FBIHQ DIOG Training

FEDERAL BUREAU OF INVESTIGATION

OVERALL CLASSIFICATION:
UNCLASSIFIED

Session A - Quantico Assessments Prelim, Full & Enterprise Investigations
DIOG Sections 5, 6, 7, 8

SSA ...

Division ...
– (Tel Number)
Participation Standards:

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

During the scenario exercises, participants will be called upon to provide their response to particular facts or circumstances. Each Unit/Section should select a representative to speak for the Unit/Section and rotate that responsibility among the group. The scenarios are meant to prompt discussion, but the presenters must keep the scenario moving forward. Please understand that everyone may not be able to voice their perspective in the group setting. Keep in mind there may be several avenues to reach the same justified conclusion. You may use your handouts and training aids to inform your decision.
DIOG Section 1: Scope & Purpose

- DIOG applies to all investigative and intelligence collection activities conducted by the FBI
  - within the United States
  - in the United States territories
  - outside the territories of all countries
- DIOG does not apply to investigative and intelligence collection activities of the FBI in foreign countries
  - governed by AGGs for Extraterritorial FBI Operations (national security and criminal)
In addition to this policy document, each FBIHQ substantive Division has a Policy Implementation Guide (PG) that supplements the DIOG.

As a result, numerous FBI manuals, electronic communications, letterhead memoranda, and other policy documents are incorporated into the DIOG and Division PGs, thus, consolidating FBI policy guidance.
The AGG-Dom replaces the following six guidelines:

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

Constitution, Statutes, and Executive Orders

AG GUIDELINES (AGG-Dom)
Apply to domestic national security and criminal investigative activities, including interagency coordination and intelligence analysis.

FBI's Domestic Investigations and Operations Guide (DIOG)

Program Policy Implementation Guides

Program Guide
<table>
<thead>
<tr>
<th>1. Scope and Purpose</th>
<th>10. Sensitive Investigative Matter</th>
</tr>
</thead>
<tbody>
<tr>
<td>2. General Authorities and Principles</td>
<td>11. Investigative Methods</td>
</tr>
<tr>
<td>3. Core Values, Roles and Responsibilities</td>
<td>12. Assistance to Other Agencies</td>
</tr>
<tr>
<td>5. Assessments</td>
<td>14. Retention and Sharing of Information</td>
</tr>
<tr>
<td>6. Preliminary Investigations</td>
<td>15. Intelligence Analysis and Planning</td>
</tr>
<tr>
<td>7. Full Investigations</td>
<td>16. Undisclosed Participation</td>
</tr>
<tr>
<td>8. Enterprise Investigations</td>
<td>17. Otherwise Illegal Activity</td>
</tr>
<tr>
<td>9. Foreign Intelligence</td>
<td>Appendices</td>
</tr>
</tbody>
</table>
The Test...

50 questions
- Multiple Choice
- True/False

* Max 20 mins each question
Taking the test...

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

* Max 20 mins each question
Overview

The Attorney General's Guidelines for Domestic FBI Operations (AGG-Dom) combine "threat assessments" under the former Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection and the "prompt and extremely limited checking out of initial leads" under the former Attorney General's Guidelines on General Crimes, Racketeering Enterprise and Terrorism Enterprise Investigations into a new investigative category entitled "assessments." All assessments must either be opened in an investigative classification as an assessment file (e.g., [Guardian]), or placed in an [Guardian]), or placed in an as discussed in greater detail below.
### Field Office Investigations Chart

<table>
<thead>
<tr>
<th>Investigation</th>
<th>Purpose</th>
<th>Duration</th>
<th>Documentation</th>
<th>Analysis</th>
<th>Justification Required</th>
<th>EM</th>
<th>Reference Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Type 1</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Full</td>
<td>To verify an &quot;important factual basis&quot; that reasonably justifies clearance of individual employees.</td>
<td>No further description of detailed contents.</td>
<td>EO</td>
<td>Every 30 days of majority employees</td>
<td>CDC Review, SAC Approval</td>
<td><strong>Investigative Squat</strong></td>
<td></td>
</tr>
<tr>
<td>Emergency</td>
<td>To verify an &quot;important factual basis&quot; that reasonably justifies clearance of individual employees.</td>
<td>No further description of detailed contents.</td>
<td>EO</td>
<td>Every 30 days of majority employees</td>
<td>CDC Review, SAC Approval</td>
<td><strong>Investigative Squat</strong></td>
<td></td>
</tr>
<tr>
<td>PV/PLJ</td>
<td>To verify an &quot;important factual basis&quot; that reasonably justifies clearance of individual employees.</td>
<td>No further description of detailed contents.</td>
<td>EO</td>
<td>Every 30 days of majority employees</td>
<td>CDC Review, SAC Approval</td>
<td><strong>Investigative Squat</strong></td>
<td></td>
</tr>
</tbody>
</table>

**Note:** The chart details the procedures and requirements for different types of investigations, including the duration, documentation, analysis, and justification required for each.
A new type of activity formed by combining:

- "threat assessments" from the former AGG for FBI National Security Investigations and Foreign Intelligence Collection
- the "prompt and extremely limited checking of initial leads" allowed under the former AGG on General Crimes, Racketeering Enterprise and Terrorism Enterprise Investigations

Assessment activities:

- must always be based on an authorized purpose
- require specific work flows for management and documentation (FD-71, Assessment Files, ...)
Before initiating or approving an assessment, an FBI employee or approving official must determine whether:

- An authorized purpose and objective exists to conduct the assessment
- The assessment is based on factors other than the exercise of First Amendment activities or the race, ethnicity, national origin or religion of the subject
- The assessment is an appropriate use of personnel and financial resources
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 5:
Type 1 and 2 Assessments

Investigative Methods in Type 1 and 2 Assessments require higher supervisory approval:

- Physical surveillance
- Certain interviews
- Tasking CHSs
### DIOG Section 5: Type 1 and 2 Assessments

<table>
<thead>
<tr>
<th>Investigation</th>
<th>Purpose</th>
<th>Duration</th>
<th>Documentation</th>
<th>Approval</th>
<th>Justification</th>
<th>Review</th>
<th>SIM</th>
<th>Responsible Entity</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Type 1</strong></td>
<td>Activities constituting violations of federal criminal law or threats to national security</td>
<td>As long as necessary to achieve purpose and objective; No time limit</td>
<td>FD-71 or Guardian</td>
<td>Any employee can initiate; SSA or SIA Approval</td>
<td>Every 30 days</td>
<td>CDC review; SAC approval</td>
<td>Investigative Squad</td>
<td></td>
</tr>
<tr>
<td><strong>Type 2</strong></td>
<td>The involvement or role of individuals, groups, or organizations in such activities (#1 above)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
DIOG Section 5:
Type 1 and 2 Assessment Example

- What would you do with this information?
DIOG Section 5:
Type 1 and 2 Assessment Example

- What can the agent do with this information?
DIOG Section 5: Type 1 and 2 Assessment Example

- What action will you take?
DIOG Type 2 Assessment: Example
• Current version of the form: FD-71 v1.4: dated 3/10/2009
• V1.4 has major changes to:
  – SIM process
  – Supervisor decisions
  – Information dissemination
• Changes or new features are highlighted in this presentation with orange text boxes
Complete the form with as much information as is provided. 
Note: All fields marked with an asterisk must be completed.
After a form is successfully advanced to a new step (submitted to a supervisor, reassigned, uploaded) a confirming message-box appears.

After a form is serialized, it automatically switches to the print view, in order for the user to print a copy.

The serial number field has been enlarged to handle up to 9 digits.
AGG DOM and Guardian

Guardian has been modified to coordinate with the 12/1/08 implementation of the new Attorney General Guidelines for Domestic FBI Operations (AGG-Dom).

There have been four changes in Guardian:

- Guardian incidents once assigned with an authorized purpose and objective are considered

Guardian incidents once assigned with an authorized purpose and objective are considered
Information NOT permitted in Guardian:

- 
- 
- 
- 
- 
- 
- 

ACLURM004316
Guardian: Ability to Delete
Investigations and Assessments are deemed "Sensitive Investigative Matters (SIMs)" when they involve activities of:

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

SIMs Require Chief Division Counsel (CDC) review, SAC approval and notice to appropriate HQ Section/Unit.
The results from a FGJS can be placed in a note in Guardian, as long as the information is not attributed to the Grand Jury.

Usage:
Add a note to the incident and choose the method “FGJS for... subscriber information” to document that a subpoena is being sought.

Example note:
When the results come back, add a new note to the incident and choose the method "Administrative note for informational purposes" and simply state the results. Do not refer to the FGJS.

Example note:
# Type 3 Assessments

<table>
<thead>
<tr>
<th>Investigation</th>
<th>Purpose</th>
<th>Duration</th>
<th>Documentation</th>
<th>Approval</th>
<th>Justification Review</th>
<th>SIM</th>
<th>Responsible Entity</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

**UNCLASSIFIED//FOUO**

As of May 19, 2009 35
Type 3 Assessment: Authorized Purpose & Objective

The authorized purpose of a Type 3 assessment is to obtain information on an identified potential threat or vulnerability in your domain.

The objective is to seek answers relating to the potential threat and vulnerability.
Type 3 Assessment: Key Points

- Opened based upon a potential identified threat or vulnerability
- One assessment file per threat or vulnerability identified
- Must initiate a separate assessment if active collection falls out of the purview of an open assessment or predicated case
- Incidental collection does not require opening a Type 3 assessment, but can be reported out of the case it was collected in

• • •
<table>
<thead>
<tr>
<th>Investigation</th>
<th>Purpose</th>
<th>Duration</th>
<th>Documentation</th>
<th>Approval</th>
<th>Justification Review</th>
<th>SIM</th>
<th>Responsible Entity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type 4</td>
<td>Obtaining information or fact sheets (documented and shared)</td>
<td>As long as necessary to achieve purpose and objective, no time limit</td>
<td>85 before initiating</td>
<td>Prior SSA or SSA Approval</td>
<td>Every 90 days, if probationary employees; every 60 days</td>
<td>CDC review, SAC approval</td>
<td>Investigative Support Can support</td>
</tr>
</tbody>
</table>

UNCLASSIFIED//FOUO

As of May 19, 2009
Type 4 Assessment: Key Points

- The authorized purpose of a Type 4 assessment is to obtain information to inform or facilitate intelligence analysis and planning.
Type 4 Assessment: Key Points

- One file per assessment
- Must have authorized purpose and objective
- SSA/SIA approval needed to initiate
- CDC review/SAC approval for Sensitive Investigative Matters
- Subjected to 90 day file review
Type 4 Assessment:
Scenario
## Type 5 Assessments

<table>
<thead>
<tr>
<th>Investigation</th>
<th>Purpose</th>
<th>Duration</th>
<th>Documentation</th>
<th>Approval</th>
<th>Justification Review</th>
<th>SIM</th>
<th>Responsible Entity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type 5</td>
<td>Identify, assess, validate or maintain the cover or credibility of a CHS</td>
<td>CHSPM and AGG-CHS</td>
<td>CHSPM and AGG-CHS</td>
<td>CHS Manual</td>
<td>Not addressed in DOIG; Follow CHS Manual</td>
<td>Investigative Squad</td>
<td></td>
</tr>
</tbody>
</table>

As of May 19, 2009
Type 5 Assessments: Key Points

• **Two Distinct Activities**
  - Seeking information on a potential series
  - **Limited techniques**

• The— created for three purposes
  - Allow for an IA to do a
  - Interim ACS solution until CHSPM is updated and approved (Difference between CHS and Type 5)
  - HUMINT Squad broad based recruitment
## Type 6 Assessments

<table>
<thead>
<tr>
<th>Investigation</th>
<th>Purpose</th>
<th>Duration</th>
<th>Documentation</th>
<th>Approval</th>
<th>Justification Review</th>
<th>SIM</th>
<th>Responsible Entity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type 6 and PFI Assessments</td>
<td>Matters of Foreign Intelligence (MI) Interest responsive to MI requirements</td>
<td>As long as necessary to achieve purpose and objective / No time limit</td>
<td>EC before initiating</td>
<td>FIOC SSA or NIH / NO/ID Approval</td>
<td>Every 90 days / Every 60 days</td>
<td>HMI Review</td>
<td>Investigative Squad can support</td>
</tr>
</tbody>
</table>

**UNCLASSIFIED//FOUO**  
As of May 19, 2009
Type 6 Assessments: Key Points

- Must be approved by DI/CPMU.
- PFI is FI that is not directly related to the FBI's core national security and law enforcement missions.
- If FI can fall under one of the substantive programs (IT, DT, CD, CYB, CID, WMD) then it is not PFI.
- One Type 6 assessment file per USIC Requirement
- Incidental collection does not require a Type 6 assessment opening and can be reported out of the case it was collected in
Type 6 Assessments: Authorized Purpose and Objective

The authorized purpose of a Type 6 assessment is to obtain positive foreign intelligence that is responsive to a USIC foreign intelligence requirement that the FBI has been designated as a primary collector.

The objective is to seek answers relating to the USIC foreign intelligence requirement that the FBI has been designated as a primary collector. The objective should define the scope, time and manner to achieve the underlying purpose.
Overview
(U) The AGG-Dom authorizes a second level of investigative activity — predicated investigations. Predicated investigations that concern federal crimes or threats to the national security are subdivided into Preliminary Investigations and Full Investigations. Preliminary investigations may be initiated on the basis of any "allegation or information" indicative of possible criminal activity or threats to the national security.
Before initiating or approving a PI, you need to determine that:

- No investigative activity may be based solely on race, ethnicity, national origin, religion of the subject, or activities protected by the First Amendment
- An authorized purpose and adequate predication exists
- It is an appropriate use of personnel and financial resources
### Field Office Investigations Chart

<table>
<thead>
<tr>
<th>Investigation</th>
<th>Purpose</th>
<th>Identification</th>
<th>Investigation Type</th>
<th>Duration</th>
<th>Processing</th>
<th>Approval</th>
<th>Justification Review</th>
<th>Initial Approval</th>
<th>Relevant Events</th>
<th>Initial Approval Days</th>
<th>Responsible Entity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type 1</td>
<td>Explores criminal activity and implicative conduct of an individual or group as a national security threat.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Type 2</td>
<td>Involves the arrest of a U.S. citizen or alien in possession of evidence of committing a felony.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Type 3</td>
<td>Identifies, assists, monitors or operates the internal security or intelligence of a U.S. person.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Project and PI</td>
<td>Involves the maintenance of a project or program that is multinational in character.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Notes:**
- Type 1: Investigative activity is conducted by a U.S. law enforcement agency.
- Type 2: Requires the coordination and cooperation of multiple federal agencies.
- Type 3: Involves the cooperation of multiple international agencies.

**As of May 16, 2003**

ACLURM004338
## DIOG Section 6: Preliminary Investigations

<table>
<thead>
<tr>
<th>Investigation</th>
<th>Predication</th>
<th>Duration</th>
<th>Documentation</th>
<th>Approval</th>
<th>Justification Review</th>
<th>SIM</th>
<th>Responsible Entity</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>November</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

As of May 19, 2009
Preliminary Investigations

Predication for a PI includes "information or allegation" that:

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

- To determine if a federal crime has occurred, is occurring or will occur
- To determine if planning or preparation for a federal crime is taking place
- To obtain evidence
- To identify, locate and apprehend the perpetrators
- To identify threats to the national security
Duration of PIs

- Must be concluded within six months
- May be extended up to six months by the SAC (cannot be delegated, but an appropriately designated A/SAC may approve)
- Can be extended beyond one year by FBIHQ for "good cause"
"Good Cause" considerations:

- Has investigation revealed incriminating or exculpatory information?
- Has progress been made to determine if the PI should be closed or converted to FI?
- Will another six months reveal information to convert or close the PI?
- Is there predication now to convert or close PI?
Sensitive Investigative Matters

- Initiating a PI with a Sensitive Investigative Matter requires CDC review, SAC approval and written FBIHQ notification
- Must provide written notification to the USAO within 30 days of initiation
- must cease until CDC review and SAC approval is obtained
Sensitive Investigative Matters include investigations of:

- A domestic public official (corruption/national security)
- A political candidate (corruption/national security)
- A religious or political organization, or individual prominent in such
- Matters having an academic nexus
- News media
- Any other matter which should be brought to the attention of FBIHQ or DOJ, in the judgment of authorizing official
DIOG Section 6: Preliminary Investigations

**Authorized Investigative Methods in a PI**

All lawful methods may be used in a PI, except for mail opening, a Rule 41 search warrant or a FISA order, electronic surveillance requiring a judicial order or warrant, or Title VII FISA requests.

Authorized methods include, but are not limited to, those listed below:

- Obtain publicly available information
- Access and examine FBI and other DOJ records, and obtain information from any FBI or other DOJ personnel
- Access and examine records maintained by, and request information from, other federal, state, local, or tribal, or foreign governmental entities or agencies
Section 6: Preliminary Investigations

Authorized Investigative Methods (cont.)

- Use online services and resources (non-profit or commercial)
- Use and recruit CHS
- Interview or request information from members of the public and private entities
- Accept information voluntarily provided by governmental or private entities
- Engage in observation or surveillance not requiring a court order
- Grand Jury Subpoenas for telephone or electronic mail subscriber information
DIOG Section 6:
Preliminary Investigations

**Authorized Investigative Methods** (cont.)
- Mail covers
- Physical searches of personal or real property where a warrant or court order is not legally required because there is no reasonable expectation of privacy
- Consensual monitoring
- Use of closed-circuit television, direction finders, and other monitoring devices
- Polygraph examinations
- Undercover operations
Authorized Investigative Methods (cont.)

- Grand jury subpoenas, other subpoenas and National Security Letters
- Accessing stored wire and electronic communications and transactional records
- Pen registers and trap and trace devices
# DIOG Section 5 & 11: Investigative Methods

As of February 20, 2009

### Assessments

<table>
<thead>
<tr>
<th>Method</th>
<th>Preliminary Investigation</th>
<th>Full Investigation</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 recruit 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 request information from members of the public and private entities (includes pretextual interviews)</td>
<td>-</td>
<td>✔</td>
</tr>
<tr>
<td>Accept information voluntarily provided by governmental or private entities</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>Consentual monitoring of communications, including consentual computer monitoring, is subject to legal review by the CDC or the FBI OLC. 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.</td>
<td>-</td>
<td>✔</td>
</tr>
<tr>
<td>Use of closed-circuit television, direction finders, and other monitoring devices, subject to legal review by the CDC or FBI OLC.</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>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)</td>
<td>-</td>
<td>✔</td>
</tr>
<tr>
<td>Accessing stored wire and electronic communications and transactional records</td>
<td>-</td>
<td>✔</td>
</tr>
<tr>
<td>Use of pen registers and trap 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>
DIOG Section 6:
Preliminary Investigations

Prior to using a method, you must consider:

• Will the method further the investigation?
• Is the method the least intrusive and is it reasonable?
• Is it an appropriate use of personnel and resources?
DIOG Section 6:
Preliminary Investigations

Administration of a PI

• File reviews every 90 days (60 days for probationary agents)
• Conversion to a Full Investigation must be documented on a EC with SSA approval
• Conversion to a Full Investigation with a SIM requires CDC review, SAC approval and FBIHQ notification
Closing a PI

- Close PI via EC (SSA must ensure all leads and methods have been completed or terminated)
- EC must state the reason for closing
- SSA approval
- PI with a SIM requires SAC approval to close
• Your agent requests to open a PI?
• What action will you take?
• What action will you take?
PI Example
Overview:

The AGG-Dom authorizes a second level of investigative activity — predicated investigations. Predicated investigations that concern federal crimes or threats to the national security are subdivided into preliminary investigations and full investigations. Full investigations may be initiated if there is an “articulable factual basis” of possible criminal or national threat activity, as discussed in greater detail in Section 7.5, below. There are three types of full investigations: (i) single and multi-subject; (ii) enterprise; and (iii) positive foreign intelligence collection.
## DIOG Section 7: Full Investigations

<table>
<thead>
<tr>
<th>Investigation</th>
<th>Predication</th>
<th>Duration</th>
<th>Documentation</th>
<th>Approval</th>
<th>Justification Review</th>
<th>SIM</th>
<th>Responsible Entity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full</td>
<td>Initiated if there is an &quot;articulable factual basis&quot; that reasonably indicates circumstances described in DIOG Section 7.5 exist</td>
<td>No time limit; Factual predication determines outcome</td>
<td>EC</td>
<td>Prior SSA with FBIHQ (&amp; DOJ notice on NSB USPER matters)</td>
<td>Every 60 days; If probationary employee, every 60 days</td>
<td>CDC Review, SAC Approval, Notification to USAO or DOJ &amp; HQ within 33 days</td>
<td>Investigative Squad</td>
</tr>
</tbody>
</table>

As of May 19, 2009
Section 7:
Full Investigations

Predication to Open:

An articulable factual basis of that reasonably indicates one the following:

1. An activity constituting a federal crime or a threat to the national security has or may have occurred, is or may be occurring, or will or may occur and the investigation may obtain information relating to the activity or the involvement or role of an individual, group, or organization in such activity.
Predication to Open: an “articulable factual basis” of that reasonably indicates one of the following (cont):

2. An individual, group, organization, entity, information, property, or activity is or may be a target of attack, victimization, acquisition, infiltration, or recruitment in connection with criminal activity in violation of federal law or a threat to the national security and the investigation may obtain information that would help to protect against such activity or threat.

3. The investigation may obtain foreign intelligence that is responsive to a Positive Foreign Intelligence Requirement.
Standards for Initiating or approving a FI:

1. An authorized purpose and adequate predication exist
2. No investigative activity may be based solely on race, ethnicity, national origin, religion of the subject, or activities protected by the First Amendment
3. FI is an appropriate use of personnel and financial resources
DIOG Section 7: Full Investigations

- Approval Process:
  - The purpose and predication must be documented in the initiating EC, effective date when EC is approved
  - Requires prior SSA approval
  - Written notification to the FBIHQ substantive unit
    - A full investigation on a United States Person related to a National Security matter, FBIHQ Unit must notify DOJ NSD within 30 days
  - File Reviews
    - Every 90 days, probationary agents - 60 days
    - No LHM, unless required by substantive unit
DIOG Section 7: Full Investigations

- Investigative Methods
  - All methods from Preliminary Investigation plus:
    - Electronic Surveillance
    - Foreign Intelligence Collection Under Title VII and FISA
    - Physical Searches, mail openings with warrant or court order
  - Note re: Consensual Monitoring — in a state that requires two-party consent, the SAC must approve this as OIA under DIOG Section 17. Per DOJ policy, this OIA authority may be delegated to an ASAC or SSA — if done in writing.
DIOG Section 5 & 11: Investigative Methods

<table>
<thead>
<tr>
<th>Assessment</th>
<th>Preliminary Investigations</th>
<th>Full Investigations</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 recruit 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 request information from members of the public and private entities (includes pretextual interviews)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Accept information voluntarily provided by governmental or private entities</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 covers)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Consensual monitoring of communications, including consensual computer monitoring, is subject to legal review by the CDC or the FBI OGC. Where a sensitive monitoring circumstance is involved, monitoring must be approved by the Criminal Division or, if the investigation concerns foreign intelligence or a threat to the national security, by the National Security Division</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Use of closed-circuit television, direction finders, and other monitoring devices, subject to legal review by the CDC or FBI OGC</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>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)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Accessing stored wire and electronic communications and transactional records</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Use of pen registers and trap 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>
STANDARDS FOR INITIATING OR APPROVING USE OF AN INVESTIGATIVE METHOD IN A FI (prior to use):

1. The investigative method is likely to further the purpose of the FI
2. The investigative method is the least intrusive, reasonable under the circumstances
3. The method to be used is an appropriate use of personnel and financial resources.
DIOG Section 7
Full Investigations

Investigations are deemed "Sensitive Investigative Matters (SIMs)" when they involve activities of:

- A domestic public official (corruption or national security)
- A political candidate (corruption or national security)
- A religious or political organization, or individual prominent in such
- Matters having an academic nexus
- News media
- Any other matter which should be brought to the attention of FBIHQ or DOJ, in the judgment of authorizing official.
• **Sensitive Investigative Matter - Full Investigation:**
  
  - Requires CDC review, SAC approval and written notification to the appropriate FBIHQ substantive Unit Chief and Section Chief. EC must include Sensitive Investigative Matter in title.
  
  - If sensitive matter arises after the initiation of a full investigation, investigative activity must cease until CDC review, SAC approval, and proper notice to FBIHQ.
DIOG Section 7: Full Investigations

• Closing Full Investigations:
  - All investigative activity is exhausted
  - SSA must assure that all pending investigative methods have been completed/terminated (mail covers, pens etc.)

• Closing approvals
  - SSA with notification to FBIHQ substantive Unit
  - Closing SIMS
    • SAC approval with written notification to FBIHQ substantive Unit and Section
DIOG Section 7: Full Investigations

Examples:
Student Organization Scenario

What action would you take?
Student Organization Scenario

- Would you open an assessment?
Student Organization Scenario

- What action would you take?

-
Student Organization Scenario

• What action do you take?
Student Organization Scenario

- What action would you take?
Investment Fraud Example
Enterprise investigations may only be opened and operated as full investigations and are subject to the same requirements that apply to full investigations described in Section 7. Enterprise investigations focus on groups or organizations that may be involved in the most serious criminal or national security threats to the public, as described in Section 8.5 below. Enterprise investigations cannot be conducted as preliminary investigations or assessments, nor may they be conducted for the sole purpose of collecting positive foreign intelligence. See Section 8.2, below, regarding preliminary investigations and assessments.
**Field Office Investigations Chart**

<table>
<thead>
<tr>
<th>Investigation</th>
<th>Process</th>
<th>Duration</th>
<th>Documentation</th>
<th>Approval</th>
<th>Justification/Re-Test</th>
<th>Exit</th>
<th>Responsible Entity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type 1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Type 2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Type 3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Type 4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Type 5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Type 6</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Type 7</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Type 8</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**UNCLASSIFIED/FINAL**

As of May 10, 2009

ACLURM004378
### DIOG Section 8: Enterprise Investigations

<table>
<thead>
<tr>
<th>Investigation</th>
<th>Predication</th>
<th>Duration</th>
<th>Documentation</th>
<th>Approval</th>
<th>Justification Review</th>
<th>SIM</th>
<th>Responsible Entity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enterprise</td>
<td>Full</td>
<td>Investigation is predicated when there is an articulable factual basis for the investigation that reasonably indicates the group or organization is engaged in Racketeering, IT, DT, or other. See DIOG Section 8.4</td>
<td>No time limit; Factual predication determines outcome</td>
<td>EC</td>
<td>Every 60 days; if probationary employees, every 60 days</td>
<td>CDC Review, SAC Approval; Notification to USAO or DOJ &amp; HQ within 3E days</td>
<td>Investigative Squad</td>
</tr>
</tbody>
</table>
DIOG Section 8: Enterprise Investigations

- May only be opened as a full investigation
- Focus on groups or organizations that may be involved in the most serious criminal activities or national security threats to examine the structure and scope, and nature of the group including:
  - Relationship to a foreign power;
  - Identity and relationship of its members, employees, or persons who are acting in furtherance of its objectives;
  - Its finances and resources;
  - Its geographical dimensions;
  - Its past and future activities;
  - Its capacity for harm
DIOG Section 8: Enterprise Investigations

- Replaces the former REI and TEI investigations
- Includes any partnership, corporation, association or other legal entity, and any union or group of individuals associated, in fact although not a legal entity
- A PI may be used to determine whether a group/organization is an “Enterprise” – subject to the same requirements (for a PI)
DIOG Section 8: Enterprise Investigations

- Follow the same requirements as other predicated investigations
  - No investigative activity may be based solely on race, ethnicity, national origin, religion of the subject, or activities protected by the First Amendment
  - Must have articulable factual basis El is an appropriate use of personnel and financial resources
  - Must utilize least intrusive methods to obtain evidence and/or intelligence
Predication to Open:

The legal authority for an enterprise investigation is based on the predication wherein the group or organization may have engaged, or may be engaged in, or may have or may be engaged in planning or preparation or provision of support for the following:
DIOG Section 8: Enterprise Investigations

- International terrorism (AGG-Dom, Part VII.J, or other threat to the national security);
- Domestic terrorism (18 U.S.C. § 2331(5) involving a violation of federal criminal law;
- Furthering political or social goals wholly or in part through activities that involve force or violence and a violation of federal criminal law; or
# DIOG Section 8: Enterprise Investigations

<table>
<thead>
<tr>
<th><strong>Duration</strong></th>
<th>No time limit — as long as necessary to achieve purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Documentation</strong></td>
<td>EC</td>
</tr>
<tr>
<td><strong>Approval</strong></td>
<td>Prior SSA approval with FBIHQ and DOJ Notification (Counterterrorism division requires FBIHQ approval prior to SSA opening the EC)</td>
</tr>
<tr>
<td><strong>File Review</strong></td>
<td>Every 90 day period (Probationary Agents every 60 days)</td>
</tr>
<tr>
<td><strong>SIM</strong></td>
<td>CDC Review, SAC approval, and notification to USAO and FBIHQ within 30 days</td>
</tr>
<tr>
<td><strong>Responsible Entity</strong></td>
<td>Investigative squads</td>
</tr>
</tbody>
</table>
The following authorized investigative methods can only be used in full/enterprise investigations:

- Electronic Surveillance authorized by Title III, FISA, or Executive Order 12333
- Physical Searches, including Mail Openings, authorized by Rule 41, FISA, or Executive Order 12333
CLOSING AN ENTERPRISE INVESTIGATION:

1. SSA approval (if opened at HQ – Unit Chief) – SSA must ensure all investigative methods have been completed/terminated (CTD requires FBIHQ approval prior to SSA closing the EI)
2. Notice to FBIHQ Unit – UACB the EI is considered closed 30 days after notice to HQ (if opened at HQ – notice to FO)
3. If the EI involved a SIM, the SAC must approve the closing and written notification must be provided to FBIHQ Unit and Section (if initiated at HQ, Section Chief must approve – notice to FO) – UACB 30 days after HQ notice
DIOG Section 8: Enterprise Investigations

As an SSA, would you authorize an enterprise investigation if:

- 
- 
- 
- 

ID7E

ACLURM004388

ACLURM004388
Thank you...

SSA