



U.S. Department of Justice

Federal Bureau of Investigation

Office of the General Counsel

Washington, D.C. 20535
December 15, 2008

The Honorable John D. Rockefeller
Chairman
Select Committee on Intelligence
United States Senate

Re: Attorney General Guidelines for Domestic FBI Operations

Dear Chairman Rockefeller:

I am writing to update you on steps the FBI has taken to implement the Attorney General Guidelines for Domestic FBI Operations (AGG) and to respond to letters from Committee Members regarding the new Guidelines. As you know, Attorney General Mukasey signed the new Guidelines on September 29, 2008, and directed them to become effective on December 1st. To implement the new Guidelines, the FBI developed and put into effect the Domestic Investigations and Operations Guide (DIOG), a comprehensive 270-page collection of procedures, standards, approval levels, and explanations designed to ensure that we respect the privacy and civil liberties of all Americans as we further our transformation into a pro-active intelligence agency.

We are hopeful that the DIOG provisions discussed below will address the concerns raised by Members in letters and hearings. We intend to keep our oversight committees fully informed as we proceed forward with the implementation of the guidelines.

Assessments: As we have discussed, increased flexibility in the techniques available during Assessments is critical to the ability of the FBI to become an intelligence-driven agency. If our ability to gather information were to be limited to circumstances where we have some specific factual predication -- similar to what is required in order to open a criminal or national security investigation -- then we would not be able effectively to fulfill our mission of identifying and preventing threats to the Nation and to our communities before they materialize. Without the ability to gather information necessary to conduct intelligence analysis, the FBI would be a reactive investigative agency that investigates crimes and terror attacks after they occur, instead of the pro-active intelligence agency the American people, through their elected and appointed representatives, have directed us to become.

Although we see our ability to gather information outside of traditional predicated investigations to be critical, we fully understand that the expansion of techniques available to do so from what was authorized by the 2003 Attorney General Guidelines signed by Attorney General Ashcroft has raised privacy and civil liberties concerns. As discussed in detail below, we believe that our policies and procedures will mitigate those concerns. Moreover, as we briefed Congressional staff, it is our plan to reassess the policy judgments made in the DIOG in one year. That re-assessment will be informed by our experience in the coming year, as well as by comments and suggestions received from Congress and other interested parties. To the extent our experience reveals that, in execution, the DIOG has not mitigated legitimate concerns, our policies will be changed.

As laid out in the DIOG, there are six types of Assessments: Types 1 and 2 involve the prompt and limited checking of leads that individuals (Type 1) or groups (Type 2) are engaged in criminal behavior or pose a nation security threat; Types 3 and 4 involve collection of information necessary to the evaluation of threats and vulnerabilities (Type 3) and to facilitate intelligence analysis and planning (Type 4); Type 5 involves information gathering for the limited purpose of identifying, vetting, recruiting, validating and maintaining the cover or credibility of human sources; and Type 6 involves the collection of foreign intelligence in response to a national intelligence requirement. A number of questions have been raised about Type 3 and 4 Assessments because they appear to authorize collection activities that are the furthest removed from traditional notions of predication. (Types 1 and 2 are essentially carried forward from the old General Crimes Guidelines; Type 5 Assessments must be pursued in compliance with the Attorney General Guidelines for Confidential Human Sources (AGG-CHS), which have been in place for several years without significant concerns; and Type 6 Assessments are limited to information gathering that is related to a positive foreign intelligence requirement that has been issued by the Director of National Intelligence - the requirement serves, in effect, as the predicate that cabins the scope of the Assessment.) Accordingly, the discussion below will focus primarily on the policy determinations we made vis-à-vis Type 3 and 4 Assessments, although these policies generally apply across all types of Assessments.

Although a traditional factual predicate is not required for these Assessments, the DIOG prohibits the opening of an Assessment based on "arbitrary or groundless speculation," solely on the exercise of First Amendment rights, or solely on the race, ethnicity, national origin, or religious practice of any person or group. In addition, these types of Assessments require the approval of a supervisory special agent or analyst, who must be satisfied that the basis of the Assessment is well-founded (which typically means supported by source information, intelligence reporting, information from other agencies or foreign partners, or public source data) and that there is a rational relationship between the stated purpose of the Assessment on the one hand and the information sought and the means proposed to obtain it on the other. All such Assessments are subject to regular file reviews (at least four (4) times per year) during which the supervisor must determine whether the Assessment should remain open. Finally, if any such Assessment involves a "sensitive investigative matter," legal counsel review and approval by the Special Agent in Charge (SAC) are required as well. Sensitive investigative matters include all

political corruption matters, religious organizations and persons prominent in them, news media, certain 3 academic entities and persons and any national security matter involving an elected official or political candidate. We believe this combination of controls will ensure that these sorts of Assessments do not devolve into intrusive collection of personally-identifiable information on large numbers of persons as to whom the FBI has no factual predication.

Assessment techniques: In addition to setting policy to ensure that Assessments have a proper, appropriately-defined purpose, we also looked hard at those techniques that are now available that had not previously been available during national security Assessments: physical surveillance; recruiting and tasking of human sources; and so-called "pretext" interviews. Our goal was to ensure that the use of these techniques during Assessments was accompanied by appropriate levels of oversight.

As an overarching control, the use of all techniques is subject to the requirement that it be the least intrusive feasible method of obtaining the desired information. For example, if a person's address can be obtained from public source data, physical surveillance to learn where he lives would not be permitted. Further, for Type 6 Assessments (information that is related to a positive foreign intelligence requirement), the use of all techniques is subject to the additional requirement that our employees must operate openly and consensually with United States Persons to the extent practicable.

In addition to those overarching controls, physical surveillance can only occur in areas open to the public (i.e., areas as to which there is no constitutionally-protected expectation of privacy), must have a specifically-articulated purpose, must be authorized by a supervisor, and is limited to 72 hours. Additional surveillance beyond 72 hours must be justified and may only be approved by the supervisor for 72 hours. There is no limit to the number of times a supervisor may approve a 72 hour block of surveillance, but each instance must be separately justified and approved. The goal of these controls is to permit employees to respond to a lead quickly and effectively or to learn limited factual information necessary to achieve the purpose of the Assessment while precluding long-term 24/7 surveillance of the lifestyle or habits of a person as to whom no investigative predication exists. We believe these limits appropriately balance our need to gather information proactively with our citizens' need to be free from unnecessary surveillance.

Recruiting and tasking sources without having an investigation open were not prohibited under the criminal guidelines for purposes of the prompt and limited checking of leads but were prohibited under the national security guidelines during threat Assessments. These techniques have now been authorized during Assessments across all FBI investigative programs. Further, on November 26, 2008, the Attorney General signed an order amending the AGG-CHS to provide that any lawful technique (not just "Assessment techniques") can be used for the purpose of identifying human sources, or assessing the suitability, credibility or value of persons as human sources, and maintaining the cover or credibility of human sources. Source recruitment, vetting, and validation are critical to the FBI's success as an intelligence agency. The AGG-CHS set forth

the rules that govern the use of FBI sources, and those guidelines have not been replaced by the new AGG. Although the Attorney General has now made available an expanded range of techniques for this purpose, we have limited our employees to the use of Assessment techniques for this purpose until we can be sure that the policies implementing the DIOG and those implementing the AGG-CHS are appropriately harmonized. We will keep your staff informed as we do so.

Putting aside the recent expansion of the techniques available for vetting and validating sources, the most significant concern raised with regard to the changes in the investigative guidelines regarding the tasking of sources related to the potential that sources would be used to infiltrate legitimate organizations as part of Assessments. As you know, pursuant to Executive Order (E.O.) 12333, no one acting on behalf of a member of the Intelligence Community may join or otherwise participate in an organization in the United States on behalf of the Intelligence Community without disclosing his or her affiliation except in accordance with procedures approved by the Attorney General. To that end, on November 26, 2008, the Attorney General, in consultation with the Director of National Intelligence (DNI), signed the policy that will govern the undisclosed participation (UDP) of FBI employees and sources in organizations and business entities. This policy has been incorporated into the DIOG and limitations have been added to ensure the technique is used properly.

At base, in addition to the overarching requirement that UDP be the least intrusive means feasible, the FBI's UDP policy imposes increasingly high supervisory approval requirements as the proposed involvement of the source in the organization becomes more active or poses a higher risk of affecting First Amendment rights. Thus, UDP in a normal business setting (e.g., where the source is an ordinary employee) during an Assessment requires first level supervisory approval; UDP during an Assessment in which a source is tasked to join an organization that advocates political change (based, for example, on credible information that suspected terrorists intend to exploit the organization for their own purposes) requires legal review, SAC approval and notice to headquarters.

Finally, the new guidelines drop the prohibition on "pretext interviews" -- a term that was never defined in the previous guidelines and that was subject to various interpretations within the FBI -- outside of predicated investigations. Although not defined by the guidelines, we never understood "pretext" was prohibited in the course of incidental or inconsequential interaction with the public. Because of the extremely varied understanding of what "pretext" means, we chose not to use the term at all in the DIOG. Instead, when discussing the policies that control interviewing or requesting information from members of the public and private entities, our policy limits the authority our employees have to withhold their FBI affiliation or the purpose of the interaction. In order to resolve Assessments in an effective and timely manner, FBI employees are permitted to attend public events, maintain an anonymous presence on the public Internet, engage in incidental contact or interaction with the public, and engage in similar activity without disclosing that they work for the FBI. The authority not to disclose FBI affiliation during interactions with the public during Assessments is limited to situations which, we believe, are

relatively non-intrusive and respectful of the rights of others and, even then, is authorized only when the technique is reasonably required to achieve the purpose of the Assessment. Employees are not permitted to conduct a traditional formal interview using a false identity and are not permitted to engage in "undercover activity," as that term is defined by the Attorney General Guidelines for FBI Undercover Operations, during an Assessment. Finally, they are not permitted to state a false purpose for contact with a member of the public that is coercive or that may be harmful to the rights or reputations of others (e.g., falsely stating that we are investigating a person's neighbor for sexual misconduct with a minor).

Racial and ethnic profiling: From the time the initial drafts of the new AGG-DOM were shared outside the Department of Justice, some have raised concerns that the Assessment authorities permit or will lead to racial and ethnic profiling. We share the concern and have devoted considerable time and effort to educating our employees regarding how race and ethnicity can - and cannot - be used during Assessments. This is an issue that we expect to monitor closely to ensure compliance with the DIOG, the AGG-Dom and the Constitution.

It is commonly accepted that race and ethnicity may be used as a specific identifier of a suspect of a crime or incident based on credible information (i.e., if the FBI receives a lead that a short, white male robbed a bank, the FBI can limit the pool of suspects to short, white males without running afoul of prohibitions on racial or ethnic profiling). As accepted as that proposition is, the prospect that race or ethnicity will be used as part of broader intelligence Assessments creates anxiety that the FBI will substitute ethnicity for information and that our activities will cast doubt on broad swaths of the population based only on race or ethnicity.

Chapter 4 of the DIOG contains extensive guidance designed to prevent racial or ethnic profiling. Specifically, it prohibits the use of race or ethnicity as the primary, dominant or sole factor in commencing an Assessment or investigation. It also prohibits basing investigative activity solely on any combination of prohibited factors-such as public statements by a Muslim from the Middle East. Finally, it prohibits the collection and analysis of ethnicity-based behavior that has no specific and well-founded relationship to a proper investigative purpose.

Nevertheless, under certain circumstances, the AGG and the DIOG do permit the consideration of race or ethnicity. If there is an articulable and well-founded nexus between that factor and the threat being assessed or the group being investigated, then race and ethnicity may be considered. For example, some criminal gangs and some terrorist organizations consist exclusively or nearly exclusively of persons of common ethnic background. When considering whether a certain person is or may be associated with such a group, it is proper to consider ethnicity to eliminate that person as an associate and it is proper to consider ethnicity as one of many factors to consider when assessing whether he or she is a possible member. To use an example: if in the wake of the attacks in India, the FBI wished to conduct an Assessment to determine whether Lashkar-e-Taiba (LET) has a presence in any particular field office's area of responsibility, it would be entirely appropriate to consider intelligence community reporting that virtually all members of LET are Pakistani Sunni Muslims. If a field office reported that it has

no ethnic Pakistani presence in the area, that would be a good indicator that it does not have an LET presence. Conversely, if a field office determined by census data that it has a large first and second generation Pakistani-American presence, that would be an indication that further work should be done to ascertain whether there may be adherents to LET in the area.

The DIOG also emphasizes that it is appropriate to collect information regarding the characteristics of a criminal or terrorist organization - patterns of behavior and conduct, for example - but it is not appropriate to collect information regarding the characteristics of the ethnic group with which the organization is identified. For example, while most members of Hizballah are from Lebanon, most Lebanese in the United States are not associated with or supportive of Hizballah. That being the case, when assessing the threat from Hizballah, the DIOG commands FBI employees to collect intelligence based on the known or suspected behavior and conduct of Hizballah, not the behavioral characteristics of the broader Lebanese community. This approach, which will be reinforced in training, recognizes the proper, limited role of ethnic identity as an investigative factor. It also will concentrate resources where they will be the most effective and should go far in reassuring ethnic communities in the United States that they are not being targeted by the FBI.

Foreign Intelligence Collection: The AGG-DOM also provide guidelines for the FBI's collection of foreign intelligence that is responsive to national intelligence requirements set by the DNI. As we have acknowledged, this authority potentially allows the FBI to gather information about Americans that is unrelated to criminal conduct or national security threats. This authority derives from the Intelligence Reform and Terrorism Prevention Act of 2004 and E.O. 12333, both of which impose upon the FBI responsibility to fulfill national intelligence requirements issued by the DNI, particularly with respect to information gathered within the United States.

This aspect of the FBI's mission has raised concerns among some. Although we understand the concerns, we believe that this very small program has substantial controls to ensure it is conducted in a way that respects the privacy interests of Americans. First, the vast majority of foreign intelligence collected by FBI employees that satisfies DNI requirements will be collected incidentally as part of national security and criminal investigations (e.g., during FISA collection that is conducted for counterintelligence purposes, the FBI may incidentally gather information regarding the military or diplomatic intentions of a foreign government). It is anticipated that only a very small and isolated portion of FBI collection efforts will be directed at what we call "positive foreign intelligence" (positive FI), i.e., foreign intelligence that is not related to international terrorism or counterintelligence. Because such foreign intelligence will be about the plans and activities of other countries, it is not likely to be focused on particular U.S. Persons. Moreover, when collecting positive FI, agents are required to operate openly and consensually with Americans to the extent operationally feasible and must always use the least intrusive technique that is feasible. Finally, investigations opened for the purpose of collection of positive FI can only be authorized by FBI Headquarters and will be closely monitored.

Sensitive Operations Review Committee: The DIOG establishes the Sensitive Operations Review Committee (SORC), a committee that is modeled on the Criminal Undercover Operations Review Committee (CUORC), which has been an integral and successful part of the FBI's undercover program for nearly 30 years. Like the CUORC, the SORC will provide review and approval of the most sensitive operations and initiatives (in both Assessments and investigations) that are not reviewed by the CUORC or other similar body comprised of senior FBI and Department of Justice executives. One example of a proposed initiative that must have prior SORC approval is pattern-based data mining. In addition, the DIOG requires notice to the SORC of other, less sensitive operations and initiatives for the purpose of ensuring high level monitoring, evaluation of trends, and to provide the ability to report the use of these matters to higher authority as required. SORC procedures and the full scope of its purview are still being developed, but we expect to complete this process in the near future. We also expect the SORC will provide our executive and legislative branch overseers with a measure of confidence in FBI operations under the new AGG, just as CUORC has done for the FBI undercover program.

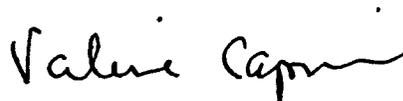
Public Release: We have provided draft copies of selected portions of the DIOG to congressional staffers and civil rights and civil liberties advocacy groups to read but not retain. Although we found that process to be valuable and we obtained useful input, we fully understand the conditions we imposed did not allow for the sort of full public vetting many would like. We are in the process of reviewing the DIOG to determine what portions can be publicly released without unduly exposing sensitive investigative techniques and methods.

Future plans: The FBI has developed a variety of methods designed to ensure the DIOG is being implemented properly and effectively. First, web-based training on the AGG and the DIOG was mandated for all operational personnel. That training was supplemented by in-person, problem-based training of the Special Agents in Charge. In-person training was also conducted for the Chief Division Counsel and the Compliance Officers. All of that training will be supplemented with future training of field office personnel that will require them to apply the DIOG provisions to sample scenarios. Second, the Office of Integrity and Compliance has devised an extensive monitoring initiative pursuant to which the managers of the significant investigative programs will examine Assessment documentation during the next year to determine on-going compliance with DIOG provisions. Third, we are encouraging our employees to report mistakes, inconsistencies, missing policies, and misunderstandings to the Corporate Policy Office so that appropriate guidance can be provided. Fourth, the Department of Justice and FBI OGC are continuing to conduct "National Security Reviews," in which teams of DOJ and FBI attorneys visit field office and national security headquarters units to review investigations and Assessments. Finally, as mentioned above, the FBI plans an extensive re-evaluation of the DIOG, including whether its protective provisions and limitations are adequate, one year from the date of issue. We would hope that during the year leading up to that re-evaluation we will also have the opportunity to receive input from Congress and the public, including from civil advocacy and civil rights groups, regarding the DIOG. To the extent we see provisions that need to be modified or receive suggestions that we believe are valuable, we will make appropriate revisions.

Conclusion: The DIOG is a significant part of the FBI's effort to transition itself into an intelligence-driven agency. We believe the new AGG give our employees the tools they need to protect the Nation from criminal and national security threats while protecting the privacy, civil rights, and civil liberties of all persons. As the Director testified before the Senate Judiciary Committee on September 17, 2008, "We know that if we safeguard our civil liberties but leave our country vulnerable to terrorism and crime, we have lost. If we protect Americans from terrorism and crime but sacrifice our civil liberties, we have lost. We are always mindful that our mission is not just to safeguard American lives, but also to safeguard American liberties." We strongly believe that the policies established in the DIOG strike the appropriate balance so that we can achieve all of those goals.

I thank you for your interest in this matter and the opportunity to explain key provisions of the DIOG. We will advise your staff as soon as public release determinations are made.

Sincerely,



Valerie Caproni
General Counsel

1 - The Honorable Christopher S. Bond
Vice Chairman
Select Committee on Intelligence
United States Senate