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

DIOG Sections 4, 9, 15

SSA ...

Division ...

- (Tel Number)

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 <u>not</u> apply to investigative and intelligence collection activities of the FBI <u>in</u> 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

- Program Guide
- Program Guide
- Program Guide

DIOG: Table of Contents

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

- [redacted]

b2
b7E

- What can you do with this information?
- [redacted]

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

UNCLASSIFIED//FOUO

As of February 20, 2009

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]	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

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	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			
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 CUORC or UCRC (EAD/DD certain cases) Approval	CDC review, SAC and AD and 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	Not Permitted
20	11.9	Administrative Subpoenas: Drugs	Not Permitted	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	Not Permitted	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	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-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

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 [redacted] b2 b7E

- **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.

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 or USIC 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 the USIC) 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 DI/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 ([redacted] [redacted] b2 b7E
- 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.

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 [redacted] or a Type 5 assessment to record information about prospective or potential sources, etc.

b2
b7E

DIOG Section 9: Example

- [redacted]

b2
b7E

- Should Indianapolis open a PFI Assessment?

DIOG Section 9: Example

b2
b7E

FBIHQ DIOG Training

Thank you...

SSA