

UNCLASSIFIED//FOUO



FEDERAL BUREAU OF INVESTIGATION

OVERALL CLASSIFICATION:

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.



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



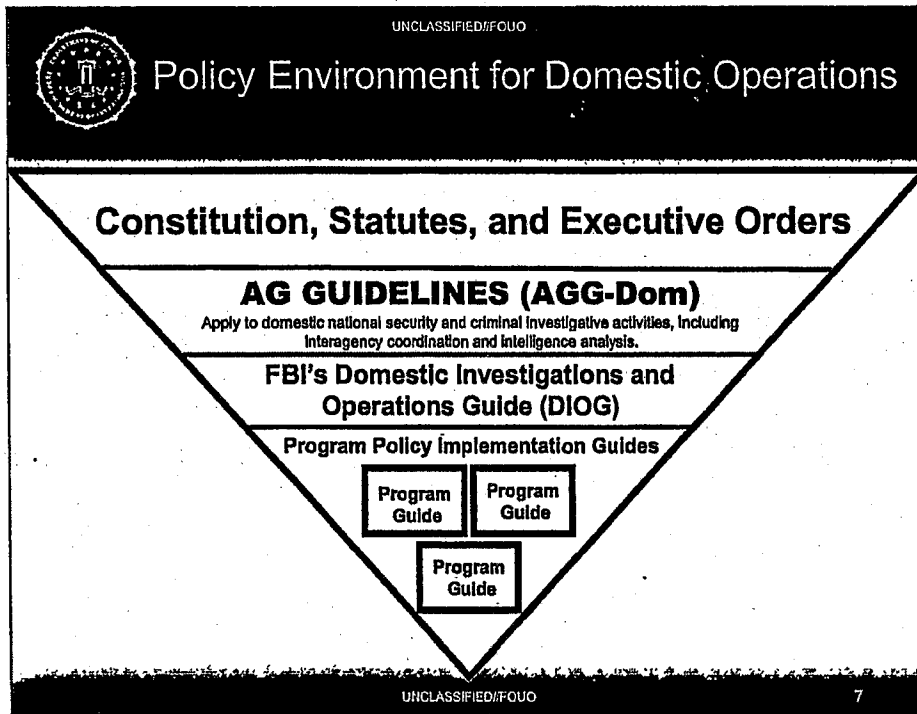
UNCLASSIFIED//FOUO

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



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



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



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



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



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

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



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



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

21

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.



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

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



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



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//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

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

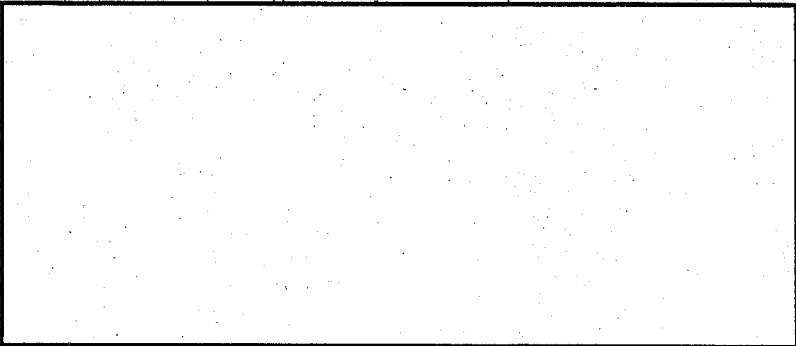
34

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



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.



Policy Environment for Domestic Operations

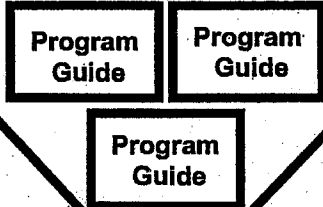
Constitution, Statutes, and Executive Orders

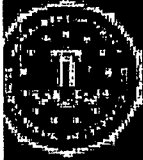
AG GUIDELINES (AGG-Dom)

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

UNCLASSIFIED//FOUO

Taking the test...

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

*** Max 20 mins each question**

UNCLASSIFIED//FOUO

11



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]

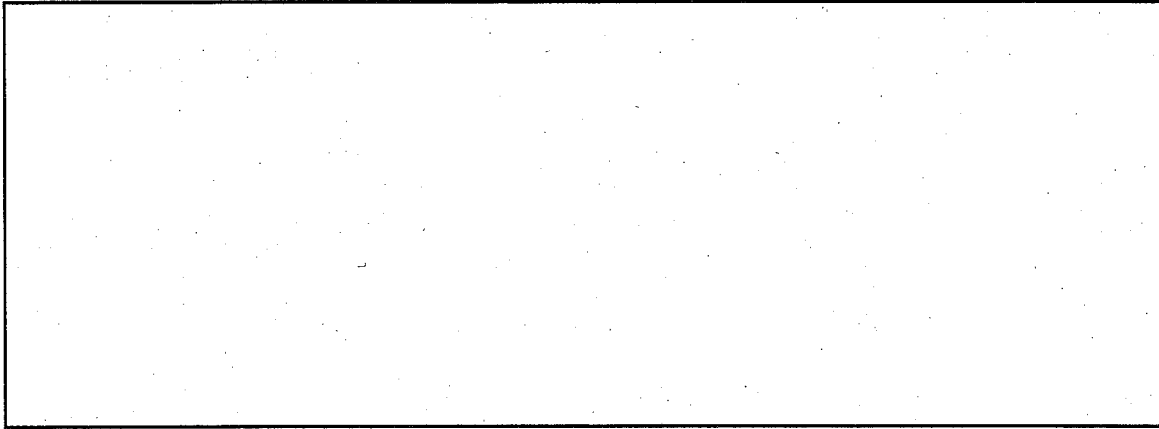
b2
b7E

- What can you do with this information?

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



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

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 in 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 OIG. 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 OIG

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
				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 (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. [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
16	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 or ASAC with delegated authority, NSB-Unit/UACB Approval
18	11.8	Undercover operations, Group I		CDC review, SAC, and AD and UCRC 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. HC: 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		
28	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 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 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



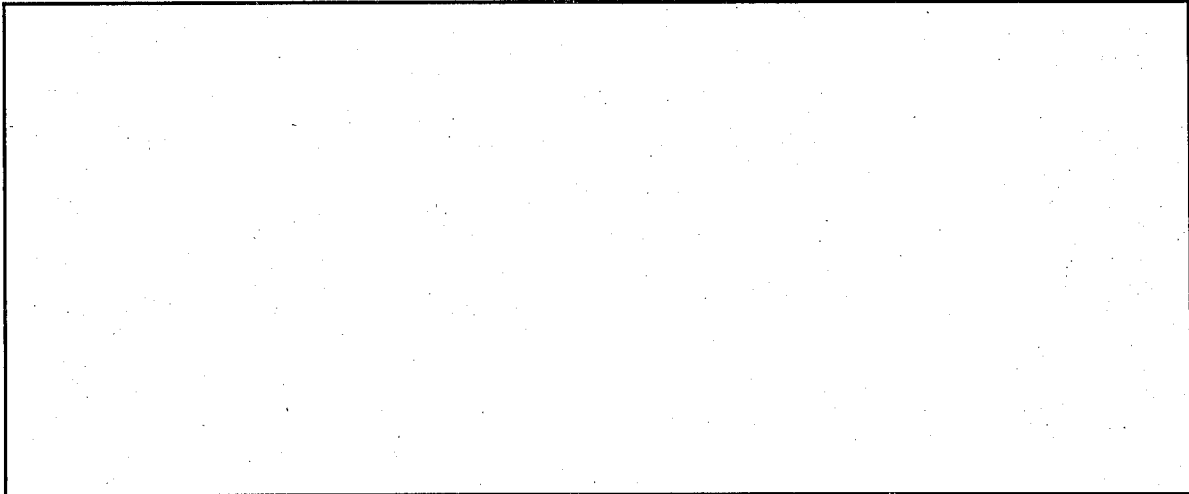
Privacy Act / USPER Considerations

- 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

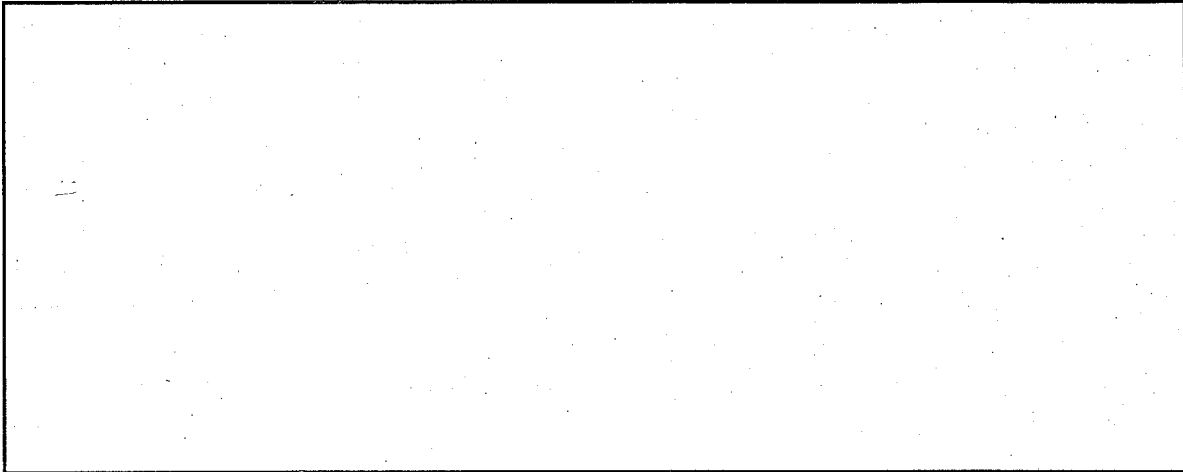


b2
b7E

- Should Indianapolis open a PFI Assessment?



DIOG Section 9: Example



b2
b7E



FBIHQ DIOG Training

Thank you...

SSA