



Public Affairs Guidance

POC: DAD Michael P. Kortan, [REDACTED] michael.kortan@ic.fbi.gov

b6
b7C

Issued as of 08/11/2008

Topic: Attorney General Guidelines for FBI Domestic Operations

Press Guidance:

Talking points and Q&As below are **for internal use only**. Any press inquiries related to this topic should be referred to the National Press Office, 202-324-3691, and to the Department of Justice (DOJ) Office of Public Affairs.

Issue:

DOJ is in the final stages of drafting the Attorney General's Guidelines for Domestic FBI Operations (AG-DOM). The week of August 11 DOJ and FBI officials will brief lawmakers and their staffs as well as civil liberties groups who will have an opportunity to voice any concerns and make suggestions for improvement. It is anticipated that the guidelines will be signed later this month and will be effective October 1, 2008.

The FBI is developing a comprehensive policy framework to implement the AG-DOM. This policy framework will include controls, checks, and oversight mechanisms to ensure full compliance with the guidelines and continued safeguarding of civil liberties and privacy rights.

The AGG-DOM will:

1. Replace 5 sets of guidelines with one uniform set of guidelines.
2. Set consistent rules for all domestic activities, regardless of whether the activity is motivated by a desire to thwart traditional criminal conduct, terrorism or counterintelligence activities.
3. Establish a category of conduct called "Assessments" which will permit the FBI to satisfy its intelligence mission in a way that respects civil liberties. Assessments are authorized for purposes of:
 - Prompt and extremely limited checking of leads (e.g., anonymous tip that X is a terrorist or drug dealer)
 - Assessing potential targets or vulnerabilities to criminal activity or threats to the national security (e.g., mapping the domain to see vulnerabilities and treats such as [REDACTED])
 - Obtaining information to inform actions of the FBI and to facilitate intelligence analysis and planning (e.g., gathering and analyze information regarding travel to areas in which there is terrorist training on-going).

b7E



- Matters of foreign intelligence (FI) interest that would be responsive to FI requirements.
- 4. Maintain traditional levels of investigation: Preliminary Investigations (investigation based on limited predication for a limited period of time with some investigative techniques not available); Full Investigations (investigations based on more compelling predication for an unlimited time with all investigative techniques available).
- 5. Rename Racketeering Enterprise Investigations as "Enterprise Investigations." Designed to permit long term investigations of groups that have an existence that continues beyond that of any group of members (e.g., Al Qaeda; La Cosa Nostra Families).

Talking Points:

- The new AG Guidelines are needed to:
 1. give the FBI a modern policy framework to help us operate in a modern threat environment in which criminal and national security matters often overlap; and
 2. enable the FBI to be more proactive, predictive, and preventative in fulfilling its mission.
- The FBI will implement the new AG Guidelines with a comprehensive policy framework that includes extensive controls and checks to ensure that civil liberties and privacy rights are protected. Policies are currently being drafted and may be revised to address any issues raised in briefings with civil liberties groups and/or Members of Congress.
- Consolidating the Guidelines into a consistent, clear, uniform set document that does not, through lack of clarity or rule differences, create a wall between national security and criminal investigations is critical to the transformation of the FBI.

Q&As:

What do the new guidelines cover?

The Attorney General's Guidelines for Domestic FBI Operations govern all FBI investigative and intelligence gathering activities conducted in the United States or outside the territories of all countries. Activities conducted inside foreign countries will be governed by the Attorney General's Guidelines for Extraterritorial FBI Operations.

What guidelines are being replaced?

The AGG-DOM will replace five existing sets of guidelines:

- The Attorney General's Guidelines on General Crimes, Racketeering Enterprise and Terrorism Enterprise Investigations (May 30, 2002)
- The Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection (October 31, 2003)



- The Attorney General's Supplemental Guidelines for Collection, Retention, and Dissemination of Foreign Intelligence (November 29, 2006)
- The Attorney General Procedure for Reporting and Use of Information Concerning Violations of Law and Authorization for Participation in Otherwise Illegal Activity in FBI Foreign Intelligence, Counterintelligence or International Terrorism Intelligence Investigations (August 8, 1988)
- The Attorney General's Guidelines for Reporting on Civil Disorders and Demonstrations Involving a Federal Interest (April 5, 1976)

When will the AGG-DOM be in effect?

The FBI expects to be operating under the new guidelines and our implementing policy on October 1, 2008.

Why are the new guidelines needed?

1. Having 5 different sets of guidelines causes irrational inconsistencies and undue complexity. Having one clear set of guidelines will help ensure consistency and compliance in the FBI's domestic operations.
 - If an agent looked to use an investigative technique, sometimes the rules governing criminal investigations would be more restrictive than the national security guidelines and sometimes less restrictive.
 - Because today's threats are intertwined and do not follow our programmatic boundaries, the FBI needs a uniform set of investigative rules, with the same definitions, approval and reporting requirements across all programs. This will eliminate the need for intelligence collectors and investigators to continuously decide which set of rules to follow in a particular situation.
2. Calls from Congress and Commissions to become an "intelligence agency" that is proactive and threat driven
 - The FBI has a mandate to stay ahead of threats and to be more predictive and preventative in executing its mission. Expectations are that we must intervene earlier and focus on disruption and dismantlement of threats in addition to investigating crimes and acts of terrorism after the fact.
 - It is not enough to wait for leads to come in and piece together intelligence from our cases. If we focus only on what we know we may fail to prevent the next terrorist attack, the next corporate fraud problem that may undermine confidence in the economy, or the violent gang starting to get a foothold in a new area. As an intelligence agency, we cannot and should not be solely driven by what we "know" from our cases; it is just as important to know what we do not know so that we can take efforts to fill in those knowledge gaps.
 - Allowing intelligence to drive our activities allows us to use our finite resources smarter; it may be, for example, that looking critically at intelligence and at



knowledge gaps, we can make a threat driven decision that some cases are simply not worth the resources they are absorbing.

- We need to be able to address needs for foreign intelligence policymakers require to conduct informed foreign relations. Among all agencies in the Intelligence Community, we are best positioned to gather such information in a way that is most respectful of US values.

What inconsistencies in the current rules will the AGG-DOM address?

Here are a few examples of inconsistencies found in our current guidelines and policy framework:

1. Different rules for national security and criminal investigations
 - The NSIG (governing all national security investigations) prohibited recruiting or tasking sources unless the FBI had at least a Preliminary Investigation open. The General Crimes Guidelines (GCG) contained no similar limitation.
 - The NSIG prohibited physical surveillance unless the FBI had at least a PI open, although it allowed information to be collected w/o an investigation through "casual observation". The GCG contained no similar limitation on physical surveillance.
 - The NSIG contained a prohibition on "pretext interviews" unless the FBI had at least a PI open. The GCG contained no similar limitation.
 - The rules on consensual monitoring were more restrictive in the criminal guidelines than in the NSIG.
 - The rules governing the "undisclosed participation" in legitimate organizations were addressed in the NSIG but not in GCG.
2. There are also differences in definitions that have the potential to cause confusion.
 - Example: The NSIG contained a clearly defined category of activity called a "threat assessment" during which non-intrusive info gathering and analysis could occur. The GCG contained no similarly defined category of activity. The GCG has a category of activity called "the prompt and limited checking of leads" which the NSIG does not have.

Are the new guidelines less restrictive overall?

1. In the FBI implementing policy being drafted, some things may be less restrictive and other things more restrictive – it depends on what set of rules a particular program was previously operating under. If an agent looked to use an investigative technique, sometimes the rules governing criminal investigations would be more restrictive than the national security guidelines and sometimes less restrictive.
2. Using a task force approach with participation by experienced Supervisory Special Agents from the field, and representing all investigative programs, the FBI is working



to develop implementing policies that will work for all programs and help us to fulfill our mandates, including protection of civil liberties.

What does the new policy framework look like for FBI domestic investigations?

At the top is the AGG-DOM. This is implemented across all programs and divisions in the Domestic Investigations and Operations Guide (DIOG), which will replace most of the existing Manual of Investigative Operations Guidelines. The DIOG is further implemented by individual program implementation guides. We expect the AGG-DOM and DIOG to be effective October 1, 2008, with program implementation guides effective December 1, 2008.

How will you educate the workforce and ensure everyone is in compliance with the new rules by October 1?

1. An aggressive training and communications strategy is planned to educate the workforce, including: mandatory web-based training, an employee town hall, user-friendly reference materials, communications tools kits for managers and Chief Division Counsels, and updates to the training curriculum for New Agents and Analysts as well as other in-service training.
2. Additionally, personnel will be able to easily locate and identify the applicable policy for a given situation through an indexed and searchable web-based portal on the FBI intranet – substantially reducing the likelihood of personnel relying on an outdated policy.

Why is there a rush for an October 1 implementation?

1. We are ready for the new guidelines and we need them. As the Director has described in recent testimony, the FBI has an aggressive effort underway to standardize and enhance our intelligence capabilities across the field. This effort will implement best practices in field office organization and functions through two-weeks of training in every field office, followed by a week of intermediate training, and “act/execute” projects with ongoing guidance and follow-up.
2. The October 1 implementation date will enable us to incorporate the new policy framework into this intelligence rollout and provide clear and consistent answers to agents’ and analysts’ questions – answers that do not differ based on the investigative program.
3. Also, the approval and reporting requirements in the policy framework being drafted will reflect the new standardized organization and work roles in field offices and the Directorate of Intelligence (for example, what is the authorization to collect intelligence to address a requirement and what investigative methods may be used?)

How will one set of guidelines work for diverse investigative programs?

To ensure the new policy framework works for all investigative programs, the drafting team includes managers from field offices and headquarters operational divisions, as well as attorneys from the Office of General Counsel, and personnel from the Corporate Policy Office. The AGG Task Force seeks input from each operational program through Division Policy Officers and attempts to reach consensus on the standardized rules to be



included. The Executive Assistant Directors meet with the task force weekly to resolve any areas of conflict.

What can the FBI do under the new guidelines that it could not do before?

The vast majority of the authorities outlined in the AGG are not new, but some techniques that were permissible under certain circumstances for criminal matters will now be available for national security matters as well, and vice versa.

1. Recruiting and tasking sources without an open PI, previously possible in criminal matters, will now be possible in an authorized assessment for national security matters as well (with all appropriate approvals).
2. Previously without a PI open, physical surveillance could be conducted in a potential criminal matter, but only "casual observation" could be used in a potential national security matter. Under the AGG-DOM, physical surveillance will be permissible in a properly authorized assessment (with all appropriate approvals).
3. Conducting a pretext interview without an open PI, previously possible in criminal matters, will now be possible in an authorized assessment for national security matters as well (with all appropriate approvals).

Is the ability to conduct an "assessment" – an investigation without factual predication – a new concept?

No, the concept is not new. The FBI has had authority to conduct "threat assessments" under the Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection, and the authority for "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. These authorities will be combined and simplified under the AGG-DOM in the new category called "Assessments," and the FBI is in the process of developing a comprehensive compliance and oversight regime to govern these activities.

What investigative methods can be used for an Assessment?

1. In a properly authorized Assessment, the FBI can:
 - Obtain publicly available information.
 - Access and examine FBI and DOJ records, and obtain information from any FBI or other Department of Justice personnel.
 - Request information from other federal, state, local, or tribal, or foreign governmental agencies.
 - Use online services and resources (whether nonprofit or commercial).
 - Use and recruit human sources
 - Interview or request information from members of the public and private entities.
 - Accept information voluntarily provided by governmental or private entities.
 - Conduct surveillance not requiring a court order.
2. Under the FBI's draft implementing policy, certain of these methods will require special levels of approval before they can be used in an assessment:



b7E

3. Methods not permitted in an assessment (except to vet or validate a CHS) include: electronic surveillance, physical searches, undercover operations, monitoring devices, consensual monitoring of communications, or any sort of compulsory process such as subpoenas and National Security Letters.

What controls are in place to ensure these new authorities are not abused?

1. The AGG-DOM contain several general statements of policy.
 - No investigation can be commenced based solely on ethnicity or the exercise of First Amendment rights.
 - The FBI should use the least intrusive method that is feasible under the circumstances.
 - In connection with Foreign Intelligence collection, agents should operate openly and overtly with US Persons if possible.
 - All activities must have an authorized and proper purpose. We interpret that to mean there has to be a purpose that is tied to an FBI mission.
2. There will be a strong regime of oversight from DOJ.
 - The oversight regime through mandatory reporting will be streamlined to focus on items of highest sensitivity (v. burying DOJ with reports).
 - On the national security side, the initiation of full investigations of US persons must be reported to DOJ.
 - All investigations with "sensitive circumstances" must be reported to DOJ. "Sensitive circumstances" means a matter involving a domestic public official, a political candidate, a religious or political organization or a person prominent in such organization or the media.
 - The initiation of enterprise investigations must be reported to DOJ (either OCRS or NSD, as appropriate).
 - The initiation of all investigations to collect foreign intelligence must be reported to the NSD. Thereafter, FBI must report annually on foreign intelligence collection matters. [Pure FI, not CI or CT matters.]



Federal Bureau of Investigation
Office of Public Affairs
National Press Office

- Assistance to foreign agencies if the assistance is of a nature that requires FBI HQ approval (those approval levels not set; will likely be required if techniques beyond assessment techniques are used).
3. Other DOJ oversight
- Traditional oversight of criminal matters continues to come through the relationship between FBI and US Attorney's Offices.
 - DOJ is generally permitted to seek information on any investigation or group of investigations as it sees fit.
 - Consensual monitoring in "sensitive monitoring circumstances" must be approved by DOJ. "Sensitive monitoring circumstances" includes, among others, consensual monitoring of high level federal officials and high level state officials.
 - "National Security Reviews" conducted jointly by DOJ's National Security Division and FBI-OGC. These grew out of the NSL situation, but the scope of the review is much broader and is intended to provide oversight of those investigations that would not likely have USAO involvement.
 - Office of Inspector General is always available with helpful reviews, audits and recommendations.
4. FBI Policy - The FBI will implement the new AG Guidelines with a comprehensive policy framework that includes extensive controls and checks to ensure that civil liberties and privacy rights are protected.
- Policies are still being drafted, but the overarching theme is to use risk analysis to govern approval levels (higher the risk either of the subject matter or the technique, the higher the level of required review). Examples follow:
 - Searching public or government data bases – low risk; no supervisor approval required
 - Conducting surveillance without sensitive circumstances during an assessment – higher risks; approval required.
- [REDACTED]
- [REDACTED] much higher risk; much higher approval levels.
5. The FBI is putting in place a framework of approvals, reporting, recordkeeping, and strong oversight to govern Assessments. There are control mechanisms at all levels.

b7E



Federal Bureau of Investigation
Office of Public Affairs
National Press Office

- Office of General Counsel is heavily involved with both the compliance efforts and with identifying areas where there may be confusion regarding the rules.
 - The new Sensitive Operations Review Committee (SORC) will provide for SES-level reviews of highly sensitive matters.
6. Congressional controls through oversight will continue.

The new domestic guidelines appear to eliminate the requirement for any predication or factual basis for a new category of FBI investigation—called an “assessment,” which only requires a “proper purpose.” Doesn’t this mean that the FBI can investigate anyone or any group in the U.S. without any factual basis to believe they are connected to crime or terrorism—as long as it is done for the right reason? If so, doesn’t this guidance return the FBI to the days of COINTELPRO when they could spy on Americans for purely political purposes?

NO. There are many safeguards within and outside the new guidelines that would prevent any return to the conduct that was permitted in the days of COINTELPRO. Here are some of them:

1. An assessment only permits the use of a limited list of investigative methods for the purposes of either assessing the validity of an allegation or “lead” or, on a pro-active basis, filling national intelligence requirements or determining the existence or absence of a criminal or national security threat or vulnerability. Persons and groups are not targeted and investigated in the traditional sense in an assessment. Allegations, threats, and vulnerabilities are examined and national intelligence requirements are filled. If the results of an assessment provide the factual predication to investigate a specific person or a group of persons, a criminal or national security investigation must be opened and pursued if the predication meets the standard set forth in the guidelines. If, on the other hand, an assessment reveals no basis to investigate a person or a group, then the matter is closed.
2. The techniques available in an assessment are geared to the gathering of publicly available information, information in government databases, or information known or lawfully obtained by human sources who are familiar with the matter being assessed. More intrusive techniques such as electronic surveillance, the use of search warrants and National Security Letters, undercover infiltration, and counter-intelligence tactics will not be permitted. Some of these techniques were used in COINTELPRO to gather intelligence—they will not be used in an assessment.
3. Since the days of COINTELPRO, the legal landscape has changed considerably. Today, law enforcement and intelligence collection activity by federal agencies must comply with the Privacy Act, the Federal Wiretap Act, the Foreign Intelligence Surveillance Act, the Right to Financial Privacy Act, the Electronic Communications Privacy Act, the Fair Credit Reporting Act, the Family Educational Records Privacy Act, the Bank Secrecy Act, the E-Government Act and a host of federal regulations and policies—all of which are still in full effect and none of which have been diminished in any way by these new guidelines. In addition, a considerable body of federal case law has matured over the past 35 years interpreting constitutional and statutory authorities which binds the FBI’s activities. Internal FBI policies and training are geared to reflect this legal landscape.



4. Two other new standards have emerged since the 1970's that are built into these new guidelines that are pertinent to this discussion:
 - No investigative activity can be conducted, and no record can be maintained, solely on the basis of a person's exercise of rights guaranteed by the First Amendment to the Constitution; and
 - No investigative activity can be conducted, and no record maintained solely, on the basis of race or ethnicity.
5. The new guidelines—like prior versions but unlike the COINTELPRO time period—contains other safeguards that are designed to protect privacy and civil liberties. These include higher approval levels and standards for investigative activity that involves what are described as “sensitive circumstances.” These circumstances include investigative activity that involves, to any degree, political, social or religious groups engaged in the exercise of First Amendment rights. A key safeguard is the requirement for a legal review by trained counsel who examines the justification for the activity, whether there are less intrusive investigative alternatives available, and whether are mitigation steps that can be taken to lessen the risk of affecting the rights of members of the public.
6. The training of new agents and analysts has evolved to include considerable emphasis on the protection of privacy and civil liberties.
7. Oversight provisions (see above)

What level of approval will be required for the FBI to conduct an assessment of a political or religious group?

No assessment, or any other type of investigative activity, can be undertaken based solely on activities protected by the First Amendment. In an instance where there is information such as a specific threat lead indicating that a group may pose a threat of violence, an assessment may be permissible, but it is safe to say that such an activity would require the highest level of scrutiny.

Does the AGG-DOM allow the FBI to conduct Assessments based on speculation?

No. The guidelines expressly state that the basis of any assessment must not be arbitrary or groundless speculation. Furthermore, there must be a rational and articulable relationship between the stated purpose of the assessment on the one hand and the information sought and the proposed means to obtain that information on the other. Management is responsible for assuring that assessments are not pursued for frivolous or improper purposes.

Is the FBI permitted to map mosques or other religious institutions?

1. The FBI cannot map a religious institution solely because it is a religious institution.
2. Pursuant to existing guidelines and the AGG-DOM, if the FBI has an open assessment, preliminary or full investigation, investigators or analysts can geo locate a facility



[REDACTED] However, the practice of religion is protected by the First Amendment and therefore cannot be the basis of any intelligence collection or analysis unless there are additional factors indicating a threat or vulnerability.

Is the FBI permitted to map racial or ethnic groups?

Under the DOJ Guidance Regarding the Use of Race by Law Enforcement Agencies, investigative activity (including collection of domestic intelligence) may not be based solely on racial or ethnic characteristics. Therefore, collecting information about—and mapping the locations of—racial or ethnic communities may not be conducted on that basis alone. There must be a valid law enforcement or national security basis for such collection. In practical terms, that means the collection must be based on the need to determine threats, vulnerabilities, and intelligence gaps in the domain and must be for one of the purposes for which an assessment is authorized under the guidelines. Documentation to justify such a collection under the assessment investigative category should include the basis for the collection and reflect a rational relationship between the threat or vulnerability to be assessed and the information to be collected.

Do the new guidelines allow the FBI to conduct data mining?

1. The vast majority of data analysis performed during FBI predicated investigations is based on subjects or events and do not meet the definition of pattern-based data mining.
2. Pattern-based data mining, defined as the use of one or more data bases to search for persons who fit a set of group characteristics or patterns of behavior (e.g., the known characteristics of a particular terrorist organization) is permitted under strict controls.
 - Any such analysis based solely on ethnic or racial characteristics is strictly prohibited.
 - SORC approval is required.
 - The FBI must report all initiatives that involve the use of pattern-based data mining to Congress.

What is required for SORC approval?

Details regarding the SORC are still being worked out, but tentatively:

1. A majority of the SORC must approve an operation before it can go forward.
2. The SORC will only approve an operation upon findings that: (1) the potential benefits to the national security or public welfare are significant; (2) the proposed course of action is necessary to achieve those benefits and is otherwise appropriate under the circumstances; (3) all reasonable mitigation measures have been considered and imposed; and (4) the anticipate benefits outweigh any risks to civil liberties, privacy, or other rights that may be affected.

How is the requirement to use the "least intrusive means" enforced?



Federal Bureau of Investigation
Office of Public Affairs
National Press Office

1. FBI policy will specify the level of approval required for each type of investigative method. The more intrusive the method, the higher level of approval is required. Supervisors, managers, and executives will be responsible for applying the appropriate standard in making the decision to approve or deny use of a particular method.
2. General controls being put in place, including reporting requirements to facilitate auditing to ensure that personnel adhere to the requirement.

If the AGG-DOM were in effect in 2001, how would they have helped the FBI prevent the 9/11 attacks?

Prior to 9/11, an agent in Phoenix noted that there were a number of Middle Eastern males in flight schools. Suppose, instead, that an agent notices lots of Middle Eastern males taking scuba lessons and there is some intelligence that Al Qai'ida is plotting something involving underwater attacks.

1. Being foreign and taking SCUBA lessons is not and should not be sufficient predication to open a preliminary investigation.
2. New guidelines would allow the following proactive steps:



b7E

AGG/FBI POLICY FAQs

What do the new guidelines cover?

The Attorney General's Guidelines for Domestic FBI Operations (AGG-DOM) govern all FBI investigative and intelligence gathering activities conducted in the United States or outside the territories of all countries. Activities conducted inside foreign countries are governed by the Attorney General's Guidelines for Extraterritorial FBI Operations.

What guidelines are being replaced?

These guidelines are expected to replace five existing sets of guidelines:

- The Attorney General's Guidelines on General Crimes, Racketeering Enterprise and Terrorism Enterprise Investigations (May 30, 2002)
- The Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection (October 31, 2003)
- The Attorney General's Supplemental Guidelines for Collection, Retention, and Dissemination of Foreign Intelligence (November 29, 2006)
- The Attorney General Procedure for Reporting and Use of Information Concerning Violations of Law and Authorization for Participation in Otherwise Illegal Activity in FBI Foreign Intelligence, Counterintelligence or International Terrorism Intelligence Investigations (August 8, 1988)
- The Attorney General's Guidelines for Reporting on Civil Disorders and Demonstrations Involving a Federal Interest (April 5, 1976)

When will the AGG-DOM be in effect?

The FBI will be operating under the new guidelines and our implementing policy on October 1, 2008.

What does the new policy framework look like for FBI domestic investigations?

At the top is the AGG-DOM. This is implemented across all programs and divisions in the Domestic Investigations and Operations Guide (DIOG), which will replace most of the existing Manual of Investigative Operations Guidelines. The DIOG is further implemented by individual program implementation guides. The AGG-DOM and DIOG are effective October 1, 2008. The program implementation guides will be effective December 1, 2008.

How will you educate the workforce and ensure everyone is in compliance with the new rules by October 1?

An aggressive training and communications strategy is planned to educate the workforce, including: mandatory web-based training, an employee town hall, user friendly reference materials, communications tools kits for managers and Chief Division Counsels, and updates to the New Agents and Analysts training curriculum as well as other in-service training.

Additionally, personnel will be able to easily locate and identify the applicable policy for a given situation through an indexed and searchable web-based portal on the FBI intranet – substantially reducing the likelihood of personnel relying on an outdated policy.

What can the FBI do under the new guidelines that it could not do before?

The vast majority of the authorities outlined in the AGG are not new. The authority to conduct “threat assessments” previously found in the Attorney General’s Guidelines for FBI National Security Investigations and Foreign Intelligence Collection and the authority for “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 are combined in the new category called “Assessments.” There are two key techniques that will now be available for Assessments that were not available under the previous guidelines:

- Previously, the FBI could not recruit and task a source without factual predication of a federal crime or national security threat justifying a Preliminary or Full Investigation. Under the new guidelines [REDACTED] even if there is no specific factual predication. b7E
- Previously, the FBI could not conduct physical surveillance without factual predication of a federal crime or national security threat. Under the new guidelines, physical surveillance can be conducted for a proper purpose. Electronic surveillance is not permissible without factual predication.
- The use of these techniques is necessary to:
 - more quickly and thoroughly track down leads
 - expand and strengthen [REDACTED]
 - make better use of existing sources (know what we *could* know)

What investigative methods can be used for an Assessment?

In a properly authorized Assessment, the FBI can:

1. Obtain publicly available information.
2. Access and examine FBI and DOJ records, and obtain information from any FBI or other Department of Justice personnel.
3. Request information from other federal, state, local, or tribal, or foreign governmental agencies.
4. Use online services and resources (whether nonprofit or commercial).
5. Use and recruit human sources
6. Interview or request information from members of the public and private entities.
7. Accept information voluntarily provided by governmental or private entities.
8. Conduct surveillance not requiring a court order.

What controls are in place to ensure these new authorities are not abused?

1. The FBI is putting in place a framework of approvals, reporting, recordkeeping, and strong oversight to govern Assessments. There are control mechanisms at all levels.

Additional internal controls include:

-
-
-
-
-
-

b7E

2. External controls include:
 - Congressional Oversight
 - Oversight by DOJ's National Security Division Oversight Section, Office of Intelligence Policy and Review, Intelligence Oversight Board, U.S. Attorneys, and Inspector General.
3. Legal protections include:
 - The Foreign Intelligence Surveillance Act of 1978
 - The Whistleblower Protection Acts of 1989 and 1998
 - The Freedom of Information Act of 1966
 - The Privacy Act of 1974

Isn't this a return to COINTELPRO?

No. The sorts of activities for which the FBI was criticized in COINTELPRO are not permitted. And to ensure there is no ambiguity, FBI policy is being developed with a regime of controls to ensure abuses do not occur.

What prevents the FBI from conducting surveillance of legitimate organizations and minority groups?

1. The guidelines allow for the use of physical surveillance in a Preliminary or Full investigation, or in an Assessment., but like all investigative activities, physical surveillance cannot be conducted based on speech or activities protected by the First Amendment.
2. Draft FBI policy would require review by the Chief Division Counsel and approval by the Special Agent in Charge, before surveillance could be conducted on a political, minority, religious, or university group. Additional notice to FBIHQ is also required for most Assessments (except for tracking leads) and notice to DOJ is required before a

When will an assessment of a political group be approved?

1. As with all Assessments, there must be an authorized purpose that is not based on activities protected by the First Amendment. Additional scrutiny is applied before an Assessment may be undertaken to look into a political, religious, news media, or university organization. The Chief Division Counsel must review and the SAC approve the initiation of such an Assessment.
2. The CDC will examine: the seriousness/severity of the violation or threat; significance of the information sought to the violation or threat; probability that the proposed course of action will be successful; risk of public exposure and possible adverse impact on civil liberties and public confidence; and risk to the national security or public welfare if the proposed course of action is not approved (i.e. the risk of doing nothing.)
3. It is also a requirement to notify the appropriate FBIHQ Section Chief and Unit Chief, the U.S. Attorney or DOJ Criminal Division or National Security Division. This is for oversight purposes.

What prevents the FBI from infiltrating legitimate organizations and minority groups?

1. Undercover operations not permitted for Assessments, nor can Agents task a Confidential Human Source to do something they could not do themselves.
2. Use of undercover operations and/or the use of Confidential Human Sources are permissible for Preliminary and Full investigations with appropriate supervisor approval. However, FBI policy will allow for

b7E

Does the AGG-DOM allow the FBI to conduct Assessments based on speculation?

No. The guidelines expressly state that the basis of any assessment must not be arbitrary or groundless speculation. Furthermore, there must be a rational and articulable relationship between the stated purpose of the assessment on the one hand and the information sought and the proposed means to obtain that information on the other. Management is responsible for assuring that assessments are not pursued for frivolous or improper purposes.

What prevents the FBI from intruding into the protected First Amendment right of association?

1. The collection of information concerning groups and individuals must be justified as reasonable and necessary for investigative purposes.
2. Information concerning the exercise of First Amendment rights should be made a matter of record only if it is pertinent to and within the scope of the authorized law enforcement activity.

b7E

What prevents the FBI from planting seeds of disruption in legitimate groups?

Is the FBI permitted to map mosques or other religious institutions?

1. The FBI cannot map a religious institution solely because it is a religious institution. The practice of religion is protected by the First Amendment and therefore cannot be the basis of any intelligence collection or analysis unless there are additional factors indicating a threat or vulnerability.
2. The collection of any data must have an authorized purpose, such as tracking a threat lead or analysis and planning.

Do the new guidelines allow the FBI to conduct data mining?

1. The vast majority of data analysis performed during FBI predicated investigations is based on subjects or events and do not meet the definition of pattern-based data mining.
2. Pattern-based data mining, defined as the use of one or more data bases to search for persons who fit a set of group characteristics or patterns of behavior, is permitted under strict controls.
 - Any such analysis based solely on ethnic or racial characteristics is strictly prohibited.

b7E

What is required for SORC approval?

1. A majority of the SORC must approve an operation before it can go forward.
2. The SORC will only approve an operation upon findings that: (1) the potential benefits to the national security or public welfare are significant; (2) the proposed course of action is

necessary to achieve those benefits and is otherwise appropriate under the circumstances; (3) all reasonable mitigation measures have been considered and imposed; and (4) the anticipate benefits outweigh any risks to civil liberties, privacy, or other rights that may be affected.

How is the requirement to use the “least intrusive means” enforced?

1. FBI policy will specify the level of approval required for each type of investigative method. The more intrusive the method, the higher level of approval is required. Supervisors, managers, and executives will be responsible for applying the appropriate standard in making the decision to approve or deny use of a particular method.
2. General controls being put in place, including reporting requirements to facilitate auditing will ensure that personnel adhere to the requirement.

DOMESTIC INVESTIGATIONS AND OPERATIONS GUIDE FREQUENTLY ASKED QUESTIONS

I. GENERAL OVERVIEW	1
A. AG Guidelines for Domestic Operations	1
B. DIOG Scope and Organization	2
C. Justification and Impact	4
D. Safeguarding Civil Liberties	6
E. Key Terminology	12
II. INVESTIGATIONS AND INTELLIGENCE GATHERING	13
A. Overview	13
B. Assessments	14
C. Preliminary Investigations	18
D. Full Investigations	20
E. Foreign Intelligence	21
F. Enterprise Investigations	23
G. Sensitive Investigative Matters	24
H. Undisclosed Participation	27
III. INFORMATION SHARING	27
IV. DOCUMENTATION AND RECORD KEEPING	28
V. IMPLEMENTING THE STRATEGIC EXECUTION TEAM (SET) INITIATIVES	29
A. Domain	30
B. Collection and Requirements	31
C. HUMINT	32
VI. TRANSITION	33

I. GENERAL OVERVIEW

A. AG Guidelines for Domestic Operations

What do the new guidelines cover?

The Attorney General's Guidelines for Domestic FBI Operations (AGG-Dom) govern all FBI investigative and intelligence gathering activities conducted in the United States or outside the territories of all countries. Activities conducted inside foreign countries are governed by the Attorney General's Guidelines for Extraterritorial FBI Operations.

What guidelines are being replaced?

The AGG-Dom replaces five sets of guidelines:

- The Attorney General's Guidelines on General Crimes, Racketeering Enterprise and Terrorism Enterprise Investigations (May 30, 2002)
- The Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection (October 31, 2003)

- The Attorney General's Supplemental Guidelines for Collection, Retention, and Dissemination of Foreign Intelligence (November 29, 2006)
- The Attorney General Procedure for Reporting and Use of Information Concerning Violations of Law and Authorization for Participation in Otherwise Illegal Activity in FBI Foreign Intelligence, Counterintelligence or International Terrorism Intelligence Investigations (August 8, 1988)
- The Attorney General's Guidelines for Reporting on Civil Disorders and Demonstrations Involving a Federal Interest (April 5, 1976)

When will the AGG-DOM be in effect?

The FBI will be operating under the new guidelines and our implementing policy on October 1, 2008.

What does the new policy framework look like for FBI domestic investigations?

At the top is the AGG-Dom. This is implemented across all programs and divisions in the Domestic Investigations and Operations Guide (DIOG), which replaces most of the existing Manual of Investigative Operations Guidelines (MIOG). The DIOG is further implemented by individual program implementation guides. The AGG-Dom and DIOG are effective October 1, 2008. The program implementation guides will be effective December 1, 2008.

What can the FBI do under the new guidelines that it could not do before?

The vast majority of the authorities outlined in the AGG are not new, but some techniques that were permissible under certain circumstances for criminal matters will now be available for national security matters as well, and vice versa.

1. Recruiting and tasking sources without an open PI, previously possible in criminal matters, will now be possible in an authorized assessment for national security matters as well (with all appropriate approvals).
2. Previously without a PI open, physical surveillance could be conducted in a potential criminal matter, but only "casual observation" could be used in a potential national security matter. Under the AGG-Dom, physical surveillance will be permissible in a properly authorized assessment (with all appropriate approvals).
3. Conducting a pretext interview without an open PI, previously possible in criminal matters, will now be possible in an authorized assessment for national security matters as well (with all appropriate approvals).

B. DIOG Scope and Organization

What is the DIOG and what does it cover?

The Domestic Investigations and Operations Guide (DIOG) is a policy implementation manual which outlines how FBI will carry out domestic operations under the new AGG-Dom.

What parts of the MIOG are superseded by the DIOG?

- Significant portions of the MIOG are superseded by the DIOG. Other portions of the MIOG will be superseded by individual program implementation guides. Those portions of the MIOG that are not impacted will be updated over time as part of the Corporate Policy Office's MIOG re-write plan.
- If you access a policy of guidance through the Corporate Policy Office's policy portal you can be assured that what you are seeing is the guidance now in effect, so it is not necessary to study a side-by-side comparison.

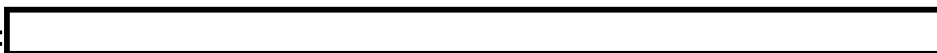
How is the DIOG organized?

The first four sections of the DIOG discuss the scope; core values, roles, and responsibilities; general authorities and principles; and privacy and civil liberties. The next five sections cover types of investigations: Assessments, Preliminary Investigations, and Full Investigations. There are special sections on foreign intelligence and enterprise investigations. The remaining sections cover: Sensitive Investigative Matters, Investigative Methods, Interviews, Undisclosed Participation, Assistance to Other Agencies, Retention and Sharing of Information, and Strategic Analysis and Planning.

Where can I find the DIOG?

The DIOG can be found on the FBI intranet at the Corporate Policy Office's central policy portal. There you will also find links to supporting documents, job-aids, communications, and related implementing program policies.

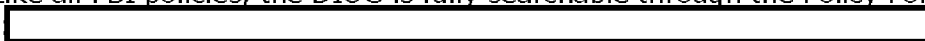
Here is a link:



I have a question, but don't know what section of the DIOG will have the answer. How do I find what I'm looking for?

b7E

Like all FBI policies, the DIOG is fully searchable through the Policy Portal on the intranet



When will the DIOG be implemented?

The FBI will be operating under the new guidelines on by October 1, 2008.

Will I receive training on the DIOG?

Yes, there will be a Virtual Academy course on the AGG-Dom and another on the DIOG. In addition, you may receive a briefing from your CDC and/or supervisor.

My investigative program has not issued policy for implementing the DIOG. How do I know what rules to follow?

1. If you go to the Policy Portal and do a search or look through the index you will find the applicable policy. The Corporate Policy Office (CPO) is responsible for ensuring that the policy currently in effect is on the portal. As the program implementation guides supersede old sections of the MIOG, the CPO will make the changes and the Portal will take you to the new policy.

2. Program policies cannot contradict the DIOG, but they can add additional requirements consistent with the DIOG and/or add clarification on definitions and procedures (ex. what constitutes "notice" for a particular program.)

How was the DIOG developed?

1. A team consisting of attorneys from the Office of General Counsel, personnel from the Corporate Policy Office, and experienced SSAs from field offices and headquarters, was assembled to draft clear policy on how the new Attorney General Guidelines will be implemented in the FBI. The AGG Task Force sought input from each operation program through division policy officers and worked hard to reach consensus on the standardized rules to be included.
2. All key decision points were presented to the EADs for final decision.
3. Additionally, personnel from the Office of Integrity and Compliance, the Training Division, and Employee Communications developed a strategy to communicate the new policies to the workforce, to provide appropriate training, and to ensure compliance mechanisms are established.

C. Justification and Impact

Why are the new guidelines needed?

1. Having 5 different sets of guidelines causes irrational inconsistencies and undue complexity. Having one clear set of guidelines will help ensure consistency and compliance in the FBI's domestic operations.
 - If an agent looked to use an investigative technique, sometimes the rules governing criminal investigations would be more restrictive than the national security guidelines and sometimes less restrictive.
 - Because today's threats are intertwined and do not follow our programmatic boundaries, the FBI needs a uniform set of investigative rules, with the same definitions, approval and reporting requirements across all programs. This will eliminate the need for intelligence collectors and investigators to continuously decide which set of rules to follow in a particular situation.
2. Calls from Congress and Commissions to become an "intelligence agency" that is proactive and threat driven
 - The FBI has a mandate to stay ahead of threats and to be more predictive and preventative in executing its mission. Expectations are that we must intervene earlier and focus on disruption and dismantlement of threats in addition to investigating crimes and acts of terrorism after the fact.
 - It is not enough to wait for leads to come in and piece together intelligence from our cases. If we focus only on what we know we may fail to prevent the next terrorist attack, the next corporate fraud problem that may undermine confidence in the economy, or the violent gang starting to get a foothold in a new area. As an intelligence agency, we cannot and should not be solely driven by what we

“know” from our cases; it is just as important to know what we do not know so that we can take efforts to fill in those knowledge gaps.

- Allowing intelligence to drive our activities allows us to use our finite resources smarter; it may be, for example, that looking critically at intelligence and at knowledge gaps, we can make a threat driven decision that some cases are simply not worth the resources they are absorbing.
- We need to be able to address needs for foreign intelligence policymakers require to conduct informed foreign relations. Among all agencies in the Intelligence Community, we are best positioned to gather such information in a way that is most respectful of US values.

What inconsistencies in the current rules will the AGG-Dom address?

Here are a few examples of inconsistencies found in our previous guidelines and policy framework:

1. Different rules for national security and criminal investigations
 - The NSIG (governing all national security investigations) prohibited recruiting or tasking sources unless the FBI had at least a Preliminary Investigation open. The General Crimes Guidelines (GCG) contained no similar limitation.
 - The NSIG prohibited physical surveillance unless the FBI had at least a PI open, although it allowed information to be collected w/o an investigation through “casual observation”. The GCG contained no similar limitation on physical surveillance.
 - The NSIG contained a prohibition on “pretext interviews” unless the FBI had at least a PI open. The GCG contained no similar limitation.
 - The rules on consensual monitoring were more restrictive in the criminal guidelines than in the NSIG.
 - The rules governing the “undisclosed participation” in legitimate organizations were addressed in the NSIG but not in GCG.
2. There were also differences in definitions with potential to cause confusion.
 - Example: The NSIG contained a clearly defined category of activity called a “threat assessment” during which non-intrusive info gathering and analysis could occur. The GCG contained no similarly defined category of activity. The GCG has a category of activity called “the prompt and limited checking of leads” which the NSIG does not have.

Are the new guidelines less restrictive overall?

1. In the FBI implementing policy (the DI OG), some things may be less restrictive and other things more restrictive – it depends on what set of rules a particular program was previously operating under. If an agent looked to use an investigative technique,

sometimes the rules governing criminal investigations would be more restrictive than the national security guidelines and sometimes less restrictive.

2. Using a task force approach with participation by experienced Supervisory Special Agents from the field, and representing all investigative programs, the FBI developed implementing policies that will work for all programs and help us to fulfill our mandates, including protection of civil liberties.

Why is there a rush for an October 1 implementation?

1. We are ready for the new guidelines and we need them. The October 1 implementation date will enable us to incorporate the new policy framework into the Strategic Execution Team's (SET's) intelligence rollout and provide clear and consistent answers to agents' and analysts' questions – answers that do not differ based on the investigative program.
2. Also, the approval and reporting requirements in the policy framework being drafted will reflect the new standardized organization and work roles in field offices and the Directorate of Intelligence (for example, what is the authorization to collect intelligence to address a requirement and what investigative methods may be used?)

How will one set of guidelines work for diverse investigative programs?

To ensure the new policy framework works for all investigative programs, the drafting team included managers from field offices and headquarters operational divisions, as well as attorneys from the Office of General Counsel, and personnel from the Corporate Policy Office. The AGG Task Force sought input from each operational program through Division Policy Officers and worked hard to reach consensus on the standardized rules to be included. The Executive Assistant Directors met with the task force weekly to resolve any areas of conflict.

I have an issue with something in the DIOG. Is there a mechanism for providing feedback?

1. Issues related to potential compliance issues may be directed to the Office of Integrity and Compliance.
2. Substantive issues may be raised to the Corporate Policy office or your program manager.

D. Safeguarding Civil Liberties

What controls are in place to ensure these new authorities are not abused?

1. The AGG-DOM contain several general statements of policy.
 - No investigation can be commenced based solely on ethnicity or the exercise of First Amendment rights.
 - The FBI should use the least intrusive method that is feasible under the circumstances.

- In connection with Foreign Intelligence collection, agents should operate openly and overtly with US Persons if possible.
- All activities must have an authorized and proper purpose. We interpret that to mean there has to be a purpose that is tied to an FBI mission.

2. There will be a strong regime of oversight from DOJ.

- The oversight regime through mandatory reporting will be streamlined to focus on items of highest sensitivity (v. burying DOJ with reports).
- On the national security side, the initiation of full investigations of US persons must be reported to DOJ.
- All investigations with "sensitive circumstances" must be reported to DOJ. "Sensitive circumstances" means a matter involving a domestic public official, a political candidate, a religious or political organization or a person prominent in such organization or the media.
- The initiation of enterprise investigations must be reported to DOJ (either OCRS or NSD, as appropriate).
- The initiation of all investigations to collect foreign intelligence must be reported to the NSD. Thereafter, FBI must report annually on foreign intelligence collection matters. [Pure FI, not CI or CT matters.]
- Assistance to foreign agencies if the assistance is of a nature that requires FBI HQ approval (those approval levels not set; will likely be required if techniques beyond assessment techniques are used).

3. Other DOJ oversight:

- Traditional oversight of criminal matters continues to come through the relationship between FBI and US Attorney's Offices.
- DOJ is generally permitted to seek information on any investigation or group of investigations as it sees fit.
- Consensual monitoring in "sensitive monitoring circumstances" must be approved by DOJ. "Sensitive monitoring circumstances" includes, among others, consensual monitoring of high level federal officials and high level state officials.
- "National Security Reviews" conducted jointly by DOJ's National Security Division and FBI-OGC. These grew out of the NSL situation, but the scope of the review is much broader and is intended to provide oversight of those investigations that would not likely have USAO involvement.
- Office of Inspector General is always available with helpful reviews, audits and recommendations.

4. FBI Policy - The FBI will implement the new AG Guidelines with a comprehensive policy framework that includes extensive controls and checks to ensure that civil liberties and privacy rights are protected.
- Policies are still being drafted, but the overarching theme is to use risk analysis to govern approval levels (higher the risk either of the subject matter or the technique, the higher the level of required review). Examples follow:
 - Searching public or government data bases – low risk; no supervisor approval required
 - Conducting surveillance without sensitive circumstances during an assessment – higher risks: approval required.

[REDACTED]
[REDACTED] – much higher risk; much higher approval levels.

b7E

5. The FBI is putting in place a framework of approvals, reporting, recordkeeping, and strong oversight to govern Assessments. There are control mechanisms at all levels, from the Supervisor signing Assessment paperwork and conducting 90-day file reviews, to Chief Division Counsel reviews of sensitive matters, to programmatic reviews from FBIHQ. Additional internal controls include:
- Office of Integrity and Compliance is putting into place a policy and methodology to ensure compliance.
 - Inspections Division will have on-going responsibility for reviewing compliance.
 - Office of General Counsel is heavily involved with both the compliance efforts and with identifying areas where there may be confusion regarding the rules.
 - The new Sensitive Operations Review Committee (SORC) will provide for SES-level reviews of highly sensitive matters.
6. Congressional controls through oversight will continue.

The new domestic guidelines appear to eliminate the requirement for any predication or factual basis for a new category of FBI investigation—called an “assessment,” which only requires a “proper purpose.” Doesn’t this mean that the FBI can investigate anyone or any group in the U.S. without any factual basis to believe they are connected to crime or terrorism—as long as it is done for the right reason? If so, doesn’t this guidance return the FBI to the days of COINTELPRO when they could spy on Americans for purely political purposes?

NO. There are many safeguards within and outside the new guidelines that would prevent any return to the conduct that was permitted in the days of COINTELPRO. Here are some of them:

1. An assessment only permits the use of a limited list of investigative methods for the purposes of either assessing the validity of an allegation or “lead” or, on a pro-active basis, filling national intelligence requirements or determining the existence or absence of a criminal or national security threat or vulnerability. Persons and groups are not targeted and investigated in the traditional sense in an assessment. Allegations, threats, and vulnerabilities are examined and national intelligence requirements are filled. If the results of an assessment provide the factual

predication to investigate a specific person or a group of persons, a criminal or national security investigation must be opened and pursued if the predication meets the standard set forth in the guidelines. If, on the other hand, an assessment reveals no basis to investigate a person or a group, then the matter is closed.

2. The techniques available in an assessment are geared to the gathering of publicly available information, information in government databases, or information known or lawfully obtained by human sources who are familiar with the matter being assessed. More intrusive techniques such as electronic surveillance, the use of search warrants and National Security Letters, undercover infiltration, and counter-intelligence tactics will not be permitted. Some of these techniques were used in COINTELPRO to gather intelligence—they will not be used in an assessment.
3. Since the days of COINTELPRO, the legal landscape has changed considerably. Today, law enforcement and intelligence collection activity by federal agencies must comply with the Privacy Act, the Federal Wiretap Act, the Foreign Intelligence Surveillance Act, the Right to Financial Privacy Act, the Electronic Communications Privacy Act, the Fair Credit Reporting Act, the Family Educational Records Privacy Act, the Bank Secrecy Act, the E-Government Act and a host of federal regulations and policies—all of which are still in full effect and none of which have been diminished in any way by these new guidelines. In addition, a considerable body of federal case law has matured over the past 35 years interpreting constitutional and statutory authorities which binds the FBI's activities. Internal FBI policies and training are geared to reflect this legal landscape.
4. Two other new standards have emerged since the 1970's that are built into these new guidelines that are pertinent to this discussion:
 - No investigative activity can be conducted, and no record can be maintained, solely on the basis of a person's exercise of rights guaranteed by the First Amendment to the Constitution; and
 - No investigative activity may be conducted, and no record maintained solely, on the basis of race or ethnicity.
5. The new guidelines—like prior versions but unlike the COINTELPRO time period—contains other safeguards that are designed to protect privacy and civil liberties. These include higher approval levels and standards for investigative activity that involves what are described as "sensitive circumstances." These circumstances include investigative activity that involves, to any degree, political, social or religious groups engaged in the exercise of First Amendment rights. A key safeguard is the requirement for a legal review by trained counsel who examines the justification for the activity, whether there are less intrusive investigative alternatives available, and whether are mitigation steps that can be taken to lessen the risk of affecting the rights of members of the public.
6. The training of new agents and analysts has evolved to include considerable emphasis on the protection of privacy and civil liberties.

What determines the “least intrusive method?”

1. You should balance the level of intrusion against investigative requirements. The DIOG outlines a number of considerations, but there is no simple checklist.
2. In determining intrusiveness, the primary factor should be the degree of procedural protection that established law and the AGG-Dom provide for the use of the method.



b7E

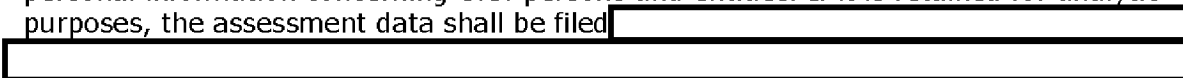
3. Consideration should be given to the: nature and scope of the information sought scope of the use of the method (how complete a picture of an individual’s activities will the method produce?); the source of the information and expectation of privacy associated with it; and the risk of public exposure.
4. Considerations on the investigative side of the balancing scale include: the seriousness of the crime or national security threat; the strength and significance of the intelligence/information to be gained; the amount of information already known about the subject or group under investigation; and the requirements of operational security, including protection of sources and methods.

How can you justify keeping files related to an Assessment for 25 years?

The 25 year retention requirement is consistent with the default policy of the National Archives and Records Administration (NARA).

If an Assessment finds that there is no indication of wrongdoing, is the record still retained?

1. Consistent with how we have handled records related to threat assessments for Guardian leads, information gained through an Assessment may be retained. Even where the assessment finds no indication of wrongdoing, the information may eventually serve a variety of valid analytic purposes as pieces of the overall intelligence picture are connected to thwart criminal and/or terrorist activities. In addition, the information may possibly assist FBI personnel in responding to any questions which may subsequently arise as to the nature and extent of the threat assessment and its results--whether positive or negative.
2. Retention of such information about an individual collected in the course of an assessment will alert other divisions considering conducting an assessment on the same individual if this particular individual is not a criminal or national security threat. As such, retaining personally identifying information collected in the course of an assessment will also serve to conserve resources and prevent the initiation of unnecessary assessments and other investigative activities.
3. Information obtained during a threat assessment that has insufficient value to justify further investigative activity (at least at the time it is obtained)—is often sensitive personal information concerning U.S. persons and entities. If it is retained for analytic purposes, the assessment data shall be filed



b7E

[REDACTED] to preclude its use as a basis for any further investigative activity unless and until such action is authorized by the AGG and the DIOG.

What level of approval will be required for the FBI to conduct an assessment of a political or religious group?

No assessment, or any other type of investigative activity, can be undertaken based solely on activities protected by the First Amendment. In an instance where there is information such as a specific threat lead indicating that a group may pose a threat of violence, an assessment may be permissible, but it is safe to say that such an activity would require the highest level of scrutiny.

Does the AGG-Dom allow the FBI to conduct Assessments based on speculation?

No. The guidelines expressly state that the basis of any assessment must not be arbitrary or groundless speculation. Furthermore, there must be a rational and articulable relationship between the stated purpose of the assessment on the one hand and the information sought and the proposed means to obtain that information on the other. Management is responsible for assuring that assessments are not pursued for frivolous or improper purposes.

Is the FBI permitted to map mosques or other religious institutions?

1. The FBI cannot map a religious institution solely because it is a religious institution.
2. Pursuant to existing guidelines and the AGG-Dom, if the FBI has an open assessment, preliminary or full investigation, investigators or analysts can geo locate a facility relevant to that assessment or investigation. However, the practice of religion is protected by the First Amendment and therefore cannot be the basis of any intelligence collection or analysis unless there are additional factors indicating a threat or vulnerability.

Is the FBI permitted to map racial or ethnic groups?

The DOJ Guidance Regarding the Use of Race by Law Enforcement Agencies, investigative activity (including collection of domestic intelligence) is still in effect and it states that investigations may not be based solely on racial or ethnic characteristics. Therefore, collecting information about—and mapping the locations of—racial or ethnic communities may not be conducted on that basis alone. There must be a valid law enforcement or national security basis for such collection. In practical terms, that means the collection must be based on the need to determine threats, vulnerabilities, and intelligence gaps in the domain and must be for one of the purposes for which an assessment is authorized under the guidelines. Documentation to justify such a collection under the assessment investigative category should include the basis for the collection and reflect a rational relationship between the threat or vulnerability to be assessed and the information to be collected.

Do the new guidelines allow the FBI to conduct data mining based on a profile?

1. The vast majority of data analysis performed during FBI predicated investigations is based on subjects or events and do not meet the definition of pattern-based data mining.

2. Pattern-based data mining, defined as the use of one or more data bases to search for persons who fit a set of group characteristics or patterns of behavior (e.g., the known characteristics of a particular terrorist organization) is permitted under strict controls.
 - Any such analysis based solely on ethnic or racial characteristics is strictly prohibited.
 - SORC approval is required.
 - The FBI must report all initiatives that involve the use of pattern-based data mining to Congress.

E. Key Terminology

A term or phrase in the DIOG seems to be used differently than I'm used to using it in my program. Which definition will apply?

You should follow the definition in the DIOG, along with any additional clarification consistent with that definition that may be found in implementing program guides.

What is the difference between an "assessment" as defined in the AGG and a "Domain Assessment"?

An assessment is a non-predicated investigation conducted for one of six authorized purposes under the AGG-Dom. A Domain Assessment is an intelligence product produced by the Field Intelligence Group to identify the key threats, vulnerabilities, and intelligence gaps, in the field office's area of responsibility or "domain." Doing a Domain Assessment does not authorize the use of methods permitted for a documented assessment under the AGG-Dom. However, as part of the domain management process, a collection plan will be created and assessments may be opened to collect intelligence in accordance with that plan.

What is a "Sensitive Investigative Matter"?

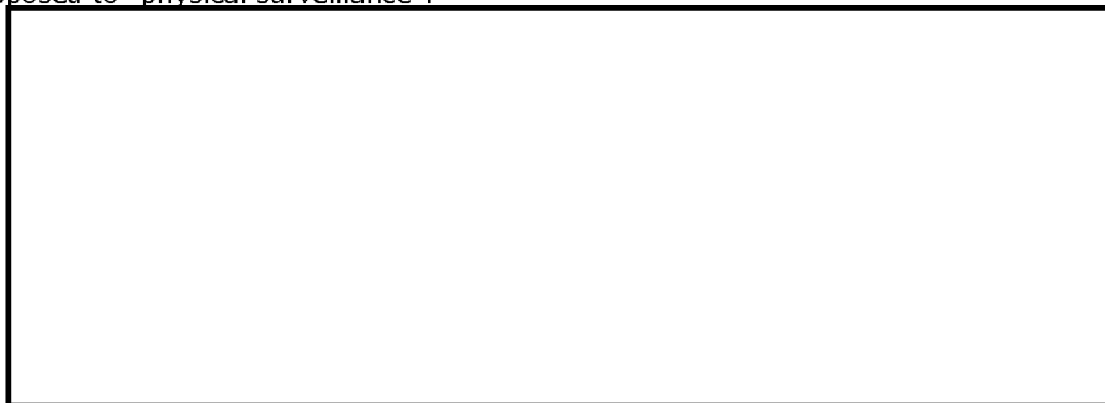
1. In the conduct of assessments and predicated investigations, a sensitive investigative matter is defined as a matter involving a domestic public official, political candidate, religious or political organization or individual prominent in such and organization, or news media, or having an "academic nexus," or any other matter which, in the judgment of the official authorizing an assessment, should be brought to the attention of FBIHQ and other DOJ officials.
2. This definition is new for all programs. Previous definitions of a Sensitive Investigative Matter should no longer be applied.

How is Physical Surveillance Defined?

Physical surveillance is defined as: deliberate observation by an FBI employee or confidential human source (CHS) of persons, places, or events, on either a limited or continuous basis, in a public or a semi-public (e.g., commercial business open to the public) setting. Physical surveillance is for the purpose of obtaining information regarding a pattern of activity over time.

What is the difference between “casual observation” and “physical surveillance?”

1. There is no bright line, but the following factors should be considered when determining whether a particular plan of action constitutes “casual observation” as opposed to “physical surveillance”:



b7E

2. “Casual observation” would be no longer in duration and no broader in scope than is necessary to determine the existence and nature of a threat.

What is the difference between a “sensitive investigative matter” and a “sensitive circumstance?”

Sensitive investigative matters refer to Assessments or predicated investigations involving a public official, political candidate, political or religious organization, news media, or university. (See section _____). The term “sensitive circumstance” relates to an undercover operation requiring FBIHQ approval. (See AGG on FBI Undercover Operations).

II. INVESTIGATIONS AND INTELLIGENCE GATHERING

A. Overview

What types of investigations are authorized?

Preliminary and Full (including FI and Enterprise), plus Assessments.

What types of investigative techniques are authorized?

See Chart [Link to Authorized Methods for Assessments and Predicated Investigations chart]

What level of approval is required for various investigative techniques?

See Chart [Link to Authorized Methods for Assessments and Predicated Investigations chart]

B. Assessments

Is the concept of an Assessment new to the FBI?

No. The FBI has been conducting Assessments to respond to threats, to check out leads, and to conduct strategic analysis. The DIOG will create one uniform set of rules for these activities and a framework for approvals, notifications, and record keeping.

What does the assessments section of the AGG-Dom replace?

The AGG-Dom combines (1) "threat assessments" under the former Attorney General's guidelines for FBI National Security Investigations and foreign Intelligence Collection and (2) 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."

What is the assessment category designed to address?

The assessment category is designed to address several things that are critical to the FBI's success as an intelligence agency:

- The need to track down and resolve threat leads.
- The need to identify key threats and vulnerabilities in our domain.
- The need to conduct analysis and planning.
- The need to develop and validate sources.
- The need to collect foreign intelligence.

When can I do an assessment?

1. In initiating or approving the conduct of an assessment or the use of an investigative method in an assessment, an agent or analyst or approving official will determine that:
 - a proper purpose and objective exists for the conduct of the assessment
 - the assessment is not based solely on the exercise of First Amendment activities;
 - the use of a particular investigative method is likely to further an objective of the assessment;
 - the investigative method selected is the least intrusive method, reasonable under the circumstances;
 - the anticipated value of the assessment justifies the use of the selected investigative method or methods; and
 - the assessment and method are an appropriate use of personnel and financial resources.
2. Special Agents, Intelligence Analysts, and supervisors are responsible for ensuring that all six criteria are met before approving and initiating an assessment.

What is a "proper purpose?"

Under the AGG-Dom it is a proper purpose for the FBI to:

1. Seek information, proactively or in response to investigative leads, relating to activities constituting violations of federal criminal law or threats to the national security;
2. Seek information, proactively or in response to investigative leads, relating to the involvement or role of individuals, groups, or organizations relating to activities constituting violations of federal criminal law or threats to the national security;
3. Identify and obtain information about potential targets of or vulnerabilities to criminal activities in violation of federal law or threats to the national security;
4. Obtain information to inform or facilitate intelligence analysis and planning.
5. Seek information to identify potential human sources, assess the suitability, credibility, or value of individuals as human sources, validate human sources, or maintain the cover or credibility of human sources, who may be able to provide or obtain information relating to criminal activities in violation of federal law, threats to the national security, or matters of foreign intelligence interest; and
6. Seek information, proactively or in response to investigative leads, responsive to foreign intelligence requirements.

Does the AGG-Dom allow the FBI to conduct assessments based on speculation?

The guidelines expressly state that the basis of any assessment must not be arbitrary or groundless speculation. Furthermore, there must be a rational and articulable relationship between the stated purpose of the assessment on the one hand and the information sought and the proposed means to obtain that information on the other. Regardless of whether a specific approval or specific documentation is required, an agent or analyst should be able if asked to explain the purpose of an assessment and the reason(s) the methods used to conduct the assessment were selected. Management is responsible for assuring that assessments are not pursued for frivolous or improper purposes.

How do we reconcile the mandate to address “gaps” and get ahead of threats with the restriction that assessments cannot be undertaken based on “groundless speculation?”

The AGG-Dom requires that there be a “rational and articulable relationship” between the stated purpose of the assessment and the proposed means to obtain it. If intelligence is being sought as a result of a disciplined Domain Management Process, and a collection plan with clear goals, and the assessment is opened for a proper purpose – as required by FBI policy – then the basis will not be arbitrary or groundless speculation.

What level of approval is required to conduct as assessment?

See Chart [insert Assessments Summary chart]

b7E

Note that in addition to general approval requirements for assessments, the use of particular investigative methods such as:

What can we do without a specific factual predication? What types of methods/activities can be done under an assessment?

1. The methods authorized in assessments are generally those of relatively low intrusiveness, such as obtaining publicly available information, checking government records, and requesting information from members of the public.
2. The following methods may be used in assessments:
 - 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.
 - Use online services and resources (whether nonprofit or commercial).
 - Use and recruit human sources in conformity with the AG's Guidelines Regarding the Use of FBI Confidential Human Sources.
 - 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.
3. Under FBI policy (the DIOG), use of a particular investigative method such as:require higher supervisory approval.
4. The following methods may not be used in assessments, unless the purpose of the assessment is to

b7E



Do I need supervisor approval to track down a Guardian lead?

Counterterrorism program leads, initial follow-up to complaints or suspicious activities, and other activities resulting in the prompt checking of leads do not require supervisory approval, unless they involve Sensitive Investigative Matters or methods requiring higher approvals. 

b7E

How long can an assessment continue?

There is no time limit on assessments. However, time limits in the CHS Manual may apply to an assessment for purpose # 5 (related to Confidential Human Sources).

An assessment may be initiated by an FBI employee for up to 15 calendar days without supervisory approval. At the conclusion of the initial 15 day period, documented supervisory approval must be acquired for each succeeding 15 day extension.

What level of approval is required to conduct surveillance for an assessment?

Generally, an assessment can continue using all permissible tools for 15 days before supervisor approval is required. However, in the case of continuous surveillance, there is a 3-day limit before supervisor approval is required.

Can I task SOG or SSG to help with an assessment?

ASAC approval is required for taskings to SOG or SSG.

What file number should be used?

The file number to use depends on the purpose of the assessment.

1. For Assessments to seek information in response to investigative leads (purpose 1 or 2), 



b7E

What level of approval will be required for the FBI to conduct an assessment of a political or religious group?

No assessment, or any other type of investigative activity, can be undertaken based solely on activities protected by the First Amendment. In an instance where there is information such as a specific threat lead indicating that a group may pose a threat of violence, an assessment may be permissible, but it is safe to say that such an activity would require the highest level of scrutiny.

C. Preliminary Investigations

When should an Agent open a Preliminary Investigation (PI)?

Preliminary investigations may be initiated on the basis of any allegation or information indicative of possible criminal activity or threats to the national security. Enterprise investigations and foreign intelligence collection cannot be conducted as a preliminary investigation. A preliminary investigation may not be initiated based solely on the exercise of First Amendment rights.

When can I open a preliminary investigation?

1. Like Assessments, a PI requires a proper purpose, but in addition there must be adequate predication.
2. A preliminary investigation may be initiated on the basis of information or an allegation indicating the existence of a circumstance described as follows:
 - 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.
 - 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.



b7E

3. In initiating or approving the conduct of a preliminary investigation or the use of an investigative method in a preliminary investigation, an agent or approving official will determine that:
 - a proper and adequate predication exist for initiating a preliminary investigation;
 - the preliminary investigation is not based solely on the exercise of First Amendment activities;

- the use of a particular investigative method is likely to further the purpose of the preliminary investigation;
- the investigative method selected is the least intrusive method, reasonable under the circumstances; and
- the preliminary investigation and method(s) are an appropriate use of personnel and financial resources.

What level of approval is required to open a PI?

1. The initiation of a PI requires the approval of the field office SSA with written notification to the appropriate FBIHQ section and unit. The initiation of a preliminary investigation does not require DOJ notification unless the preliminary investigation involves a sensitive investigative matter.
2. The initiation of a preliminary investigation involving a sensitive investigative matter requires:
 - a. **Field Office:** CDC review, SAC approval, and written notification to the appropriate FBIHQ Section Chief and Unit Chief. Additionally, written notification shall be made by the field office to the United States Attorney or by the appropriate FBIHQ section to the DOJ Criminal Division or NSD as soon as practicable but no later than 30 calendar days after the initiation of such an investigation. The notice shall identify all known sensitive investigative matters involved in the investigation.
 - b. **FBIHQ:** OGC review, Section Chief approval, and written notification to the United States Attorney or the DOJ Criminal Division or NSD as soon as practicable but no later than 30 calendar days after the initiation of such an investigation. The notice shall identify all known sensitive investigative matters involved in the investigation.
3. The FBI shall notify the Deputy Attorney General if FBI Headquarters disapproves a field office's initiation of a preliminary investigation relating to a threat to the national security on the ground that the predication for the investigation is insufficient.

How should I document a request to open a PI?

Use an Electronic Communication (EC)

What if I need to extend a PI?

A PI must be concluded within six months of its initiation, but may be extended up to six months by the SAC. Extensions of preliminary investigations beyond a year must be approved by the appropriate FBIHQ section/unit.

How do I close a PI?

Closing a preliminary investigation requires approval from the initiating FBI field office's SSA and written notice to the appropriate FBIHQ section/unit. When closing the investigation, the field office will affirm that there is a specific factual basis on which to determine that the allegation or information which predicated the investigation has been

resolved. When closing a preliminary investigation, the SSA shall ensure that all pending investigative methods have been completed/terminated (e.g., mail covers and pen register/trap and trace).

D. Full Investigations

What is required to open a full investigation?

Full investigations require a more substantial factual predication than is required for preliminary investigations. A Full Investigation may be initiated if there is an articulable factual basis that reasonably indicates one of the following circumstances exists:

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.
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 foreign intelligence requirement.

What are some examples of justifications for a Full Investigation?

The following examples have a proper purpose and predication for initiating a full investigation:



b7E

What types of full investigations are available and where are these covered in the DIOG?

Single, multi-subject, foreign intelligence, and enterprise. Policies related to single and multi-subject can be found in the "Full Investigations" section of the DIOG. Foreign Intelligence and Enterprise Investigations each have their own section in the DIOG.

How do I open a full investigation?

1. You must document in an EC the purpose of and predication for a full investigation and get SSA approval. You should also notify the FBIHQ substantive unit. In

national security cases involving a U.S. Person, you must also notify the DOJ National Security Division.

2. Enterprise investigations require SSA and FBIHQ approval with notification to the FBIHQ substantive unit, DOJ, and the U.S. Attorney's Office.

3. Full investigations involving Sensitive Investigative Matters

b7E

4. See Chart [[link to Predicated Investigations Summary chart](#)]

How do I close a full investigation?

Although there is no duration requirement for full investigations, the investigation must be closed upon all investigative activity being exhausted.

1. Closing a full investigation requires approval from the FBI field office SSA with written notification to the FBIHQ section/unit and the SAC in sensitive investigative matters.
2. The closing of a full investigation for the purpose of foreign intelligence collection requires SSA approval with concurrence from FBIHQ Foreign Intelligence Collection Oversight Unit.

E. Foreign Intelligence

How is FI defined in the DIOG?

The AGG and DIOG define "Foreign Intelligence" as information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations or foreign persons, or international terrorists.

What is the difference between a "matter of Foreign Intelligence Interest" and "requirements-driven Foreign Intelligence collection?"

Assessments to collect on matters of "Foreign Intelligence Interest" require documented authorization from the Foreign Intelligence Collection Oversight Unit, FBIHQ. Matters of Foreign Intelligence Interest, an authorized purpose for an assessment, are different than "requirements-driven Foreign Intelligence collection" which are conducted as Full investigations. The Directorate of Intelligence division program guide further describes this distinction.

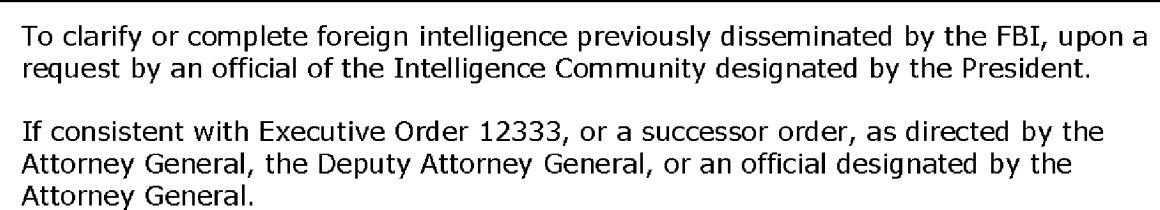
[I'd like a clearer explanation of when you go the assessment route versus full.]

If the Directorate of Intelligence has issued an intelligence requirement, do we open an assessment or a full investigation?

As with requirements originating from the Office of the Director of National Intelligence, requirements coming from the FBI DI justify a full investigation. This is because in the process of identifying and validating a requirement the DI will determine if there is sufficient predication for a full investigation.

What if I want to open an FI investigation based on a local requirement?

Only the FBIHQ DI may approve the initiation of the conduct of a foreign intelligence assessment or full investigation. Field offices may ask the DI to initiate such investigative activity based upon the following four standards for initiating and approving foreign intelligence collection:

1. 
2. 
3. To clarify or complete foreign intelligence previously disseminated by the FBI, upon a request by an official of the Intelligence Community designated by the President.
4. If consistent with Executive Order 12333, or a successor order, as directed by the Attorney General, the Deputy Attorney General, or an official designated by the Attorney General.

b7E

What are the reporting requirements re U.S. Persons?

Can I open a PI on an FI matter?

No. Foreign intelligence collection cannot be conducted as a preliminary investigation.

How do I open a full investigation on an FI matter?

1. The purpose of and objective or requirement a full investigation shall be documented in the initiating electronic communication (EC).
2. Opening a full investigation on an FI matter requires SSA approval and approval by the FBIHQ DI. Additionally, written notification to FBIHQ Foreign Intelligence Collection Oversight Unit (FICOU) and DOJ NSD is required as soon as practicable within 30 calendar days of initiation.



b7E

What are the notification requirements for FI investigations?

1. There is no DOJ notification requirement for matters of foreign intelligence interest conducted under an assessment.
2. Notification of the initiation of a full investigation, including a sensitive investigative matter that involves foreign intelligence collection shall be forwarded from FBIHQ DI to the DOJ National Security Division as soon as practicable within 30 calendar days.
3. FBIHQ DI shall notify the Deputy Attorney General if FBIHQ disapproves a field office's request for the initiation of a foreign intelligence full investigation.

F. Enterprise Investigations

1. Enterprise investigations focus on groups or organizations that may be involved in the most serious criminal or national security threats to the public. Enterprise investigations cannot be conducted as preliminary investigations or assessments.
2. The term "enterprise" includes any individual, partnership, corporation, association, or other legal entity, and any union or group of individuals associated in fact although not a legal entity. An enterprise investigation examines the structure, scope, and nature of the group or organization including: its relationship, if any, to a foreign power; the identity and relationship of its members, employees, or other persons who may be acting in furtherance of its objectives; its finances and resources; its geographical dimensions; its past and future activities and goals; and its capacity for harm.

When should I open an enterprise investigation as opposed to a multi-subject investigation?

A full investigation of a group or organization may be initiated as an enterprise investigation if there is an articulable factual basis for the investigation that reasonably indicates that 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:

1. a pattern of racketeering activity as defined in 18 U.S.C. 1961(5);
2. international terrorism or other threat to the national security;
3. domestic terrorism as defined in 18 U.S.C. 2331(5) involving a violation of federal criminal law;
4. furthering political or social goals wholly or in part through activities that involve force or violence and a violation of federal criminal law; or
5. an offense described in 18 U.S.C. 2332b(g)(5)(B) or 18 U.S.C. 43.

What is required to open an enterprise investigation?

Direct information such as statements made in furtherance of the enterprise's objectives or the nature of the conduct engaged in by the enterprise, which show a purpose of committing crimes or securing their commission by others establishes the predicate

(articulate factual basis) for initiating an enterprise investigation. A group's activities and the statements of its members may properly be considered in conjunction with each other. A combination of statements and activities may justify a determination that the threshold predication is satisfied, even if the statements alone or the activities alone would not warrant such a determination.

What approvals are required for opening an Enterprise Investigation?

The initiation of an enterprise investigation by an FBI field office requires the approval of the field office SSA with written notification to the appropriate FBIHQ substantive unit and DOJ. FBIHQ Divisions may require specific facts to be included in this notification. This notice shall include sensitive investigative matters. Enterprise investigations involving sensitive investigative matters require CDC review, SAC approval, and written notification to DOJ.

What DOJ component should be notified?

1. FBIHQ shall provide notification of an enterprise investigation initiation to the appropriate DOJ component within 30 days of the date of the initiation. Notifications should go to the National Security Division, except where the enterprise investigation relates to a pattern of racketeering activity that does not involve an offense or offenses described in 18 U.S.C. 2332b(g)(5)(B), in which case the responsible DOJ component is the Organized Crime and Racketeering Section of the Criminal Division.
2. FBI field offices shall notify any relevant United States Attorney's Office of the initiation of all enterprise investigations, except in an investigation relating to espionage as discussed above.

How do I close an Enterprise Investigation?

The closing of an enterprise investigation by an FBI field office requires the approval of the field office SSA with written notification to the appropriate FBIHQ substantive unit, 30 days unless advised contrary by the Bureau (UACB).

Can I open a PI on an enterprise investigation?

No. Enterprise investigations cannot be conducted as a preliminary investigation.

G. Sensitive Investigative Matters

What is a Sensitive Investigative Matter?

In the conduct of assessments and predicated investigations, a sensitive investigative matter (SIM) is defined as a matter involving a Domestic public official, political candidate, religious or political organization or individual prominent in such and organization, or news media, or having an "academic nexus," or any other matter which, in the judgment of the official authorizing an assessment, should be brought to the attention of FBIHQ and other DOJ officials.

I have SIM. What does this mean for my investigation?

If your investigation concerns a SIM, additional levels of approval and reporting will be required both for opening the investigation and for the use of particular investigative methods.

What is an "Academic Nexis"?

1. As a matter of FBI policy, an academic nexus is considered a SIM. An academic nexus exists if:

A large rectangular box with a black border, used for redaction of text.

2. As a matter of FBI policy, the following are not SIMs despite having a potential academic nexus:

A large rectangular box with a black border, used for redaction of text.

b7E

Can I conduct an assessment of a SIM? What level of approval is required?

The initiation of an assessment involving a SIM requires CDC review, SAC approval and notification to the appropriate FBIHQ Section Chief and Unit Chief.

How do I open a Preliminary or Full investigation on a SIM?

1. From a field office - The initiation of a predicated investigation involving a SIM requires CDC review, SAC approval, and notification to the appropriate FBIHQ Section Chief and Unit Chief. Additionally, notification shall be made by the field office to the United States Attorney or by the appropriate FBIHQ section to the DOJ Criminal Division or NSD as soon as practicable but no later than 30 calendar days after the initiation of such an investigation. The notice shall identify all known sensitive investigative matters involved in the investigation.
2. From FBIHQ - The initiation of a predicated investigation by FBIHQ requires OGC review, Section Chief approval, and notification to the United States Attorney or the DOJ Criminal Division or NSD as soon as practicable but no later than 30 calendar days after the initiation of such an investigation. FBIHQ must, as appropriate, also notify the affected field office. The notice shall identify all known SIMs involved in the investigation.

What is the SORC and what does it do?

1. The Sensitive Operations Review Committee (SORC) was created to provide an additional level of review for certain SIMs. This committee will have two related functions:
 - approve—or recommend for approval—specified categories of sensitive operations before they are undertaken; and
 - conduct periodic review of other sensitive operations after the fact.
2. The Membership Chair is a rotating position [REDACTED]

b7E

When do I need to get SORC approval?

There are ten circumstances that require SORC approval:

[REDACTED]

b7E

How do I initiate SORC review?

You may initiate SORC review with an EC from your division. The appropriate FBIHQ division must endorse your request and present it to the committee.

What is required for SORC approval?

Details regarding the SORC are still being worked out, but tentatively:

1. A majority of the SORC must approve an operation before it can go forward.
2. The SORC will only approve an operation upon findings that: (1) the potential benefits to the national security or public welfare are significant; (2) the proposed course of action is necessary to achieve those benefits and is otherwise appropriate under the circumstances; (3) all reasonable mitigation measures have been considered and imposed; and (4) the anticipate benefits outweigh any risks to civil liberties, privacy, or other rights that may be affected.

What if we have an emergency situation and do not have time to go through the SORC approval process?

FBI policy has a provision related to emergency approvals.

H. Undisclosed Participation**What changes are being made to the rules on undisclosed participation?**

Generally the new rules are less restrictive. Limits that previously were applied to companies and other entities are now limited and apply only to groups protected by the First Amendment.

III. INFORMATION SHARING**What is the difference between "permissive" and "required" sharing?**

"Permissive sharing" is sharing that is authorized, but not required. Required sharing is mandatory and includes requirements to share found in statutes, treaties,

Executive Orders, Presidential directives, National Security Council directives, Homeland Security Council directives, and Attorney General-approved policies, memoranda of understanding, or agreements.

IV. DOCUMENTATION AND RECORD KEEPING

How and where should an assessment be documented?

1

2

3

[REDACTED] a file must be opened in the appropriate investigative classification as an assessment file or opened as an 800 file. A new 800 classification has been created for certain assessments that pertain to Domain Management.

4. Additionally, SSA approval must be acquired for the opening EC which must document the purpose and objective of the assessment. When the objective is met, the closing EC must be prepared, approved by the SSA and uploaded to the file. If additional objectives arise during the assessment, they must be documented in an EC, approved by the SSA, and uploaded to the file.

b7E

b7E

How long will an assessment file be retained?

The FBI has requested a 25 year disposition authority for zero sub-assessment files in accordance with National Archives and Records Administration (NARA) regulations. The record retention period for assessments filed under investigative classifications are governed by the individual classification's disposition authority.

What is the requirement to document assistance to other agencies?

All investigative and technical assistance provided to other agencies beyond those methods authorized for assessments [REDACTED]

b7E

b7E

**V. IMPLEMENTING THE STRATEGIC EXECUTION TEAM
(SET) INITIATIVES**

b7E

A. Domain

I'm working on a Domain Assessment. How should I document and file information related to this activity?

The Field Intelligence Group should [REDACTED] for materials related to Domain Management.

May I open an assessment in order to collect information for our Domain Assessment?

You should first [REDACTED] for the Domain Assessment. This is not an assessment that would give you authority to collect intelligence. The next step is to create a collection plan that establishes a framework for addressing gaps, vulnerabilities, and threats through assessment activity. The collection plan should tie into collection requirements. You may then open an assessment based on intelligence gaps identified in the collection plan. Once it has been designated an assessment, an assessment file number will be created.

As part of our Domain Management efforts, we need to identify and obtain information about potential targets of or vulnerabilities. How do we approach this if there is no specific factual predication?

1. It is a proper purpose to conduct an assessment investigation to identify and obtain information about potential targets of or vulnerabilities to criminal activities in violation of federal law or threats to the national security.
2. Assessments to collect this sort of information require SSA or SIA approval. If the purpose is to obtain information relevant to a Sensitive Investigative Matter, SIM approvals apply.
3. All assessments conducted pursuant to this subsection must be opened [REDACTED]
[REDACTED]
[REDACTED] Additionally, an opening electronic communication (EC) must document a proper purpose and contain the objective for the assessment. When the objective has been met, a closing EC must be approved the SSA/SIA and uploaded to the file.

What if we just need the information to assist with strategic planning or resource allocation?

Under the AGG-Dom it is a proper purpose to conduct an Assessment to "Obtain information to inform or facilitate intelligence analysis and planning."

1. Assessments to collect this sort of information require SSA or SIA approval. If the purpose is to obtain information relevant to a sensitive investigative matter, then the initiation of the assessment requires CDC review and SAC approval, with written notification to the appropriate FBI Headquarters Section Chief and Unit Chief.
2. All assessments conducted pursuant to this subsection must be opened [REDACTED]
[REDACTED]
[REDACTED] Additionally, an opening electronic communication (EC) must document a

proper purpose and contain the objective for the assessment. When the objective has been met, a closing EC must be approved the SSA/SIA and uploaded to the file.

Does FI activity collection authority allow me to collect Domain information?

Yes. FI collection is considered a full investigation so the agent has the use of all lawful investigative techniques, subject to proper approval and subject to limitations on the use of specific techniques.

Will the new AG Guidelines for Domestic FBI Operations allow the FBI to recruit new sources and task existing sources under a Threat Assessment?

Yes. The AGG-Dom, as currently drafted however, will no longer have a Threat Assessment. Instead, a Threat Assessment will be replaced by an **Assessment Investigation**. Like the Threat Assessment, the Assessment Investigation will require a proper investigative purpose but not any particular factual predication. The purpose of an Assessment Investigation must be to detect, obtain information about, or prevent or protect against federal crimes or threats to national security or to collect foreign intelligence. FBI policy implementing the authorization to recruit and task sources during an Assessment Investigation is currently being drafted.

How can I collect intelligence without having an open investigation (i.e. Domain, intelligence requirements, FI)?

You cannot collect information unless it is pursuant to an assessment, preliminary investigation, full investigation, or foreign intelligence. Pursuant to the lowest authorized level of investigation, a non-predicated assessment, you must at a minimum be collecting intelligence for the purpose of detecting, obtaining information about, or preventing or protecting against federal crimes or threats to the national security or to collect foreign intelligence.

B. Collection and Requirements

What can be collected outside of a case?

An agent should not be collecting anything that does not fall within an assessment, preliminary, full investigation, or foreign intelligence investigation.

Can we collect intelligence just to address a requirement?

Before any investigative activity is initiated in order to respond to an FBI National Collection Requirement, an assessment must be initiated or already open. This is true for FBI National Collection Requirements (which may be issued by FBIHQ Directorate of Intelligence, after coordination with FBIHQ Office of General Counsel, other FBIHQ substantive divisions and field offices) and for FBI Field Office Collection Requirements (established by the Intelligence Program Coordinator (SIA), consistent with FBI National Priorities as established by FBIHQ).

If I do not have a case driving my collection activities, can I document lawfully collected Domain information in an FBI database or FBI control file?

An agent should not be collecting information unless it is in support of an assessment, preliminary investigation or full investigation. All collection activities should be documented in the appropriate file.

How are we tracking activities conducted in response to a requirement?

Each FBI requirements must be tied to a specific program requirement, whether it is WMD, Cyber, CI, CTD, etc. Each FBI requirement also needs a unique identifier, and will be housed in the National Requirements Collection Library.



b7E

Will the new AGG and FBI policy allow SAs to use all the techniques which are currently taught in training classes? (i.e. DHCC, etc.)

The only techniques authorized for use are those contained in the AGG-Dom for assessment, preliminary and full investigations. As authorized by Part II.A.3.h of the AGG-Dom, assessment investigations, opened for the sole purpose of assessing a source, are authorized to use other the lawful investigative methods contained in Part V.A.1-12 of the AGG-Dom. The FBI is currently reviewing which of those other authorized investigative methods are lawful when used during an assessment investigation for the sole purpose of assessing a source.

C. HUMINT

When can I open a source?

1. You may open a source to support a preliminary or full investigation.
2. Under the AGG-Dom you may also open a source under an assessment investigation. It is a proper purpose to conduct an assessment to: "Seek information to identify potential human sources, assess the suitability, credibility, or value of individuals as human sources, validate human sources, or maintain the cover or credibility of human sources, who may be able to provide or obtain information relating to criminal activities in violation of federal law, threats to the national security, or matters of foreign intelligence interest."

- An agent or analyst may initiate an assessment under this subsection without supervisory approval unless the assessment will, or is likely to obtain information relevant to a Sensitive Investigative Matter, in which case, SIM approvals would apply.
3. As a matter of FBI policy, CHS case files shall be maintained [redacted]
 4. All activities related to Confidential Human Sources must be conducted in conformity with the AG Guidelines regarding the Use of FBI Confidential Human Sources and the FBI's CHS Manual.

b7E

How far can I task my source under an assessment?

1. A CHS cannot be tasked to do what an agent cannot legally do. [redacted]
[redacted]
2. Supervisory approval levels for tasking a CHS depend upon the nature of the tasking.
3. CHS use and direction must be limited in focus and scope to what is necessary to accomplish the specific purpose and objective for which the CHS is being used. The agent's tasking of the CHS, to include the focus and scope, must be included in the agent's report [redacted]
4. A CHS may be directed to seek information about an individual, group or organization [redacted]
[redacted]
5. Infiltration by a CHS into a legitimate group or organization is a highly intrusive investigative method that requires special levels of approval and may require approval as an "Undisclosed Participation" (UDP) [redacted]
[redacted]

b7E

VI. TRANSITION

I currently have an open Threat Assessment, do I have to open an assessment file under the new rules?

Yes.

I'm working on a case that was opened prior to October 1, 2008. Which rules apply?

From October 1 forward, the only applicable guidelines are the AGG-Dom and the only applicable policy is the DIOG and related program guides.

There is a new requirement to report_____. Do I have to do this if the activity started prior to October 1, 2008?

Who should I call if I have questions?