DIOG Section 17: Otherwise Illegal Activity (OIA)

- Conduct in the course of duty by an FBI employee or CHS which constitutes a crime under local, state, or federal law if engaged in by a person without authorization to engage in that conduct.

- Applies to undercover activity and use of CHS
DIOG Section 17: OIA for CHS

- Must be approved in conformity with AGG-CHS and FBI's CHSPM
- Defined in CHS policy as either Tier I or Tier II activity
- Different approval levels
  - Tier I - DOJ/appropriate FPO or NSD Atty approval
  - Tier II - SAC approval
DIOG Section 17:
TIER I OIA

- Certain specified activity that would constitute a misdemeanor or felony under federal, state, or local law; and involves:
  - Commission of, or significant risk of, act of violence by persons other than by CHS
  - Corrupt conduct or significant risk of corrupt conduct by senior federal, state, or local public officials
  - Manufacturing, importing, exporting, possession, or trafficking of controlled substances (U.S.S.G.)
DIOG Section 17:
Tier I OIA

- Significant financial loss exceeding those specified in U.S.S.G. (Currently $1M)
- The provision to another person of
  - any item, service, or expertise necessary for a federal, state, or local offense that the person would otherwise have difficulty obtaining
  - any quantity of a controlled substance, explosive, firearm, or other weapon without expectation of its recovery
DIOG Section 17:
TIER II OIA

- Any other activity that would constitute a misdemeanor or felony under federal, state, or local law if engaged in by a person acting without authorization.

- NEW: includes consensual monitoring of communications in states where two-party consent required and a viable LE exception is not available. (CHSPM to be updated)
TIER II OIA Authorization

- Must be authorized in writing in advance for a specified period
- By SAC (CFP and SAC can agree on delegation)
- Not to exceed 90 days, but may be renewed
<table>
<thead>
<tr>
<th>DIOG Section 17: OIA PROHIBITIONS</th>
</tr>
</thead>
</table>

- FBI can never authorize a CHS to:
  - participate in an act of violence except in self-defense; or
  - participate in an act designed to obtain information for the FBI that would be unlawful if conducted by a law enforcement agent (illegal wiretaps, illegal searches, etc.)
DIOG Section 17: OIA for CHS

- CHSPM Provisions for
  - Emergency Authorization
  - Reporting requirements
  - Admonishments to CHS
  - Precautionary measures
  - Special notice requirements
  - Revocation of OIA approval
DIOG Section 17: OIA in UC ACTIVITY

- Criminal: Must be approved in conformity with AGG-UCO. If so approved, satisfies DIOG requirements
- Tier I/II approach not applicable
- Felony OIA will make case Group I UCO, but there are listed exceptions that may be approved as Group II UCO by SAC
DIOG Section 17:
OIA in UC Activity

- National Security / FI: Must be approved in conformity with AGG-Dom and DIOG
- DOJ/NSD is approving component for OIA beyond that authorized for an SAC in DIOG 17.5
DIOG Section 17:
OIA in UC Activity

• SAC Approval permitted for:
  – Misdemeanors
  – Consensual monitoring, even if a crime under state, local, or tribal law
  – Controlled purchase, receipt, delivery, sale of drugs, stolen property, contraband
  – Payment of bribes (but other FBI policy may limit amounts—consult CID PG)
DIOG Section 17:
OIA in UC Activity

- SAC Approval permitted (Cont.)
  - Making false representations as to personal identity or true ownership of a proprietary
  - Money Laundering not exceeding $1M
  - Special rules if OIA involves material support to terrorism, violation of export controls, or proliferation of WMD
DIOG Section 17: Consensual Monitoring of Communications as OIA

- Policy: For those state, local, and tribal governments that do not sanction or provide a viable LE exception for one party consent, the SAC must approve the consensual monitoring as OIA
  - One party consent must be first obtained
  - SAC authority to approve OIA regarding consensual monitoring is delegable to ASACs and SSAs

Teaching Point: The law of the state where the monitoring occurs will determine OIA. The SAC of the division where the CHS is operated will approve the OIA.
OIA Example

- In your office, your state law requires both parties consent to record telephone conversations. You task a CHS to place a consensually monitored telephone call to arrange a multi-kilo drug deal. The case agent brings you the FD-759 for your signature.
- Can you, as the SSA, approve the FD-759?

Teaching Point: The SSA can generally approve the FD-759 for consensual recordings in conjunction with CDC review. However, recording the telephone conversation is OIA because of the state law requirement of two party consent, and SAC approval is required. The SAC may delegate OIA authority to the ASAC or SSA. This written delegation must be done before this SSA can sign the FD-759. The FD-759 is currently under revision to include OIA approval authority.

Because this conversation involves the arrangement of a multi-kilo drug purchase, this would constitute a criminal activity which would require separate OIA authority to be approved per the CHSPM.

DIOG 17.5B An SAC may authorize the following Otherwise Illegal Activity (OIA) for an FBI employee when consistent with other requirements of this section, the AGG-UCO, and other FBI policy: B. Consensual monitoring of communications, even if a crime under state, local, or tribal law;

Note: For those state, local and tribal governments that do not sanction or provide a law enforcement exception available to the FBI for one-party consent recording of communications with persons within their jurisdiction, the SAC must approve the consensual monitoring of communications as an OIA. Prior to the SAC authorizing the OIA, one-party consent must be acquired.

Section 17.5.B permits the SAC to delegate authority to the ASAC or SSA. This written delegation must be done before this SSA can sign the FD-759.
OIA Example

- Your Field Office territory covers 4 states; two of which require two-party consent and the other two only require one-party consent to record conversations. Your CHS is directed to make a recorded telephone call from a one-party consent state to the subject in the two-party consent state.

- What approvals do you need?

- The CHS is now going to travel from the one-party consent state to the state which requires two-party consent to record conversations with a subject.

- What approvals do you need for consensual monitoring?

Teaching Point:
In first example, obtain CM approval. It is not considered OIA. In the second example, OIA approval is required.

OIA approval can be delegated in writing to the ASAC or SSA for CM.

Obtain OIA approval if there is a possibility the CHS travels to two-party states to record conversations.

DIOG 17.4 Because this involves a CHS and consensual monitoring, follow current CHS guidelines.

DIOG 17.5B An SAC may authorize the following Otherwise Illegal Activity (OIA) for an FBI employee when consistent with other requirements of this section, the AGG-UCO, and other FBI policy: B. Consensual monitoring of communications, even if a crime under state, local, or tribal law.

Note: For those state, local and tribal governments that do not sanction or provide a law enforcement exception available to the FBI for one-party consent recording of communications with persons within their jurisdiction, the SAC must approve the consensual monitoring of communications as an OIA. Prior to the SAC authorizing the OIA, one-party consent must be acquired.

Section 17.5.8 permits the SAC to delegate authority to the ASAC or SSA. This written delegation must be done before an SSA can sign the FD-759.

State where call is monitored controls OIA authorization.
OIA Example

- Your SAC has delegated his/her authority to approve OIA consensual recordings in your two-party state to the SSA. The SSA is on AL for the afternoon.
- Can the primary or secondary relief supervisor approve the FD-759 for a recording that will take place in a two-party consent state? Does it make a difference if the SSA is on a 90 day TDY?

Teaching Point: (OIA) DIOG Section 17.5.B permits the SAC to delegate authority to the ASAC or SSA. This written delegation must be done before an SSA or relief can sign the FD-759.

DIOG Section 3.4 C A supervisor may delegate authority to a supervisor one level junior to himself or herself, unless specified otherwise (e.g., the SAC may delegate authority to the ASAC).

The delegation to the SSA must be specific and in writing. The delegation EC should state to which position, primary or secondary relief supervisor, this authority is given. If the delegation EC also includes Acting SSAs and primary or secondary relief SSAs, then both could approve.

DIOG 17.5B An SAC may authorize the following Otherwise Illegal Activity (OIA) for an FBI employee when consistent with other requirements of this section, the AGG-UCO, and other FBI policy: B. Consensual monitoring of communications, even if a crime under state, local, or tribal law;

Note: For those state, local and tribal governments that do not sanction or provide a law enforcement exception available to the FBI for one-party consent recording of communications with persons within their jurisdiction, the SAC must approve the consensual monitoring of communications as an OIA. Prior to the SAC authorizing the OIA, one-party consent must be acquired.
**OIA Example**

- An agent wants to obtain OIA authority for a CHS to send money overseas to a known terrorist group for purposes of bolstering his credibility and position within the group he is trying to infiltrate.
- Can the SAC approve this OIA request?

**Teaching Point:** No, per the AGG-DOM (Part V.C.3) and DIOG (17.5.F).

**DIOG 17.5F** The SAC may not authorize an activity that may constitute material support to terrorism, a violation of export control laws, or violation of laws that concern proliferation of weapons of mass destruction. Such requests must be submitted to the HQ Substantive Division, who must obtain this approval from DOJ/NSD.

**Note:** New OIA Policy on material support EC dated 1/16/2009

This policy is effective immediately.

1. If funds, items, or services that will be provided to a subject as part of a national security investigation may constitute material support to terrorism, a Federal Bureau of Investigation (FBI) Assistant Director, with oral approval from the National Security Division (NSD), may authorize the provision of such funds, items, or services if their value does not exceed $2,000 per transaction and $10,000 per operation per year. The preceding sentence applies only if the goods or services are available to the general public and if the Assistant Director reasonably believes that the funds, items or services will not be used to pose an imminent significant threat to any individual.

2. NSD has represented that, except in exceptional circumstances, NSD shall act upon such an oral request within 24 hours and shall, within 72 hours, provide the FBI documentation of the authorization.
### DIOG Section 10: Sensitive Investigative Matter

- Investigations and Assessments are deemed "sensitive" when they involve activities of:
  - A domestic public official (corruption or nat'l security threat)
  - A political candidate (corruption or nat'l security threat)
  - A religious or political organization or individual prominent in such organization (as either a victim or the subject of the assessment or investigation)
  - 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

### Teaching Point:

Certain investigative matters should be brought to the attention of FBI management and DOJ officials because of the possibility of public notoriety and sensitivity. Accordingly, assessments and predicated investigations involving "sensitive investigative matters" have special approval and reporting requirements.

In the past, these terms have not been defined. In an effort to assist FBI employees in conducting assessments/predicated investigations involving a sensitive investigative matter, the following definitions are contained in the DIOG and, where applicable, have been approved by DOJ.

The language "involve activities of" in DIOG section 10 is broadly interpreted by FBI policy to include victim or subject. A religious or political organization or individual prominent in such organization (as either a victim or the subject of the assessment or investigation).
DOMESTIC PUBLIC OFFICIAL Defined:
An individual elected or appointed to a position of trust in a federal, state, local or tribal government entity or political subdivision thereof. A matter involving a domestic public official is a sensitive investigative matter if the assessment or predicated investigation involves corruption or a threat to the national security.

Teaching Point:
The definition of a domestic public official is broad (e.g., includes the local dog catcher, if elected). However, in order to be a sensitive investigative matter, the assessment or predicated investigation must involve a domestic public official who is involved in "corruption" or a "threat to the national security." Corruption and threat to the national security are defined in the next slide.
DIOG Section 10:
Sensitive Investigative Matter

• Corruption Defined:
  Typically involves payment of bribes, kickbacks or other things of value in exchange for official action or inaction with respect to the public official's duties.

• Threat to the National Security Defined:
  International terrorism; espionage and other intelligence activities, sabotage, and assassination, conducted by, for, or on behalf of foreign powers, organizations, or persons; foreign computer intrusion; and other matters determined by the Attorney General, consistent with E.O. 12333.

Teaching Point:
Accordingly, if the domestic public official is suspected of armed bank robbery, it would not be a sensitive investigative matter.
UNCLASSIFIED:

DIOG Section 10:
Sensitive Investigative Matter

- **Political Candidate Defined:**
  An individual who is seeking election to, or nomination for election to, or who has authorized others to explore on his or her behalf the possibility of election to, an office in a federal, state, local or tribal governmental entity or political subdivision thereof. As with domestic public officials, a matter involving a political candidate is a sensitive investigative matter if the assessment or predicated investigation involves corruption or a threat to the nation security.

Teaching Point:
Same rationale for a sensitive investigative matter applies to a political candidate.
• Political Organization or Individual Prominent is such an Organization Defined:

Teaching Point:
DIOG Section 10: Sensitive Investigative Matter

- Religious Organization or Individual Prominent in such an Organization Defined:
DIOG Section 10: Sensitive Investigative Matter

- Member of Media or News Organization Defined:
• Other Matters Defined:
  - Any matter that in the judgment of the official authorizing an investigation that should be brought to the attention of FBIHQ and other DOJ officials.
  - As a matter of FBI policy, "judgment" means the decision of the authorizing official is discretionary.

Teaching Point:
The FBI policy that "judgment" is discretionary is for the purpose of providing the authorizing official the ability to make such a decision based solely upon his/her judgment.
Teaching Point:
For the first condition to be a sensitive investigative matter, the administrator or faculty member must be involved in activity related to the individual's position at the college or university. For example, if a professor has child pornography on his home or office computer, this would not be a sensitive investigative matter because it is not related to his responsibilities at the university nor is it related to his position at the university.

Likewise, if a student organization is not "recognized and approved" by the institution, it is not a sensitive investigation matter.
Teaching Point:
These factors are considered in addition to the standards for approving the investigative activity such as:

1. An authorized purpose and objective/adequate predication exists for conducting/initiating the assessment/investigation;

2. The assessment/investigation is based on factors other than the exercise of First Amendment activities or the race, ethnicity, national origin or religion of the subject; and

3. The assessment/investigation is an appropriate use of personnel and financial resources.

Particular care should be taken when considering whether the planned course of action is the least intrusive method feasible.
Teaching Point:
Sensitive Investigative Matter developing after the initiation of the Assessment includes things such as: (i) tasking a CHS to acquire information involving the activities of a political organization even though the political organization, itself, is not the subject of the assessment.

Pursuant to DIOG Section 3.4.C., the SAC may delegate approval of sensitive investigative matter to the ASAC. Delegation must be in writing and appropriately retained. ASAC is not authorized to delegate this authority.

Pursuant to DIOG Section 3.5, CDC review may be performed by the Associate Division Counsel, Legal Advisor or designated Acting CDC. All CDC delegations must be made in writing and retained appropriately.
Sensitive Investigative Matter

- Types 3, 4, and 6 Assessments:

  If sensitive investigative matter circumstances are known to exist before initiating assessment, prior CDC review and SAC approval are required.

  If SIM circumstances develop after initiating assessment, investigative activities must stop until CDC review and SAC approval have been obtained.

  FBIHQ notification is not required.

  All Type 6 Assessments require prior FBIHQ CMS approval. If a sensitive investigative matter arises after initiation of Type 6 Assessment, notice must be provided to FBIHQ CMS.

Teaching Point:

For assessments initiated by FBIHQ that involve a sensitive investigative matter, OGC review and Section Chief approval is required. If a sensitive investigative matter arises after the initiation of an assessment, investigative activity must cease until OGC review and Section Chief approval is acquired.
DIOG Section 10: 
Sensitive Investigative Matter

- Predicated Investigations (Preliminary and Full):
  - Prior CDC review and SAC approval required
  - Written notification to the appropriate FBIHQ Unit Chief and Section Chief
  - Notice to United States Attorney's Office, if applicable
  - FBIHQ Section must provide written notification to DOJ Criminal Division or NSD no later than 30 calendar days after initiation
  - See DIOG

Teaching Point:
Notice must identify all known sensitive investigative matters involved in the investigation.

FBIHQ initiated predicated investigations involving a sensitive investigative matter required OGC review, Section Chief approval and written notification to the United States Attorney, DOJ Criminal Division or DOJ NSD no later than 30 days after initiation. If sensitive investigative matter arises after the initiation of the predicated investigation, investigative activity must cease until OGC review and Section Chief approval is acquired and notice is furnished.
DIQG Section 10:
Sensitive Investigative Matter

- Sensitive Monitoring Circumstance: Consensual monitoring of communications when a sensitive monitoring circumstance is involved requires approval by the DOJ Criminal Division or, if the investigation concerns foreign intelligence or a threat to the national security, by the DOJ National Security Division.

- A Sensitive Monitoring Circumstance includes electronic monitoring in an:
  - Investigation of a member of Congress, a federal judge, a member of the Executive Branch at Level IV or above, or a person having served in such capacity in the previous two years (continued on next slide)

Teaching Point:

Do not confuse a "sensitive investigative matter" with a "sensitive monitoring circumstance." "Sensitive monitoring circumstance" is only related to consensual monitoring.
DIOG Section 10: Sensitive Investigative Matter

- A sensitive monitoring circumstance includes (cont.):
  - Investigation of the governor, lieutenant governor, or attorney general of any state or territory, or a judge or justice of the highest court of any state or territory, concerning an offense involving bribery, conflict of interest, or extortion.
  - A party to the communications in the custody of the Bureau of Prisons or the U.S. Marshal Service or is being or has been afforded protection in the Witness Security Program.
  - Any occasion where the U.S. Attorney General, the Deputy Attorney General, or an Assistant Attorney General has requested the FBI to obtain prior approval for the use of consensual monitoring in a specific investigation.
SIM Example

- An investigative news reporter broadcasts a story alleging a candidate for United States Senate has been receiving kickbacks from a lobbyist.
- An investigative news reporter broadcasts a story alleging a candidate for city council has child pornography on his home computer.
- From a DIOG perspective, how do these two scenarios differ?

Teaching Point: The first scenario is considered a SIM because it is a matter involving a public official which involves corruption. It would also be a SIM if the matter was a threat to national security.

In the second scenario, even though the subject of the assessment/investigation is a political candidate, the alleged criminal matter does not concern corruption or a threat to national security thus may not be considered a Sensitive Investigative matter. (Consider informing SAC regardless)

Note: This is not a SIM due to the news media reporting because the investigation does not involve the activities of the news media organization.

10.2. Purpose, Scope and Definitions

A sensitive investigative matter is defined as an investigative matter involving the activities of a domestic public official or political candidate (involving corruption or a threat to the national security), religious or political organization or individual prominent in such an organization, or news media, or any other matter which, in the judgment of the official authorizing an investigation, should be brought to the attention of FBI Headquarters and other DOJ officials. (AGG-Dom, Part VII.N.) As a matter of FBI policy, "judgment" means that the decision of the authorizing official is discretionary.
SIM Example

- An anonymous caller states that a college student has child pornography on his computer in his fraternity house.
- An anonymous caller states that the Dean of Students at a local university has child pornography on his computer in his office.
- From a DIOG perspective, are either or both of these examples of SIMs?

Teaching Point:

DIOG Section 10.3: Factors to Consider When Initiating or Approving an Investigative Activity Involving a Sensitive Investigative Matter

In addition to the standards for approving investigative activity in Sections 5, 6, 7 and 9, the following factors should be considered by the: (i) FBI employee who seeks to initiate an assessment or predicated investigation involving a sensitive investigative matter; (ii) CDC or OGC when reviewing such matters; and (iii) approving official in determining whether the assessment or predicated investigation involving a sensitive investigative matter should be authorized:

A. Seriousness/severity of the violation/threat;
B. Significance of the information sought to the violation/threat;
C. Probability that the proposed course of action will be successful;
D. Risk of public exposure, and if there is such as risk, the adverse impact or the perception of the adverse impact on civil liberties and public confidence; and
E. Risk to the national security or the public welfare if the proposed course of action is not approved (i.e., risk of doing nothing). In the context of a sensitive investigative matter, particular care should be taken when considering whether the planned course of action is the least intrusive method feasible.
SIM Example

- During a routine US Dept of Education audit, it was discovered that a prominent university professor may have been embezzling funds from a federal grant.
- Does this example meet the standard of a SIM?

Teaching Point: SIM

DIOG 10.2 F
• Policy driven by EO 12333
• AGG-Dom required a UDP policy and AG approval of that policy
• FBI Policy seeks uniformity in National Security Investigations and Criminal investigations
• A risk management approach – the greater the risk, the higher the approval level
DIOG Section 16: Undisclosed Participation

Teaching Point:
DIOG Section 16: Undisclosed Participation

Participation:

Teaching Point:
Teaching Point:
Teaching Point:
DIQG Section 16:
Undisclosed Participation

Teaching Point:
DIOG Section 16: Undisclosed Participation
DIOG Section 16:
UDP Approval

• SEE HANDOUT CHART
Teaching Point:
DIOG Section 16:
Standards for Review and Approval
DIOG Section 16:
Standards for Review and Approval
Teaching Point:

DIOG 16.2.G -

DIOG 16.2.G -
Teaching Point: If it is determined that participation in the group is