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

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)
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"
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
<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Scope and Purpose</td>
</tr>
<tr>
<td>2.</td>
<td>General Authorities and Principles</td>
</tr>
<tr>
<td>3.</td>
<td>Core Values, Roles and Responsibilities</td>
</tr>
<tr>
<td>4.</td>
<td>Privacy and Civil Liberties, and Least Intrusive Methods</td>
</tr>
<tr>
<td>5.</td>
<td>Assessments</td>
</tr>
<tr>
<td>6.</td>
<td>Preliminary Investigations</td>
</tr>
<tr>
<td>7.</td>
<td>Full Investigations</td>
</tr>
<tr>
<td>8.</td>
<td>Enterprise Investigations</td>
</tr>
<tr>
<td>9.</td>
<td>Foreign Intelligence</td>
</tr>
<tr>
<td>10.</td>
<td>Sensitive Investigative Matter</td>
</tr>
<tr>
<td>11.</td>
<td>Investigative Methods</td>
</tr>
<tr>
<td>12.</td>
<td>Assistance to Other Agencies</td>
</tr>
<tr>
<td>14.</td>
<td>Retention and Sharing of Information</td>
</tr>
<tr>
<td>15.</td>
<td>Intelligence Analysis and Planning</td>
</tr>
<tr>
<td>16.</td>
<td>Undisclosed Participation</td>
</tr>
<tr>
<td>17.</td>
<td>Otherwise Illegal Activity</td>
</tr>
<tr>
<td></td>
<td>Appendices</td>
</tr>
</tbody>
</table>
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)
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 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)
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.
### 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 Collecting, Retaining, and Disseminating of Foreign Intelligence Information
  - The Attorney General’s Procedures 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 Terminal 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, Warranted Monitoring of Verbal Communications (superseded, as to the FBI)
- Numerous and different guidelines used for compliance
- Different roles 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
### Comparison of Prior and New Attorney General Guidelines

#### Assessments

<table>
<thead>
<tr>
<th>Prior AGG (Threat Assessments)</th>
<th>New AGG (Assessments)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Authorized Methods</strong></td>
<td><strong>Authorized Methods</strong></td>
</tr>
<tr>
<td>• Obtain publicly available information</td>
<td>• Obtain publicly available information</td>
</tr>
<tr>
<td>• Access and examine FBI/DGU records, and obtain information from any FBI/DGU personnel</td>
<td>• Access and examine FBI and other OGJ records, and obtain information from any FBI or OGJ personnel</td>
</tr>
<tr>
<td>• Check other federal, state, and local records</td>
<td>• Access and examine records maintained by, and request information from, other federal, state, local, tribal, or foreign government or agencies</td>
</tr>
<tr>
<td>• Use online services and resources</td>
<td>• Use online services and resources</td>
</tr>
<tr>
<td>• Interview previously established Human Sources (not including new tasking of such sources)</td>
<td>• Interview or request information from members of the public and private entities</td>
</tr>
<tr>
<td>• Interview or request information from members of the public and private entities (other than preset interviews or requests)</td>
<td>• Accept voluntarily information</td>
</tr>
<tr>
<td>• Accept voluntarily information</td>
<td><strong>Reporting Requirements</strong></td>
</tr>
<tr>
<td><strong>None</strong></td>
<td><strong>None</strong></td>
</tr>
</tbody>
</table>

**UNCLASSIFIED//FOOU**
## Comparison of Prior and New Attorney General Guidelines

### Preliminary Investigations

<table>
<thead>
<tr>
<th>Prior AGG</th>
<th>New AGG</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Authorized Methods</strong></td>
<td><strong>Authorized Methods</strong></td>
</tr>
<tr>
<td>- All Threat Assessment techniques</td>
<td>- All Assessment Methods</td>
</tr>
<tr>
<td>- Interviews (including pretext) of subject and others</td>
<td>- Mail covers</td>
</tr>
<tr>
<td>- Recruitment of new human sources &amp; tasking of existing sources</td>
<td>- Physical searches of personal or real property where a warrant or order is not legally required because there is no reasonable expectation of privacy</td>
</tr>
<tr>
<td>- Inquiry of foreign law enforcement, intelligence, or security agencies</td>
<td>- Concealment monitoring of communications (including consensual computer monitoring)</td>
</tr>
<tr>
<td>- Mail covers</td>
<td>- Closed circuit TV, direction finders, and monitoring devices</td>
</tr>
<tr>
<td>- Covert surveillance of communications</td>
<td>- Polygraph examinations</td>
</tr>
<tr>
<td>- Closed circuit TV, direction finders, and monitoring devices</td>
<td>- Undercover operations</td>
</tr>
<tr>
<td>- Undercover operations</td>
<td>- Compulsory process as authorized by few Federal Grand Jury and other subpoenas and National Security Letters</td>
</tr>
<tr>
<td>- Physical, photo, and video surveillance</td>
<td>- Accessing store wire and electronic communications and transactional records</td>
</tr>
<tr>
<td>- Polygraph examinations</td>
<td>- Use of pen registers and trap and trace devices</td>
</tr>
<tr>
<td>- National Security Letters</td>
<td></td>
</tr>
<tr>
<td>- Accessing stored wire/electronic communications</td>
<td><strong>Reporting Requirements</strong></td>
</tr>
<tr>
<td>- Pen registers/Taps &amp; Trace</td>
<td>- Only if sensitive investigative matter - Notify FBIHQ and DOJUS, Attorney - Notify FBI if sensitive matter is a national security threat (NLT 30 Days)</td>
</tr>
<tr>
<td>- Obtain business records</td>
<td>- FBIHQ notify DAG if initiation is disapproved</td>
</tr>
<tr>
<td>- Grand Jury subpoenas</td>
<td>- FBIHQ notify the DAG if initiative is disapproved based on insufficient justification for national security matters</td>
</tr>
</tbody>
</table>
## Comparison of Prior and New Attorney General Guidelines

### Full Investigations

<table>
<thead>
<tr>
<th>Prior AGG</th>
<th>New AGG</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Authority Methods</strong></td>
<td><strong>Authority Methods</strong></td>
</tr>
<tr>
<td>- All Threat Assessment techniques</td>
<td>- All Assessment Methods</td>
</tr>
<tr>
<td>- All preliminary investigation techniques</td>
<td>- All Preliminary Investigation Methods</td>
</tr>
<tr>
<td>- Electronic Surveillance</td>
<td>- Electronic Surveillance</td>
</tr>
<tr>
<td>- Physical searches and Mail openings</td>
<td>- Foreign Intelligence collection under Title VII of FISA</td>
</tr>
<tr>
<td><strong>Reporting Requirements</strong></td>
<td><strong>Reporting Requirements</strong></td>
</tr>
<tr>
<td>- Field notification of initiation to FBHQ (10 Days)</td>
<td>- Notify FBHQ and DOJ/U.S. Attorney sensitive investigative matter - Notify NSE if sensitive matter is a national security threat (NLT 20 days)</td>
</tr>
<tr>
<td>- FBHQ notification to OLC/IG of initiation (10 Days)</td>
<td>- FBHQ notification to DOJ/NSD (NLT 30 Days) only if:</td>
</tr>
<tr>
<td>- FBHQ notify DAG if initiation is disapproved</td>
<td></td>
</tr>
<tr>
<td>- Annual summary submitted to DOJ/CA</td>
<td>- Initiation on U.S. person relating to a national security threat</td>
</tr>
<tr>
<td></td>
<td>- Initiation based on foreign intelligence requirement</td>
</tr>
<tr>
<td></td>
<td>- FBHQ notify the DAG if initiation is disapproved based on insufficient predication for national security matters</td>
</tr>
</tbody>
</table>
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)
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
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)
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.
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.
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

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
Authority 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


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

- Conducting background checks and inquiries 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
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

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).
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

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 3.2:

- 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.
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

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.
( 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 3.4.A – Supervisor Defined:

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

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.
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

**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
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

Teaching Points: ACS Investigative Case management Case Review report.
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

Teaching Points: DIOG Section 5 details file review requirements.
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

Teaching Points: Probationary Agent File reviews conducted at least every 60 days, recommend 30 days
Note: the FD-71 provides a new mechanism to assign an Assessment to an electronic Unaddressed Work File in the appropriate classification.
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.
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
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.
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
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.

Teaching Point:
The FBI is a very important agency with dedicated, highly professional, greatly disciplined Government servants. These words, uttered in 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.
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.
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).

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.
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?

Teaching Point:
Questions continue on next slide
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.
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.
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
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.

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.
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
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
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**

**DIQG Section 5 &11: Investigative Methods**

Authorized Methods for Assessments and Predicated Investigations

<table>
<thead>
<tr>
<th>Method Description</th>
<th>Authorization</th>
<th>Information Collection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Obtain publicly available information</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Access and examine FBI and other DOJ records, and obtain information from any FBI or DOJ personnel</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Access and examine records maintained by, and request information from, other federal, state, local, tribal, or foreign governmental entities or agencies</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Use online services and resources (whether nonprofit or commercial)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Use and monitor human sources in conformity with AG Guidelines Regarding the Use of FBI Confidential Human Sources</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Interview or required information from members of the public and private sources (includes pretrial interviews)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Accept information voluntarily provided by governmental or private sources</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Engage in observation or surveillance not requiring a court order</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mail covers</td>
<td></td>
<td></td>
</tr>
<tr>
<td>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 cans)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Conversational monitoring of communications, including conversational computer monitoring, is subject to legal review by the CDC or the FBI ODC. Where a sensitive monitoring circumstance is involved, monitoring must be approved by the Criminal Investigation Division or, if the investigation concerns foreign intelligence or a threat to the national security, by the National Security Division.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Use of closed-circuit television, closed circuit security monitoring, and other monitoring devices, subject to legal review by the CDC or FBI ODC</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Polygraph examinations</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Undercover operations</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Compromise 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)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Accompany stored wire and electronic communications and transactional records</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Use of pen registers and tap and trace devices</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Electronic surveillance</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Foreign intelligence collection under Title VII of FISA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Physical searches, including mail openings, where a warrant or court order is legally required because there is an expectation of privacy.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
# Investigative Methods/Approvals Chart

<table>
<thead>
<tr>
<th>Authorized Method/OSO Reference</th>
<th>Apprval Levels for Assessment and Preauthorization</th>
<th>Assessment</th>
<th>Preauthorization</th>
<th>Post Approval</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 SIA</td>
<td>Obtain publicly available information</td>
<td>Not Required</td>
<td>Not Required</td>
<td>Not Required</td>
</tr>
<tr>
<td>2 SAC</td>
<td>Tasking OIC in a public setting (TAC)</td>
<td>Not Required</td>
<td>SSIA Approval</td>
<td>SSIA Approval</td>
</tr>
<tr>
<td>3 SAC</td>
<td>Physical surveillance of a person or group (Techniques other than traffic surveillance or with reasonable expectation of collection)</td>
<td>Memo Required</td>
<td>Not Required</td>
<td>Not Required</td>
</tr>
<tr>
<td>4 SAC</td>
<td>DOO for surveillance</td>
<td>Not Required</td>
<td>Not Required</td>
<td>Not Required</td>
</tr>
<tr>
<td>5 SAC</td>
<td>Access to and examine FBI and other Department of Justice (DOJ) records, and obtain information from an FBI or other DOJ personnel</td>
<td>Not Required</td>
<td>Not Required</td>
<td>Not Required</td>
</tr>
<tr>
<td>6 SAC</td>
<td>Access to and examine records maintained by, and those involving persons, other federal, state, or local government entities or agencies</td>
<td>Not Required</td>
<td>Not Required</td>
<td>Not Required</td>
</tr>
<tr>
<td>7 SAC</td>
<td>The value nature and purpose (whether commercial or non-commercial)</td>
<td>Not Required</td>
<td>Not Required</td>
<td>Not Required</td>
</tr>
<tr>
<td>8 SAC</td>
<td>Information or research information from a person or public or private entity</td>
<td>Not Required</td>
<td>Not Required</td>
<td>Not Required</td>
</tr>
<tr>
<td>9 SAC</td>
<td>The number or location, and purpose of the individual(s)</td>
<td>Not Required</td>
<td>Not Required</td>
<td>Not Required</td>
</tr>
<tr>
<td>10 SAC</td>
<td>Access to and examine records maintained by</td>
<td>Not Required</td>
<td>Not Required</td>
<td>Not Required</td>
</tr>
<tr>
<td>11 SAC</td>
<td>The number of people involved</td>
<td>Not Required</td>
<td>Not Required</td>
<td>Not Required</td>
</tr>
<tr>
<td>12 SAC</td>
<td>The number and location of the individual(s)</td>
<td>Not Required</td>
<td>Not Required</td>
<td>Not Required</td>
</tr>
<tr>
<td>13 SAC</td>
<td>The number of people involved</td>
<td>Not Required</td>
<td>Not Required</td>
<td>Not Required</td>
</tr>
</tbody>
</table>

**Teaching Points:**

1. **Obtain Publicly Available Information:** Sensitive approval is not required for use of this method, access to information gathered at a religious service, mentioning any other policy, holding a CHS or UCE to attend a religious service during a predetermined investigation, whether open to the public or not, requires SSA approval. Taking a CHS to attend a religious service, whether open to the public or not, during an investigation requires SAC approval.

2. **Entice to observation or surveillance or not requires a court order:** Use of noncoercive devices operated by a user (e.g., binoculars/hand-held camera/measuring devices) is authorized in physical surveillance provided the device is not used to capture information on a person for a reasonable expectation of activity (e.g., equipment such as a pedestrian i.e., a pedestrian) or where an activity would involve a private conversation or thermal imaging is being used (as in case-by-case situations).

**Physical Surveillance Prior Approval:**

- FBI employee cannot obtain multiple requests for one interview.
- No limit on use of field of moving physical surveillance. For preauthorized investigations: no limit on use of field

- SAC can delegate approval to SSA or BIA. Must be in writing and appropriately filed.

**Interviews:**

- SAC can delegate approval to SSA or BIA. Must be in writing and appropriately filed.

3. **Interviews:**

- SSA shall interview FBI and other DOJ personnel, and obtain information from any FBI or other DOJ personnel. Sensitive approval is not required to use this method during assessments or preauthorization investigations.

4. **Surveillance Reporting:**

- Each FBI interview conducted pursuant to a FISA, a FISA, a Foreign Intelligence Surveillance Act (FISA) or all other investigatory methods must be reviewed by the OIA and FBI.

**Pattern-Based Data Mining:**

- Use of one or more data bases to search for patterns or a set of group characteristics or patterns of behavior (e.g., the known characteristics of a particular terrorist organization).

**Interviewed Data:**

- 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 qualitative investigation.

5. **Interviews:**

- SAC should interview FBI personnel with FISA and other OIA personnel.
- FBI personnel may not state or admit any way that the information is considered to provide information on the subject or any other manner.
- A representative of the OIA should interview the subject to determine if the interview is being conducted.

**Interviews:**

- SAC can delegate approval to SSA or BIA. Must be in writing and appropriately filed.

6. **Surveillance Reporting:**

- OIA shall interview FBI and other DOJ personnel, and obtain information from any FBI or other DOJ personnel. Sensitive approval is not required to use this method during assessments or preauthorization investigations.

**Surveillance Reporting:**

- Each FBI interview conducted pursuant to a FISA, a FISA, a Foreign Intelligence Surveillance Act (FISA) or all other investigatory methods must be reviewed by the OIA and FBI.

**Pattern-Based Data Mining:**

- Use of one or more data bases to search for patterns or a set of group characteristics or patterns of behavior (e.g., the known characteristics of a particular terrorist organization).

**Interviewed Data:**

- 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 qualitative investigation.

**Interviews:**

- SAC should interview FBI personnel with FISA and other OIA personnel. FBI personnel may not state or admit any way that the information is considered to provide information on the subject or any other manner. A representative of the OIA should interview the subject to determine if the interview is being conducted.

**Interviews:**

- SAC can delegate approval to SSA or BIA. Must be in writing and appropriately filed.
### Investigative Methods/Approvals Chart

<table>
<thead>
<tr>
<th>Authorized Method and DIOG Restrictions*</th>
<th>Approvals for Investigations Non-FBI Data Sources ho That Require Security Clearances or FBI Data Sources</th>
<th>Non-FBI Data Sources ho That Require Security Clearances</th>
<th>FBI Data Sources</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.1 Mail covers</td>
<td>Not Permitted</td>
<td>Permitted</td>
<td>Permitted</td>
</tr>
<tr>
<td>11.1.1 Proposed wireless or encrypted mail is sent to or from a legitimate recipient for which permission has been obtained.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11.1.2 Covert or dual-sourcewiretaps are used. The warrant specifically permits the use of wiretaps.</td>
<td>Not Permitted</td>
<td>Permitted</td>
<td>Permitted</td>
</tr>
<tr>
<td>11.2 Discreet interception methods, including electronic or non-electronic methods.</td>
<td>Not Permitted</td>
<td>Permitted</td>
<td></td>
</tr>
<tr>
<td>11.2.1 Covert or dual-sourcewiretaps are used. The warrant specifically permits the use of wiretaps.</td>
<td>Not Permitted</td>
<td>Permitted</td>
<td></td>
</tr>
<tr>
<td>11.3 Other methods of interception, including electronic or non-electronic methods.</td>
<td>Not Permitted</td>
<td>Permitted</td>
<td></td>
</tr>
<tr>
<td>11.3.1 Covert or dual-sourcewiretaps are used. The warrant specifically permits the use of wiretaps.</td>
<td>Not Permitted</td>
<td>Permitted</td>
<td></td>
</tr>
<tr>
<td>11.4 Distribution of information.</td>
<td>Not Permitted</td>
<td>Permitted</td>
<td></td>
</tr>
<tr>
<td>11.4.1 Counterintelligence activities.</td>
<td>Not Permitted</td>
<td>Permitted</td>
<td></td>
</tr>
<tr>
<td>11.4.2 Covert or dual-sourcewiretaps are used. The warrant specifically permits the use of wiretaps.</td>
<td>Not Permitted</td>
<td>Permitted</td>
<td></td>
</tr>
<tr>
<td>11.5 Surveillance procedures.</td>
<td>Not Permitted</td>
<td>Permitted</td>
<td></td>
</tr>
<tr>
<td>11.5.1 Covert or dual-sourcewiretaps are used. The warrant specifically permits the use of wiretaps.</td>
<td>Not Permitted</td>
<td>Permitted</td>
<td></td>
</tr>
<tr>
<td>11.6 Other methods of surveillance.</td>
<td>Not Permitted</td>
<td>Permitted</td>
<td></td>
</tr>
<tr>
<td>11.6.1 Counterintelligence activities.</td>
<td>Not Permitted</td>
<td>Permitted</td>
<td></td>
</tr>
<tr>
<td>11.6.2 Covert or dual-sourcewiretaps are used. The warrant specifically permits the use of wiretaps.</td>
<td>Not Permitted</td>
<td>Permitted</td>
<td></td>
</tr>
</tbody>
</table>

*As of May 8, 2009

### Teaching Points:

1. **Mail Covers**: The DIOC 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 receipt and concurrence, the NSLB shall transmit the letter request for signature to the EAD, National Security Branch, or, in his or her absence, to the Director.

2. **Consensual Monitoring**: 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 may 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.

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; AD/CIs in NY, DC and LA; and all SACs. Every NSL must be reviewed and approved by a CDC or NSLB attorney.