approved by the Criminal Division or, if the investigation concerns foreign intelligence or a threat to the national security, by the National Security Division	○	○	○
Use of closed-circuit television, direction finders, and other monitoring devices, subject to legal review by the CDC or FBI OGC	○	○	○
Polygraph examinations	○	○	○
Undercover operations	○	○	○
Compulsory process as authorized by law, including Federal Grand Jury and other subpoenas and National Security Letters (Federal Grand Jury subpoenas for telephone and electronic mail subscriber records can be used during type 1 and 2 Assessments only)	○	○	○
Accessing stored wire and electronic communications and transactional records	○	○	○
Use of pen registers and trap and trace devices	○	○	○
Electronic surveillance	○	○	○
Foreign intelligence collection under Title VII of FISA	○	○	○
Physical searches, including mail openings, where a warrant or court order is legally required because there is an expectation of privacy	○	○	○



UNCLASSIFIED//FOUO

Investigative Methods/Approvals Chart

Authorized Method and DIOG Reference*		Approval Levels for Assessments and Predicated Investigations		
		Assessments	Predicated	Foreign Intelligence
1	5.8A Obtain publicly available information	None Required	None Required	None Required
	Taskforce a DICE to attend a religious service	Not Permitted	SSA Approval	SSA Approval
2	5.8B Physical surveillance of a person or group (Consult the DIOG for handheld photo and video surveillance with no reasonable expectation of privacy)	None Required	None Required	None Required
		Consult DIOG for requirements	None Required	None Required
		ASAC Approval	ASAC Approval	ASAC Approval
3	5.8C Access and examine FBI and other Department of Justice (DOJ) records, and obtain information from any FBI or other DOJ personnel	None Required	None Required	None Required
4	5.8D Access and examine records maintained by, and request information from, other federal, state, local, or tribal, or foreign governmental entities or agencies	None (Unless such approval is required by MOU or other agreements)	None (Unless such approval is required by MOU or other agreements)	None (Unless such approval is required by MOU or other agreements)
5	5.8E Use online services and resources (whether nonprofit or commercial)	None Required	None Required	None Required
6	5.8F Interview or request information from members of the public and private entities	None Required except for contact with represented persons, members of U.S. Congress, or their staffs, White House personnel, or other substantive division requirements	None Required except for contact with represented persons, members of U.S. Congress, or their staffs, White House personnel, or other substantive division requirements	None Required except for contact with represented persons, members of U.S. Congress, or their staffs, White House personnel, or other substantive division requirements
7	5.8G Accept information voluntarily provided by governmental or private entities	None Required	None Required	None Required
8	5.8H Use and recruit human sources	None Required (utilize [redacted])	None Required (utilize Delta)	None Required (utilize Delta)
	Taskforce a CHS to attend a religious service	SAC Approval	SSA Approval	SSA Approval
9	5.8I Federal Grand Jury subpoenas for telephone or electronic mail subscriber information	US Attorney Office Approval (Type 1 and 2 Assessments Only)	US Attorney Office Approval	Not Permitted
10	5.8C Pattern Based Data Mining	SORC	SORC	SORC

b2
b7E

UNCLASSIFIED//FOUO

As of May 19, 2009

57



UNCLASSIFIED//FOUO

Investigative Methods/Approvals Chart

Authorized Method and DIOG Reference*		Approval Levels for Assessments and Predicated Investigations		
		Assessments	Predicated	Foreign Intelligence
11	11.3 Mail covers	[redacted]	[redacted]	[redacted]
12	11.4 Physical searches of personal or real property where a warrant or court order is not legally required because there is no reasonable expectation of privacy (e.g.)	[redacted]	[redacted]	[redacted]
13	11.5 Consensual monitoring of communications, including consensual computer monitoring	Not Permitted	CDC or OGC Review SSA Approval	CDC or OGC Review SSA Approval
14	11.5 Consensual monitoring of communications, including consensual computer monitoring, with a sensitive monitoring circumstance	Not Permitted	CDC or OGC Review, SAC Approval, DOJ Criminal or DOJ NSD Approval	CDC or OGC Review, SAC Approval, DOJ Criminal or DOJ NSD Approval
15	11.6 Use of closed-circuit television, direction finders, and other monitoring devices	[redacted]	[redacted]	[redacted]
16	11.7 Polygraph examinations	Not Permitted	SSA Approval	SSA Approval
17	11.8 Undercover operations, Group II	[redacted]	CDC Review, SAC or ASAC with delegated authority, National Security cases also require NSD consent (US/IS)	CDC Review, SAC or ASAC with delegated authority, NSB-UNH/UNCB Approval
18	11.8 Undercover operations, Group I	Not Permitted	CDC review, SAC and AD and UICRG or UICRG (EAD/DO certain cases) Approval	CDC review, SAC and AD and UICRG (EAD/DO certain cases) Approval
19	11.9 Computer process as authorized by law, Federal Grand Jury and trial subpoenas	[redacted]	US Attorney's Office Approval	[redacted]
20	11.9 Administrative Subpoenas: Drugs	Not Permitted	SAC, ASAC, SSRA, or Drug Squad SSA	Not Permitted
	11.9 Administrative Subpoenas: Sexual Exploitation		[redacted]	
	11.9 Administrative Subpoenas: Medicare Fraud		U.S. Attorney's Office Approval	
21	11.9 National Security Letters	Not Permitted	Field Office: CDC Review, ADIC or SAC Approval; HQ: NSLB Review, DD or EAD-NSB or AD & DADs CT/ADIC/D or GC or Deputy GC-NSLB Approval	Not Permitted
22	11.10 Accessing stored wire and electronic communications and transactional records	Not Permitted	Statute/Court Order, Consult DIOG	Not Permitted
23	11.11 Use of pen registers and trap and trace devices	Not Permitted	FISA Court or District Court Order	Only Available for Non-US/IS by FISA Court order
24	11.12 Electronic surveillance	Not Permitted	[redacted]	[redacted]
25	11.13 Physical searches, where there is reasonable expectation of privacy, including mail openings	[redacted]	[redacted]	[redacted]
26	11.14 Acquisition of foreign intelligence information in conformity with Title VIII of the Foreign Intelligence Surveillance Act	[redacted]	FISA Court Order Permitted in Full Investigations Only	FISA Court order

b2
b7E

UNCLASSIFIED//FOUO

As of May 19, 2009

58



**Directorate of Intelligence
Geospatial Intelligence Unit (GIU)**

Reference Sheet for the Domestic Investigations and Operations Guide (DIOG)

This document provides a listing of particular references to Geospatial Intelligence (GEOINT) and related matters in the DIOG.¹ It is **not** a replacement for reading all relevant portions of the DIOG, nor is it legal advice. Any reader is strongly encouraged to review and comply with the DIOG in its entirety.² All legal questions regarding the content of the DIOG should be referred to the FBI Office of General Counsel (OGC) or Chief Division Counsel (CDC).

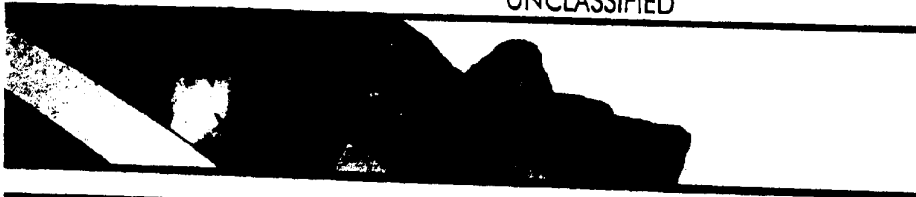
Subject	Reference
1. Mapping ethnic/racial demographics	4.3 C. 2. b.
2. FBI employee may produce GEOINT	5.1
3. [REDACTED]	5.2 A.
4. [REDACTED]	5.6 A. 4.
5. [REDACTED]	11.10.3 B. 6.
6. [REDACTED]	11.10.3 B. 6. d.
7. Systematically assessing particular geographic areas or sectors	15.2 B. 1.
8. Analysis and Planning not Requiring the Initiation of an AGG-DOM Part II Assessment	15.2 C.
9. Domain Management by Field Offices	15.7 A. 1.
10. Written Intelligence Products	15.7 B.
11. United States Person (USPER) Information	15.7 B.
12. FBI authorized to operate Intelligence Systems	15.7 C.
13. Definition of Geospatial Intelligence (GEOINT)	15.7 D.
14. GEOINT Acronym	Appendix F-3

b2
b7E

¹ [Link to the DIOG Table of Contents \(TOC\)](#). This link will take you to the DIOG Table of Contents on the FBI Corporate Policy Office Policy & Guidance Web.

² The FBI has a long-established commitment to Privacy and Civil Liberties. The DIOG Section 4. Privacy and Civil Liberties, and Least Intrusive Methods must be followed.

UNCLASSIFIED



The State of the NSB



(U) The State of the NSB

EAD-NSB Arthur M. Cummings II

(U) In early August, I had the opportunity to meet with employees from the Baltimore, Norfolk, Richmond, and Washington field offices who were at Headquarters for the second major phase of Strategic Execution Team training. Among the things I told these analysts and agents – who were the first to go through the initial SET rollout back in April – is how pleased I am about the pace at which the intelligence operations of the Bureau are changing in response to SET guidelines

and recommendations.

(U) As we continue to build capacity and roll out SET, it is incumbent on us to ensure we have policies in place to guide these enhanced capabilities. Now that we are almost a third of the way through rolling out the new intelligence operations structure and functions to the field offices, I want to address some questions that have arisen about domain management activities within field offices, particularly domain mapping.

(U) The basic concept of domain management is simple: We need to develop a comprehensive understanding of the threats and vulnerabilities in each territory, so we can effectively deploy resources to support strategies that counter those threats. While we are still fine-tuning the policy that governs appropriate intelligence collection and domain mapping, field offices are collecting intelligence to understand their domain and address emerging threats.

“... you need to draw on intelligence requirements to articulate what the threat is before you start mapping it.”

(U) In doing so, the most important thing to keep in mind is collection must always start with a threat. The new Attorney General Guidelines

that are expected to be signed next month give us the authority collect intelligence outside of predicated cases. But in undertaking this collection, we must have an indication of a threat.

(U) Put another way, you need to draw on intelligence requirements to articulate what the threat is before you start mapping it.

(U) I envision appropriate collection and mapping in five steps: intelligence, analysis, analytic judgments, requirements, and operations. New intelligence comes in that indicates there is a threat. That intelligence is analyzed, and judgments are made about the threat to U.S. national security. Then we distill the intelligence down to collection requirements and start collecting.

(U) As a hypothetical example,

[Redacted]

(U)

[Redacted]

What's the first step? We take the initial intelligence, and analyze it. Then we start making some judgments about it. Is it credible? Is there a threat to our national security?

In This Issue:

Page One

The State of the NSB

On This Date

This Month's Hot Topic: New Law Codifies FBI Information Sharing Initiatives

NSB News

Resources

NSB Q&A

NSB Memo Survey

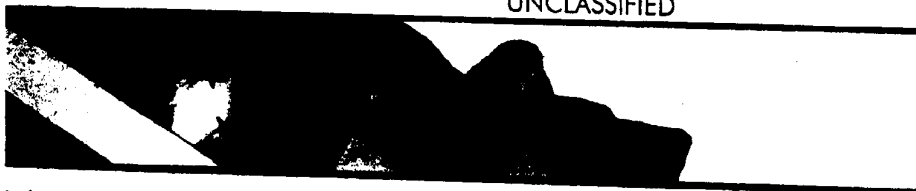
Archives

Contact Us

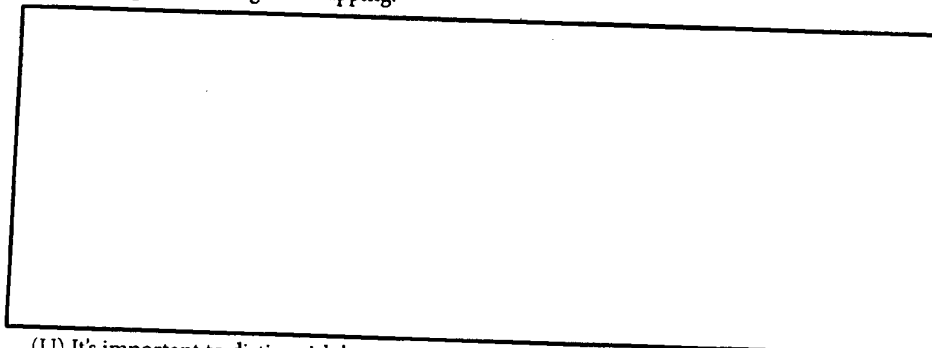
b2
b7E

Top of Page ▲

Next Page ►



What is the nature and scope of the threat? What is the extent of the presence in the United States? We'll distill those judgments into collection requirements, and send those out to the field to begin collecting and mapping.



(U) It's important to distinguish between mapping of a specific demographic within a community, and mapping the population in general. To understand your domain, you can map an entire set of demographics across all lines to better understand your constituency. We want field offices to know what's in their territory. But if you want to map just a specific category in the city's population, you need to do it because intelligence indicates the threat can be found from within a defined demographic. Once again, the key is in the ability to articulate the intelligence and analytic judgments that meet a reasonableness standard for non-predicated collection.

(U) We simply cannot afford to be seen as biased or arbitrary in our collection. Never forget that it is our responsibility to uphold and protect the civil rights of the American people. Carrying out our mission in large part depends on our ability to maintain the trust the American people have placed in us. If we always start with a threat, and match it with appropriate collection requirements, we can confidently do our job of protecting the American people and their liberties.

In This Issue:

Page One

The State of the NSB

On This Date

This Month's Hot Topic: New Law Codifies FBI Information Sharing Initiatives

NSB News

Resources

NSB Q&A

NSB Memo Survey

Archives

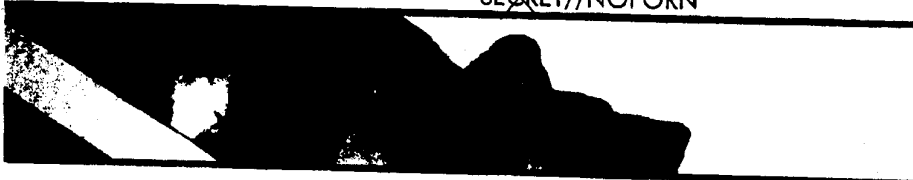
Contact Us

b2
b7E

Top of Page ▲

Aug 2008

~~SECRET~~//NOFORN



The State of the NSB



(U) The State of the NSB

EAD-NSB Arthur M. Cummings II

(U) In early August, I had the opportunity to meet with employees from the Baltimore, Norfolk, Richmond, and Washington field offices who were at Headquarters for the second major phase of Strategic Execution Team training. Among the things I told these analysts and agents – who were the first to go through the initial SET rollout back in April – is how pleased I am about the pace at which the intelligence operations of the Bureau are changing in response to SET guidelines

and recommendations.

(U) As we continue to build capacity and roll out SET, it is incumbent on us to ensure we have policies in place to guide these enhanced capabilities. Now that we are almost a third of the way through rolling out the new intelligence operations structure and functions to the field offices, I want to address some questions that have arisen about domain management activities within field offices, particularly domain mapping.

(U) The basic concept of domain management is simple: We need to develop a comprehensive understanding of the threats and vulnerabilities in each territory, so we can effectively deploy resources to support strategies that counter those threats. While we are still fine-tuning the policy that governs appropriate intelligence collection and domain mapping, field offices are collecting intelligence to understand their domain and address emerging threats.

“... you need to draw on intelligence requirements to articulate what the threat is before you start mapping it.”

that are expected to be signed next month give us the authority collect intelligence outside of predicated cases. But in undertaking this collection, we must have an indication of a threat.

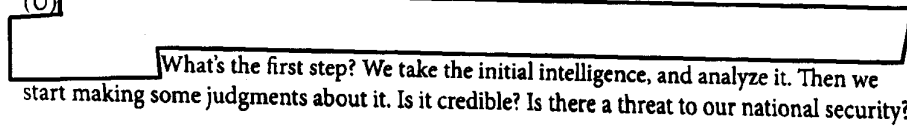
(U) Put another way, you need to draw on intelligence requirements to articulate what the threat is before you start mapping it.

(U) I envision appropriate collection and mapping in five steps: intelligence, analysis, analytic judgments, requirements, and operations. New intelligence comes in that indicates there is a threat. That intelligence is analyzed, and judgments are made about the threat to U.S. national security. Then we distill the intelligence down to collection requirements and start collecting.

(U) As a hypothetical example,



(U)



What's the first step? We take the initial intelligence, and analyze it. Then we start making some judgments about it. Is it credible? Is there a threat to our national security?

In This Issue:

Page One

The State of the NSB

On This Date

This Month's Hot Topic: New Law Codifies FBI Information Sharing Initiatives

NSB News

Resources

NSB Q&A

NSB Memo Survey

Archives

Contact Us

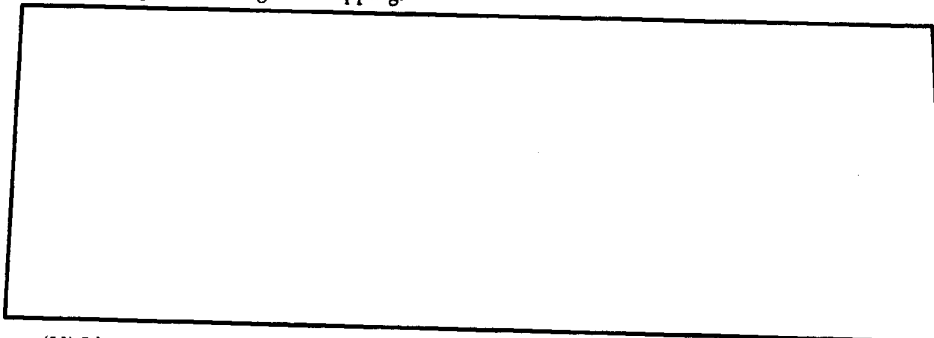
b2
b7E

Top of Page ▲

Next Page ►



What is the nature and scope of the threat? What is the extent of the presence in the United States? We'll distill those judgments into collection requirements, and send those out to the field to begin collecting and mapping.

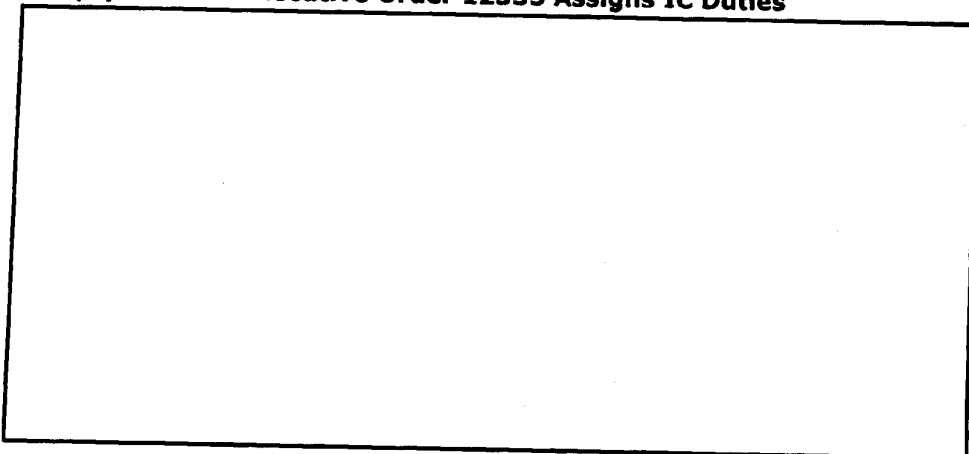


(U) It's important to distinguish between mapping of a specific demographic within a community, and mapping the population in general. To understand your domain, you can map an entire set of demographics across all lines to better understand your constituency. We want field offices to know what's in their territory. But if you want to map just a specific category in the city's population, you need to do it because intelligence indicates the threat can be found from within a defined demographic. Once again, the key is in the ability to articulate the intelligence and analytic judgments that meet a reasonableness standard for non-predicated collection.

(U) We simply cannot afford to be seen as biased or arbitrary in our collection. Never forget that it is our responsibility to uphold and protect the civil rights of the American people. Carrying out our mission in large part depends on our ability to maintain the trust the American people have placed in us. If we always start with a threat, and match it with appropriate collection requirements, we can confidently do our job of protecting the American people and their liberties.

This Month's Hot Topic

(U) Revised Executive Order 12333 Assigns IC Duties



In This Issue:

Page One

The State of the NSB

On This Date

This Month's Hot Topic: New Law Codifies FBI Information Sharing Initiatives

NSB News

Resources

NSB Q&A

NSB Memo Survey

Archives

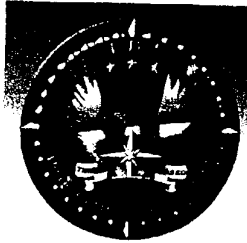
Contact Us

b2
b7E

Outside the Scope of Request

Top of Page ▲

Next Page ►



DIRECTORATE OF INTELLIGENCE



Geospatial Intelligence Unit

What We Do



Geospatial Intelligence Unit (GIU) Directorate of Intelligence



GIU Areas of Focus

- Executive Production
- GEOINT Analysis
- Standards, Policy & Administration
- Data Identification & Systems
- Training & Development
- Operational Support



Executive Production



FBIHQ Executive Management

- **Director's Office**
 - Director's Travel Book
 - Presidential Daily Brief
 - Director's Strategic Briefing
 - SAC Conference
 - AEAD Mullen Targeting Brief
 - **Brief to Undersecretary of Defense for Intelligence (USDI)**
 - 07/29/2009
 - **Briefings to AD's Favreau & Reinhold**
 - **Investment Management Board (IMB)**
-



GEOINT Analysis



- Primary center of GEOINT analysis and product creation
- Leverage internal and external data sets to continuously create GEOINT products based on FBI priorities. Threats, vulnerabilities and gaps will be analyzed visually.
- Close work and support to Executive Production
- Develop relevant tradecraft, techniques, etc. for GEOINT in the FBI
- Identify geospatial relationships of significance
- Use GEOINT to better understand threats and vulnerabilities to inform investigations, analysis and resource allocations



GEOINT Analysis (cont.)



- Provide access to National Level Data sets for national threats and vulnerabilities
- Provide access to National Level Data sets for Strategic and Tactical Analysis
- Tactical Analysis for priority investigations
- GEOINT Analysis for FBIHQ Units
- Imagery....



GEOINT methodology



Define/visualize the Domain

Foundational datasets (boundaries, topography, demographics, etc.)

Describe/visualize threats and vulnerabilities within the Domain

Use available data to show specific activities, events, and areas of interest

Analyze/evaluate threats and vulnerabilities within the Domain

Regression Analysis, Data Modeling, Predictive Analysis

Develop analytical conclusions to support Domain Management

Threat Prioritization, Vulnerability Awareness, Resource Allocation



Standards, Policy & Administration



- Develop and implement standards within the FBI for GEOINT products
- Quality control on FBI GEOINT products.
- Legal and regulatory matters for GEOINT in the FBI
- Close coordination with the FBI Office of General Counsel (OGC)
- Develop and Implement Imagery Policy for the FBI

CLASSIFICATION

FOI See

Map Title
Map Sub-Title
Legend

File Number
Date Stamp

Date Generated

Map Date
Project/Project Segment
Created by
File Date (Created)

Text Box

Page 1 of 1
Scale 1:100,000

Directorate of Intelligence
Geospatial Intelligence Unit (GIU)

Reference Sheet for the Domestic Investigations and Operations Guide (DIOG)

This document provides a listing of particular references to Geospatial Intelligence (GEOINT) and related matters in the DIOG.¹ It is not a replacement for reading all relevant portions of the DIOG, nor is it legal advice. Any reader is strongly encouraged to review and comply with the DIOG in its entirety.² All legal questions regarding the content of the DIOG should be referred to the FBI Office of General Counsel (OGC) or Chief Division Counsel (CDC).

Subject	Reference
1. Mapping ethnolinguistic demographics	4.2 C. 2. b.
2. FBI employes may produce GEOINT	5.1
3. [REDACTED]	5.2 A.
4. [REDACTED]	5.6 A. 4.
5. [REDACTED]	11.10.3 B. 6.
6. [REDACTED]	11.10.3 B. 6. d.
7. Systematically assessing particular geographic areas or sectors	15.2 B. 1.
8. Analysis and Planning not Requiring the Inclusion of an AGO/COM/Ext. II Assessment	15.2 C.
9. Domain Management by Field Offices	15.7 A. 1.
10. Written Intelligence Products	15.7 E.
11. United States Person (USPER) Information	15.7 E.
12. FBI authorized to operate Intelligence Systems	15.7 C.
13. Definition of Geospatial Intelligence (GEOINT)	15.7 D.
14. GEOINT Acronym	Appendix P-3

¹ Link to the [DIOG Table of Contents \(TOC\)](#). This link will take you to the DIOG Table of Contents on the FBI Corporate Policy Office Policy & Guidance Web.

² The FBI has a long established commitment to Privacy and Civil Liberties. The DIOG, Section 1, Privacy and Civil Liberties, and Law Enforcement Methods must be followed.

b2
b7E



Data Identification & Systems



- Expertise and zealous advocacy for the development of IT hardware and software solutions that match user requirements for GEOINT in the FBI
- SSA presentation to follow

b6
b7c

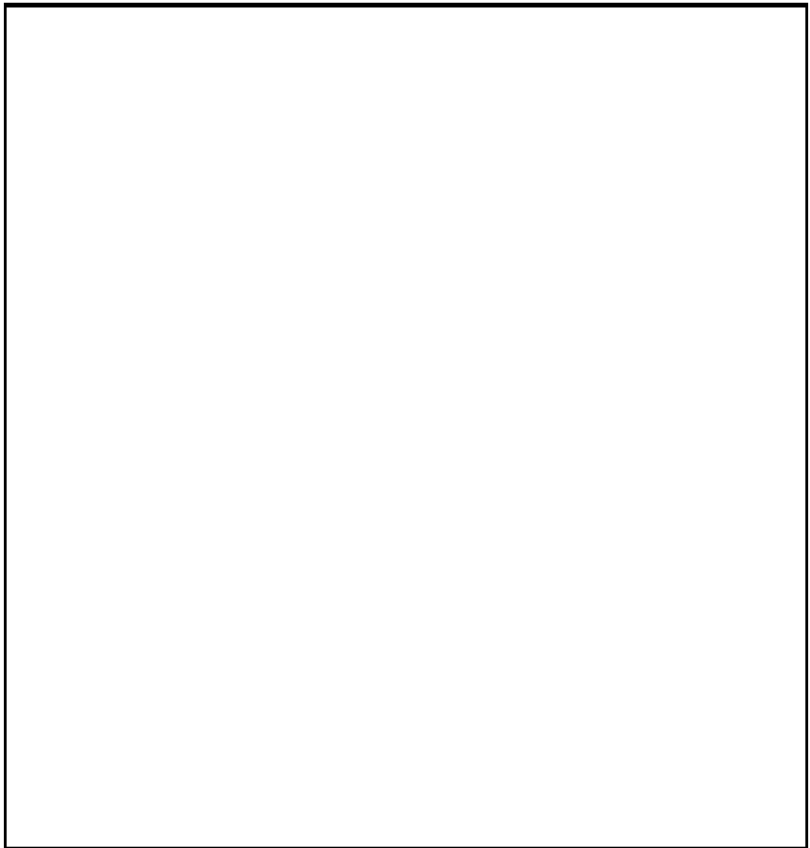


iDX3

(formerly iDomain)



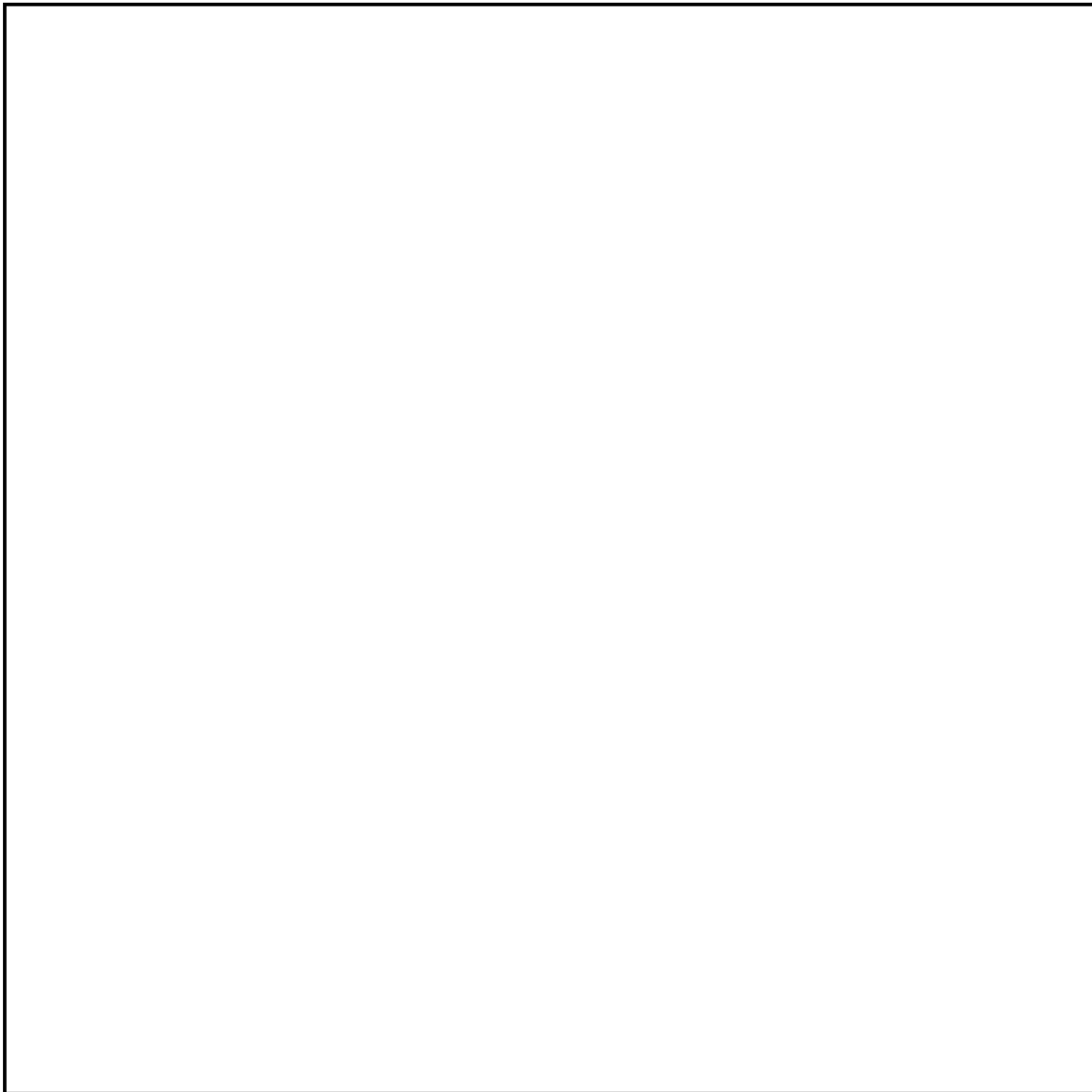
- Enterprise wide technology application
 - FBI web-based mapping application
 - Modeled after NGA's Palanterra X3
 - Manage, Manipulate, Query and display geospatial data
- Multiple Data Sources
- Robust Requirements Process
- Analytical Tools
 - Routes, Drive Time, etc.
 - Buffers
- Data Sharing
- Imagery!



b2
b7E



FIELD/HSIP



b2
b7E



Training & Development

- Training Accomplishments
 - As of 05/26/2010:
 - FBI Personnel trained for FBI Basic GEOINT
 - trained in FY 2010
 - external training opportunities in FY 2010
 - ESRI, Universities, etc.
 - NGA College
 - NGA Analyst Exchange

b2
b7E

- Daily Technical Support to the field and FBIHQ

b6
b7C

- GIA position

-
-

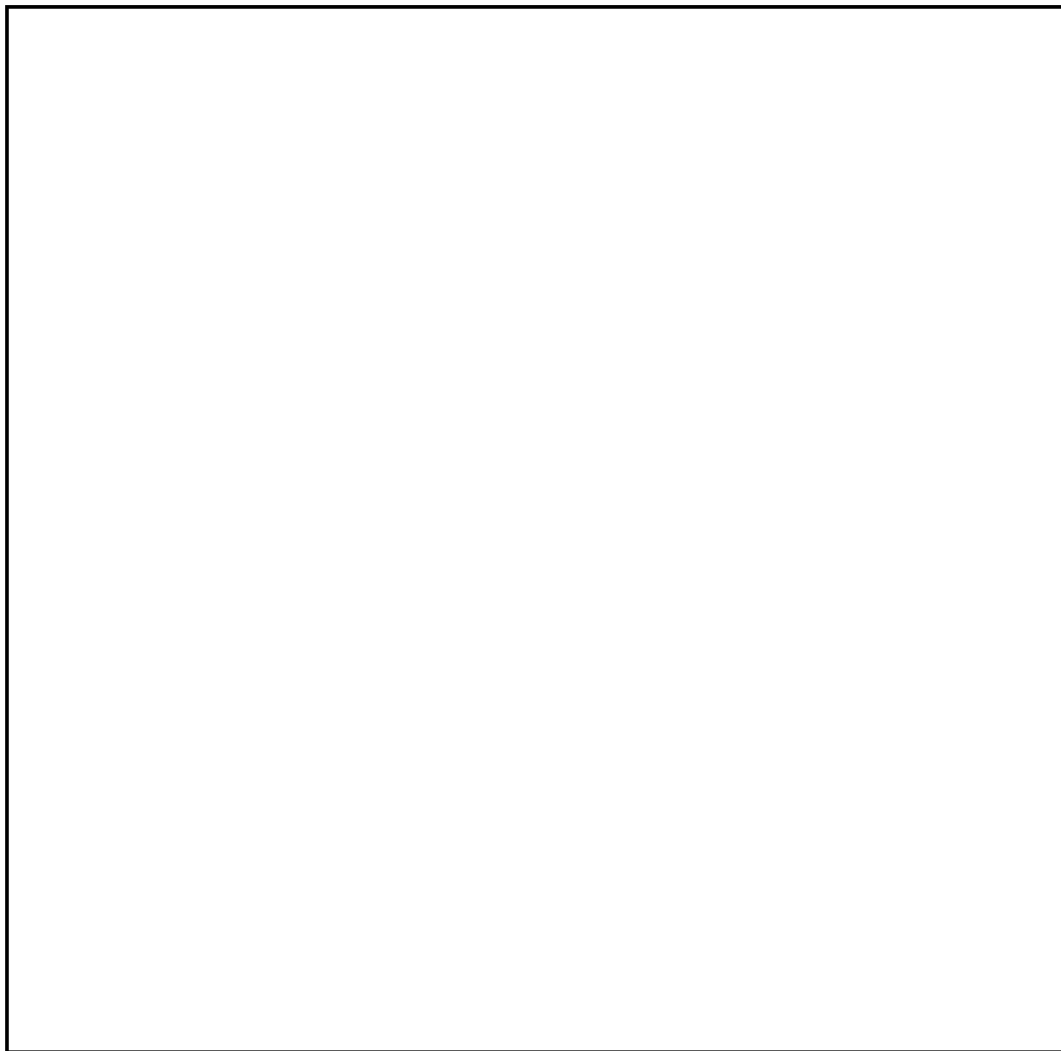
b2
b7E



Training & Development



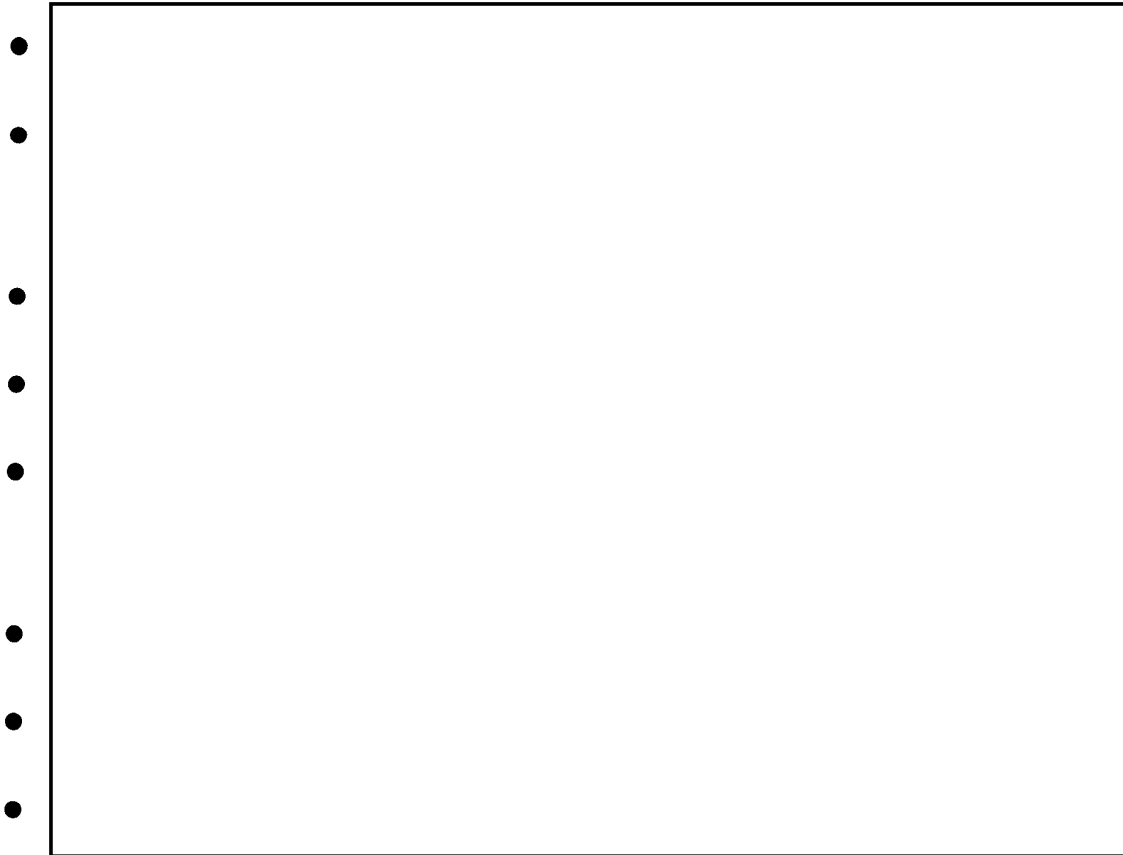
- Training Planned for FY 2011



b2
b7E



Operational Support

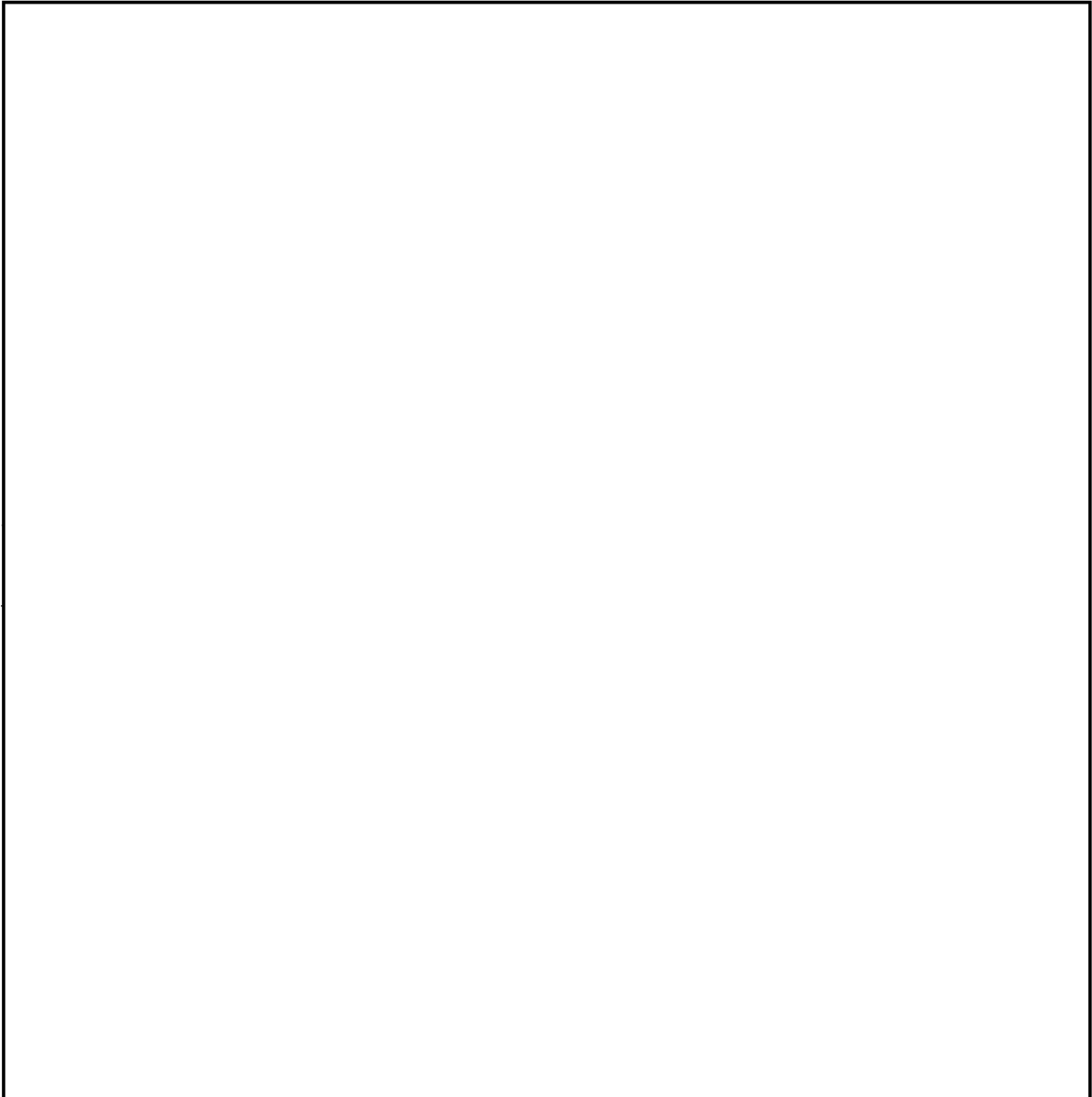


b2
b7E

- Guardian/eGuardian



NGA



b2
b6
b7C
b7E




Questions?



GEOINT Techniques





b2
b7E

- National Strategic Maps
 - Risk Based Planning
 - PDB
- Network Analyst/Tracking Analyst

- Canvass
 - Narrow down interview area
 - Narrow down interview list
- Travel (CONUS & OCONUS)
 - Analyze travel patterns
 - Route Analysis
 - Determine destinations of interest
 - Population densities as a relevant factor
- Confidential Human Sources
 - Source coverage
 - Reporting areas
 - Gaps in reporting
 - Vetting/Validation

- Financial Transactions


- FBI Data


- Imagery


- Communications Analysis


- Cases
 - Historical v. Present
 - Sophisticated Techniques (THH, FISA, etc.)
 - Division/County/Address views