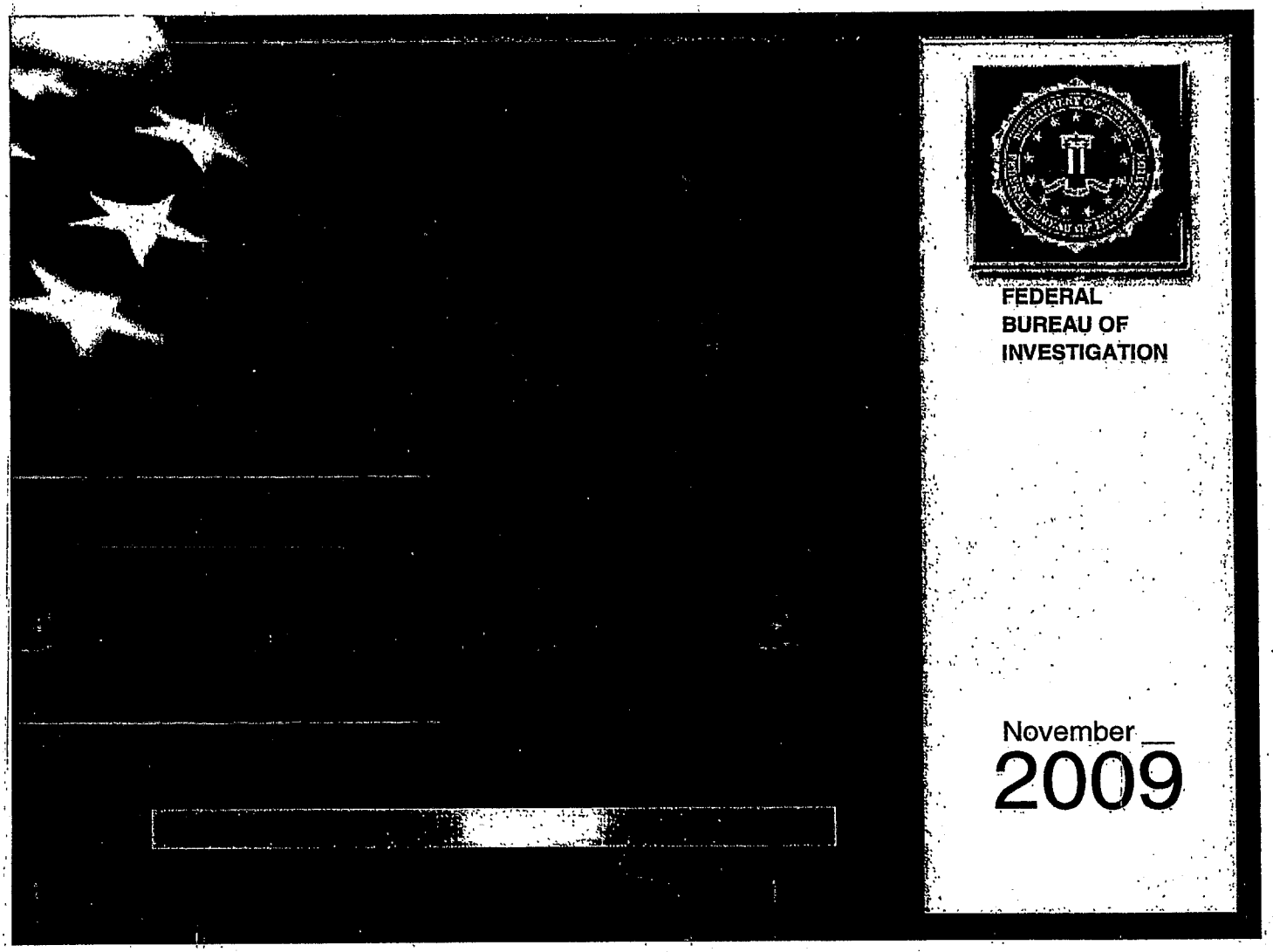


FEDERAL
BUREAU OF
INVESTIGATION

November
2009

- The DIOG was written to implement The Attorney General's Guidelines for Domestic FBI Operations (AGG-DOM) and applies to all domestic investigative activities and intelligence collection conducted by the FBI.
- The Domestic Investigations and Operations Guide (DIOG) was approved by FBI Director Robert Mueller on December 16, 2008.
- The purpose of the DIOG is to standardize policy to ensure that criminal, national security, and foreign intelligence investigative activities are consistent throughout the FBI.
- The DIOG applies to all FBI employees, Task Force Officers, and all other individuals operating under FBI authority.

The DIOG provides guidance throughout the FBI investigative process. Investigations progress through the following three phases:

- Assessment
- Preliminary Investigation
- Full Investigation

Prior to opening an assessment, an FBI employee must:

- determine an authorized purpose;
- follow specific work flows for management and documentation;
- not initiate based solely on the exercise of these First Amendment rights; (unless a group exercising its First Amendment rights also threatens or advocates violence or destruction of property)
- and must ensure that the assessment is an appropriate use of personnel and financial resources.

A Preliminary Investigation may be initiated if:

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

The AGG-DOM authorizes a third level of investigative activity-predicated investigations. Full Investigations may be initiated if there is an "articulable factual basis" of possible criminal or national threat activity.

The three types of Full Investigations include:

- Single and Multi-subject
- Enterprise
- Positive Foreign Intelligence.

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

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

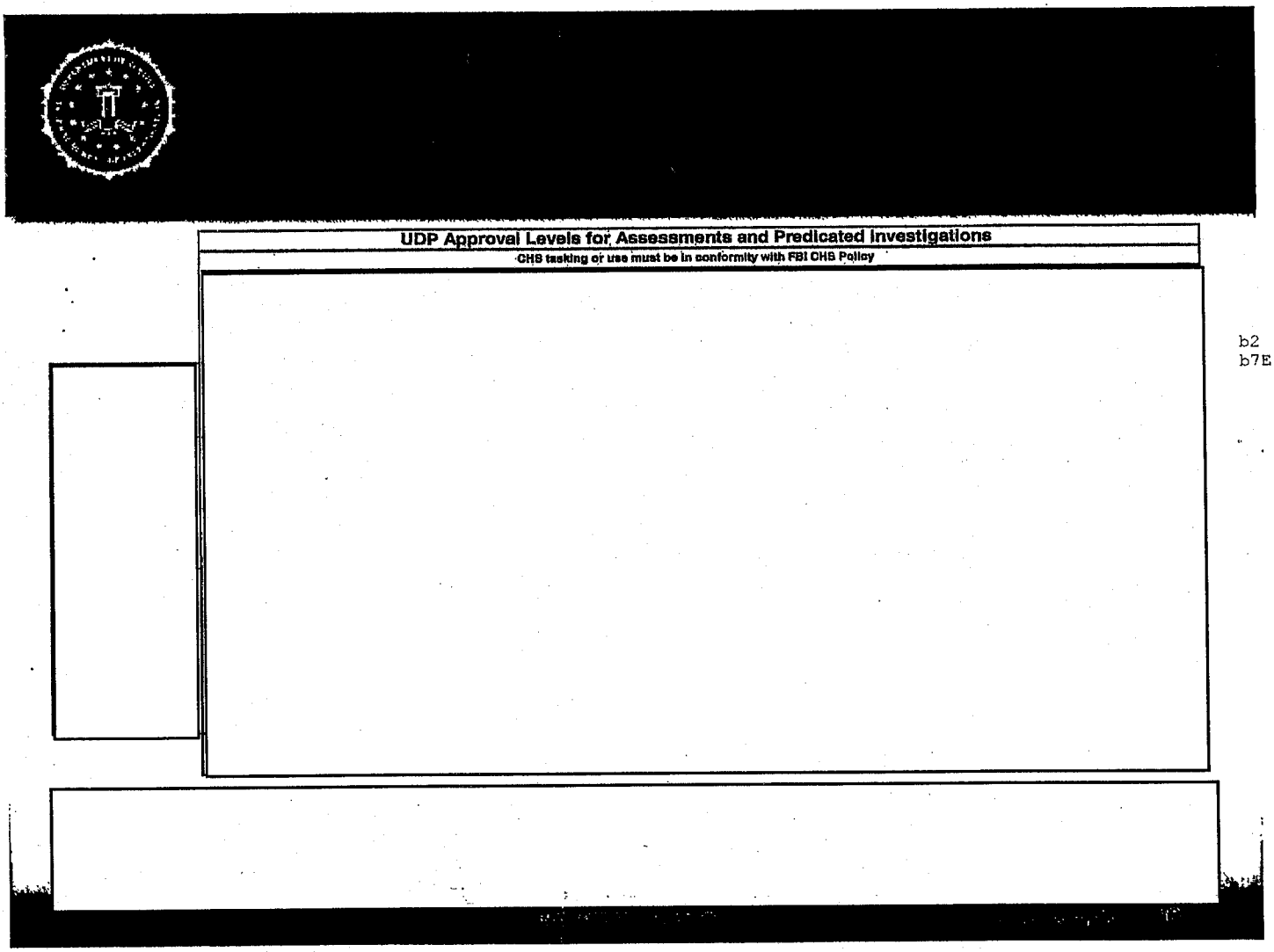
- Policy driven by EO 12333
- AGG-Dom required a UDP policy and AG approval of that policy
- FBI Policy seeks uniformity in National Security Investigations and Criminal investigations
- [redacted]

b2
b7E

General Undisclosed Participation (UDP):

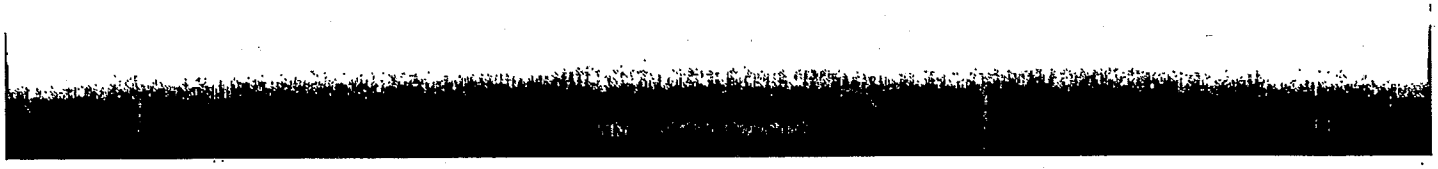
- General UDP occurs when an FBI employee or Confidential Human Source (CHS), acting on behalf of the FBI, becomes a member or participates in the activity of an organization without disclosing FBI affiliation to an appropriate official of the organization
- "Organization" means an association of two or more persons formed for any lawful purpose (social, political, religious, business, etc.)

b2
b7E


UDP Approval Levels for Assessments and Predicated Investigations
CHS tasking or use must be in conformity with FBI CHS Policy

b2
b7E

The following charts outline Investigative Methods and approval requirements for these methods, as well as the categories of Investigations.



Field Office Investigations Chart

Investigation	Purpose	Duration	Documentation	Approval	Justification Review	SIM	Responsible Entity
Type 1	Activities constituting violations of federal criminal law or threats to the national security	As long as necessary to achieve purpose and objective; No time limit	FD-71 or Guardian as soon as practical	Any employee can initiate; SSA or SIA Approval	Every 30 days	CDC review; SAC approval	Investigative Squad
Type 2	The involvement or role of individuals, groups, or organizations in such activities (# 1 above)						
Type 3	Potential targets of or vulnerabilities to criminal activities in violation of federal law or threats to the national security	As long as necessary to achieve purpose and objective; No time limit	EC before initiating	Prior SSA or SIA Approval	Every 90 days; if probationary employee, every 60 days	CDC review; SAC approval	FIG (Collection Management) or Investigative Squad
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
Type 5	Identify, assess, validate or maintain the cover or credibility of a CHS	CHSPM and AGG-CHS	[redacted] classification	CHSPM and AGG-CHS	CHS Manual	Not addressed in DIOG; Follow CHS Manual	FIG or Investigative Squad
Type 6 and PFI Assessments	Matters of PositiveForeign Intelligence (PFI) interest responsive to FI requirement	As long as necessary to achieve purpose and objective; No time limit	EC before initiating	Prior SSA or SIA, and HQ/DI Approval	Every 90 days: If probationary employee, every 60 days	CDC Review, SAC Approval	FIG (Investigative Squad can support)

Investigation	Predication	Duration	Documentation	Approval	Justification Review	SIM	Responsible Entity
PI	Initiated on the basis of "information or an allegation" indicating the existence of a circumstance described in DIOG Section 6.5	6 months; One extension by SAC, not delegable. Beyond 1 year CHQ unit and section (for "good cause")	[redacted]	Prior SSA Approval (CI also requires FBIHQ notice)	Every 90 days; if probationary employee, every 60 days	CDC Review, SAC Approval; Notification to USAO or DOJ & HQ within 30 days	Investigative Squad
Full	Initiated if there is an "articulable factual basis" that reasonably indicates circumstances described in DIOG Section 7.5 exist	No time limit; Factual predication determines outcome	EC	Prior SSA with FBIHQ (& DOJ notice on NSB USPER matters)	Every 90 days; if probationary employee, every 60 days	CDC Review, SAC Approval; Notification to USAO or DOJ & HQ within 30 days	Investigative Squad
Enterprise Full	Investigation is predicated when there is an articulable factual basis for the investigation that reasonably indicates the group or organization is engaged in Racketeering, IT, DT, or other. See DIOG Section 8.4	No time limit; Factual predication determines outcome	EC	Prior SSA with FBIHQ and DOJ notice	Every 90 days; if probationary employee, every 60 days	CDC Review, SAC Approval; Notification to USAO or DOJ & HQ within 30 days	Investigative Squad
PFI Full	Investigation may obtain Positive Foreign Intelligence (PFI) that is responsive to a foreign intelligence requirement	Until the requirement is met; No time limit	EC	Prior DI/CMS approval; notice to DOJ/NSO within 30 days	Every 90 days; if probationary employee, every 60 days	CDC Review, SAC Approval; Section Chief approval	FIG

b2
b7E

	Assessments	Preliminary Investigations	Full Investigations
Obtain publicly available information			
Access and examine FBI and other DOJ records, and obtain information from any FBI or DOJ personnel			
Access and examine records maintained by, and request information from, other federal, state, local, tribal, or foreign governmental entities or agencies			
Use online services and resources (whether nonprofit or commercial)			
Use and recruit human sources in conformity with AG Guidelines Regarding the Use of FBI Confidential Human Sources			
Interview or request information from members of the public and private entities			
Accept information voluntarily provided by governmental or private entities			
Engage in observation or surveillance not requiring a court order			
Mail covers			
Physical searches of personal or real property where a warrant or court order is not legally required because there is no reasonable expectation of privacy (e.g., trash covers)			
Consensual monitoring of communications, including consensual computer monitoring, is subject to legal review by the CDC or the FBI OGC. Where a sensitive monitoring circumstance is involved, monitoring must be approved by the Criminal Division or, if the investigation concerns foreign intelligence or a threat to the national security, by the National Security Division			
Use of closed-circuit television, direction finders, and other monitoring devices, subject to legal review by the CDC or FBI OGC			
Polygraph examinations			
Undercover operations			
Compulsory process as authorized by law, including Federal Grand Jury and other subpoenas and National Security Letters (Federal Grand Jury subpoenas for telephone and electronic mail subscriber records can be used during type 1 and 2 Assessments only)			
Accessing stored wire and electronic communications and transactional records			
Use of pen registers and trap and trace devices			
Electronic surveillance			
Foreign intelligence collection under Title VII of FISA			
Physical searches, including mail openings, where a warrant or court order is legally required because there is an expectation of privacy			

Authorized Method and DIOG Reference*			Approval Levels for Assessments and Predicated Investigations		
			Assessments	Predicated	Foreign Intelligence
1	5.9A	Obtain publicly available information	None Required	None Required	None Required
		Tasking a UCE to attend a religious service	Not Permitted	SSA Approval	SSA Approval
2	5.9B	Physical surveillance of a person or group (Consult the DIOG for handheld photo and video surveillance with no reasonable expectation of privacy)	[redacted] consult DIOG for requirements	None Required	None Required
		[redacted]	[redacted]	Field Office Approval	Field Office Approval
		[redacted]	ASAC Approval	ASAC Approval	ASAC Approval
3	5.9C	Access and examine FBI and other Department of Justice (DOJ) records, and obtain information from any FBI or other DOJ personnel	None Required	None Required	None Required
4	5.9D	Access and examine records maintained by, and request information from, other federal, state, local, or tribal, or foreign governmental entities or agencies	None (Unless such approval is required by MOU or other agreements)	None (Unless such approval is required by MOU or other agreements)	None (Unless such approval is required by MOU or other agreements)
5	5.9E	Use online services and resources (whether nonprofit or commercial)	None Required	None Required	None Required
6	5.9F	Interview or request information from members of the public and private entities	None Required except for contact with represented persons, members of U.S. Congress, or their staffs, White House personnel, or other substantive division requirements	None Required except for contact with represented persons, members of U.S. Congress, or their staffs, White House personnel, or other substantive division requirements	None Required except for contact with represented persons, members of U.S. Congress, or their staffs, White House personnel, or other substantive division requirements
7	5.9G	Accept information voluntarily provided by governmental or private entities	None Required	None Required	None Required
8	5.9H	Use and recruit human sources	None Required (utilize [redacted]	None Required (utilize Delta)	None Required (utilize Delta)
		Tasking a CHS to attend a religious service	SAC Approval	SSA Approval	SSA Approval
9	5.9I	Federal Grand Jury subpoenas for telephone or electronic mail subscriber information	US Attorney Office Approval (Type 1 and 2 Assessments Only)	US Attorney Office Approval	Not Permitted
10	5.9C	Pattern Based Data Mining	SORC	SORC	SORC

b2
b7E

Authorized Method and DIOG Reference*			Approval Levels for Assessments and Predicated Investigations		
			Assessments	Predicated	Foreign Intelligence
11	11.3	Mail covers			
12	11.4	Physical searches of personal or real property where a warrant or court order is not legally required because there is no reasonable expectation of privacy (e.g			
13	11.5	Consensual monitoring of communications, including consensual computer monitoring	Not Permitted	CDC or OGC Review SSA Approval	CDC or OGC Review SSA Approval
14	11.5	Consensual monitoring of communications, including consensual computer monitoring, with a sensitive monitoring circumstance	Not Permitted	CDC or OGC Review, SAC Approval, DOJ Criminal or DOJ NSD Approval	CDC or OGC Review, SAC Approval, DOJ Criminal or DOJ NSD Approval
15	11.6	Use of closed-circuit television, direction finders, and other monitoring devices			
16	11.7	Polygraph examinations		SSA Approval	SSA Approval
17	11.8	Undercover operations, Group II		CDC Review, SAC or ASAC with delegated authority; National Security cases also require NSD unit UACB	CDC Review, SAC or ASAC with delegated authority, NSB-Unit/UACB Approval
18	11.8	Undercover operations, Group I		CDC review, SAC, and AD and CUORC or UCRC (EAD/DD certain cases) Approval	CDC review, SAC and AD and UCRC (EAD/DD certain cases) Approval
19	11.9	Compulsory process as authorized by law; Federal Grand Jury and trial subpoenas		US Attorney's Office Approval	
20	11.9	Administrative Subpoenas: Drugs Administrative Subpoenas: Sexual Exploitation Administrative Subpoenas: Healthcare Fraud	Not Permitted	SAC, ASAC, SSRA, or Drug Squad SSA U.S. Attorney's Office Approval	Not Permitted
21	11.9	National Security Letters	Not Permitted	Field Office: CDC Review, ADIC or SAC Approval. HQ: NSLB Review; DD or EAD-NSB or AD & DADs CT/CD/CyD or GC or Deputy GC-NSLB Approval	Not Permitted Not Permitted
22	11.10	Accessing stored wire and electronic communications and transactional records	Not Permitted	Statute/Court Order, Consult DIOG	Not Permitted
23	11.11	Use of pen registers and trap and trace devices	Not Permitted	FISA Court or District Court Order	Only Available for Non-USPER by FISA Court order
24	11.12	Electronic surveillance			
25	11.13	Physical searches, where there is reasonable expectation of privacy, including mail openings			
26	11.14	Acquisition of foreign intelligence information in conformity with Title VII of the Foreign Intelligence Surveillance Act		FISA Court Order	FISA Court order

b2
b7E

- Section 4 of the DIOG, *Privacy and Civil Liberties, and Least Intrusive Methods* outlines the FBI's oversight, self-regulation, and strict adherence to the Constitution of the United States.

- Throughout section 4, the DIOG discusses the protection of First Amendment rights (Freedom of Speech, Freedom of the Press, Freedom of Peaceful Assembly and to Petition of Government for Redress of Grievances, and Exercise of Religion), civil liberties and privacy issues, and Equal Protection of all Americans under the Fourteenth Amendment.

- Section 4.4 of the DIOG requires FBI employees to use the "Least Intrusive" means or method possible to obtain intelligence or evidence.

- The DIOG reiterates Department of Justice (DOJ) guidance which permits the consideration of ethnic and racial identity information based on specific reporting (i.e. eyewitness accounts).

- Consideration of race or ethnicity is permitted in investigative or collection scenarios, if relevant. Examples may include investigations of ethnic-based gangs or terrorist organizations known to be comprised of members of the same ethnic grouping.

- The DIOG also reiterates DOJ guidance permitting the collection and analysis of demographics if the identification of concentrated ethnic communities will reasonably aid in the analysis of potential threats and vulnerabilities or assist domain awareness for the purpose of performing intelligence analysis.

- In addition, the locations of ethnic-oriented businesses or other facilities may be collected if their locations will reasonably contribute to an awareness of threats and vulnerabilities and intelligence collection opportunities.

- If the collection of ethnic/racial demographics is legally allowable in an investigation, it may also be "mapped" using sophisticated computer geo-mapping technology.
- These maps may be used for domain awareness of an area of responsibility, to track crime trends, or to identify specific communities or areas of interest to support specific assessments or investigations.
- Regardless of the purpose for its use, the relevance of the ethnic or racial information must be clearly demonstrated and documented.

The FBI determined that several types of information should be redacted in the Public Release of the DIOG. These types of information include:

Redaction: FBI Policy Directives
Justification: These are internal FBI policies that govern administrative and operational matters not directly related to the DIOG.

Redaction: Terms and Definitions
Justification: Knowledge of specific FBI terms and definitions could allow for circumvention of investigations and spoofing.

Redaction: Collection and/or Analysis of Information
Justification: Knowledge of these internal decision-making criteria could allow for circumvention of collection and analytical techniques.

Redaction: FBI Data Systems
Justification: Many data systems used by the FBI are proprietary.

Redaction: Scenarios & Examples
Justification: Many scenarios and examples used in the DIOG involve sensitive information, such as the names actual terrorist organizations, and provide insight into targeting, recruitment, or FBI assimilation of such organizations.

Redaction: Surveillance and Monitoring Techniques
Justification: Knowledge of these specific criteria could allow for circumvention of the techniques.

Redaction: Time Periods
Justification: Knowledge of time period requirements for investigative techniques could damage the effectiveness of the technique or allow for circumvention. For example, a person who believes he may be under investigation may stop using his celluiar phone for the specifled period of time, thereby hindering the investigation.

Redaction: Notes
Justification: Notes in the DIOG provide internal guidance to FBI operators and Intelligence Analysts.

Redaction: Internal Web and E-mail Addresses
Justification: Publicly releasing contact information of FBI staff could allow for harassment, spam, or spoofing.