U.S. Department of Justice

Office of Legislative Affairs

Washington, D.C. 20530

January 25, 2008

The Honorable Patrick J. Leahy
Chairman
Committee on the Judiciary
United States Senate
Washington, D.C. 20510

Dear Mr. Chairman:

Please find enclosed responses to questions posed to FBI Director Robert S. Mueller III, following Director Mueller's appearance before the Committee on March 27, 2007. The subject of the hearing was "Oversight of the Federal Bureau of Investigation."

The Office of Management and Budget has advised us that from the perspective of the Administration's program, there is no objection to the submission of this letter. Please do not hesitate to contact this office if we may be of further assistance with this, or any other matter.

Sincerely,

Brian A. Benczkowski
Principal Deputy Assistant Attorney General

Enclosures

cc: The Honorable Arlen Specter
Ranking Minority Member

**Responses of the Federal Bureau of Investigation
Based Upon the March 27, 2007 Hearing Before the
Senate Committee on the Judiciary
Regarding FBI Oversight**

Questions Posed by Senator Leahy

NATIONAL SECURITY LETTERS

1. Despite the recent report by the Department of Justice Inspector General finding illegal and improper use of National Security Letters and so-called "exigent letters," I understand that the FBI may still be using exigent letters. Is the FBI still using exigent letters and if so, why have you not stopped this practice?

Response:

Effective March 1, 2007, the FBI prohibited the use of "exigent letters" as they are described in the report by the Department of Justice (DOJ) Office of the Inspector General (OIG) (that is, a letter that simply asserted that exigent circumstances existed and advised that a grand jury subpoena or national security letter (NSL) had been requested when, in fact, it had not). That practice has been stopped. The OIG objection to the "exigent letters" rested on several facts: (1) there was not always a true emergency and, even when there was, it was not documented; (2) the letters appeared to be coercive; (3) the letters advised that future legal process of a particular type (grand jury subpoena) had already been requested when, in fact, no legal process had yet been requested and the anticipated future legal process was different from that described in the letter; and (4) in many cases, the future legal process was not delivered at all or was delivered months later.

Emergency disclosures by communications service providers to the government pursuant to 18 U.S.C. § 2702(c)(4) are entirely lawful and will continue under appropriate circumstances. Section 2702(c)(4), which has been a part of the Electronic Communications Privacy Act since 2001, provides that an electronic communications service provider may voluntarily disclose to a governmental entity a record or other information pertaining to a subscriber or customer (other than the contents of communications) if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay. On March 1, 2007, the FBI reaffirmed its intention to continue to use this valuable tool, setting out clear procedures for invoking this provision. Pursuant to this process, the FBI can present a provider

with information indicating the existence of an emergency and asking the provider to produce covered information. Pursuant to these procedures, the FBI Special Agent (SA) seeking the records must make clear to the provider that any production of documents is entirely voluntary, no other legal process may be promised, and, by policy, the emergency justifying the request must be documented.

2. The Attorney General's guidelines require that the FBI use the least intrusive investigative tools to obtain the information that it needs. During the recent hearing that the Committee held on NSLs, Inspector General Glenn Fine testified that the least intrusive NSL are the ones seeking telephone records and that NSLs for financial records and for credit reports are more intrusive of Americans' privacy. During the hearing, you testified that you believed that NSLs seeking credit reports could be intrusive, but less so than those seeking telephone toll records. Does the FBI have a policy in place requiring that agents first use the least intrusive types of NSLs - such as NSLs seeking telephone toll records - when conducting investigations? If not, will you adopt such a policy to better safeguard Americans' privacy?

Response:

The requirement to use the "least intrusive means" originates in Executive Order 12333 and is reiterated in Attorney General (AG) Guidelines. This mandate applies to all intelligence activities conducted by the FBI, and generally requires consideration of the relative intrusiveness of various investigative techniques. For example, obtaining toll billing records from a communications service provider is clearly less intrusive than searching a subject's home for the same information. The FBI's Office of the General Counsel (OGC) is drafting advice to the field to assist SAs in applying the "least intrusive means" concept during national security investigations.

3. I am also concerned about the kind of information that the FBI is seeking in its National Security Letters.

a. Is it true that most of the FBI's NSLs seeking telephone or Internet records under the Electronic Communications Privacy Act ("ECPA") seek only subscriber identifying information? What percentage of these NSLs seek other transactional information, such as toll records or billing records?

Response:

The response to this inquiry is classified and is, therefore, provided separately.

b. With regard to NSLs that seek bank or other financial records under the Right to Financial Privacy Act, the Fair Credit Reporting Act and the National Security Act, what percentage of these NSLs seek detailed financial transaction information, such as bank account records and/or full credit reports?

Response:

The response to this inquiry is classified and is, therefore, provided separately.

4. During the hearing, you testified that the information that the FBI improperly obtained through unlawful NSLs has been placed into the FBI's database. What steps have you taken to track all of this improperly obtained information, and have you removed it from all of the FBI's files and databases?

Response:

The FBI's Inspection Division has been directed to investigate the use of NSLs as an investigative tool in all 56 FBI field offices and at FBI Headquarters (FBIHQ) to address the concerns raised in the OIG report. Both the Inspection Division and the OIG are also taking an additional, and closer, look at the use of "exigent letters" by the FBIHQ unit identified in the OIG report. If any of those reviews reveal that the FBI used "exigent letters" to obtain information that was not relevant to an authorized national security investigation, that information will be removed from the FBI's databases and destroyed.

5. Has any of the information improperly obtained through unlawful NSLs been used in any criminal cases or investigations and, if so, have you notified appropriate authorities at the Justice Department in order to make sure none of this information has been improperly used in our justice system?

Response:

The information obtainable through NSLs, the overwhelming majority of which is subscriber information or toll billing records, would only rarely be used as evidence in a courtroom. Such information is typically a very small part of a very large and complex investigation, most often a small stepping stone through which one terrorism subject is linked to others. The primary benefit of NSLs is not to obtain evidence for criminal prosecutions (which is more the function of other vehicles, such as grand jury subpoenas), but instead to obtain leads to other information; these pieces of information form the building blocks of national security investigations. In popular parlance, NSLs allow us to obtain "dots" that can be connected to lead to the identification and disruption of terrorist networks.

As indicated in response to Question 4, above, if the FBI determines that we have obtained through exigent letters information that was not relevant to an authorized investigation or was not obtained in conjunction with an actual emergency, this information will be removed from FBI databases. In addition, a report to the President's Intelligence Oversight Board (IOB) will be made in appropriate cases.

6. Do you believe that the FBI's failure to follow the law in obtaining NSLs may be exculpatory, or *Giglio* information, that needs to be disclosed if the information is used in court?

Response:

Under the circumstances in which these NSLs and the NSL-derived information have been used, we do not believe the shortcomings identified in the OIG report constitute exculpatory, or *Giglio*, material. We understand, however, that what might be helpful to an individual defendant or might bear on the credibility of a witness in an individual case can be very fact-specific. If the OIG, OPR, or the FBI's Inspection Division determine that an FBI employee violated the law relative to the use of NSLs, that information might constitute impeachment material if that employee were subsequently to testify in a related criminal proceeding. In such a circumstance, the information would be provided to the appropriate Assistant United States Attorney (AUSA) for evaluation. Likewise, if a particular criminal defendant were to move to suppress or dismiss based on an alleged improper use of an NSL, then facts about that particular NSL might be relevant. We would note, however, that there is not typically a suppression remedy for violations that do not rise to a Constitutional level.

7. The Judiciary Committee has received letters and briefings from FBI and Justice Department officials in the past, assuring us that NSLs were being used properly, and that all appropriate safeguards and legal authorities were being followed. For example, in a November 2005 letter to this Committee (attached), the Justice Department asserted emphatically that the FBI was not abusing the process for seeking NSLs, and that all NSL activity was accurately being reported to Congress as required by law. In light of the Inspector General's report, will you review those letters and briefings to see if anyone at the FBI or the Justice Department has misled this Committee about NSLs?

Response:

The FBI has acknowledged shortcomings in its efforts to ensure adequate safeguards were in place to oversee the use of NSL authorities and in tabulating data the for purposes of Congressional reporting. There are ongoing

investigations by the FBI's Inspection Division, DOJ's OIG, and DOJ's Office of Professional Responsibility (OPR). If any of these investigations indicate that an FBI employee intentionally misled Congress, appropriate steps will be taken and our Congressional oversight committees will be informed.

8. According to the Inspector General's report, one of the major reasons that the FBI failed to report thousands of NSLs to Congress was because of a malfunction in a FBI's computer database. Apparently, this breakdown occurred in 2004, causing the loss of information about more than 8,000 NSL requests. What was the cause of this malfunction, and have you corrected it? Why did you fail to report this problem to Congress?

Response:

What the OIG report described as a "crash" and data loss appears to have been an incident in which the creator of OGC's NSL database was locked out from accessing the database. That lock-out was bypassed by a technician, who imported the data into a new database. The "glitch" was fixed and there appears to have been no loss of data.

Review of the data since release of the OIG report reinforces our belief that no data was lost. We are discussing our review with the OIG in an effort to reconcile our disparate conclusions and are continuing to work to determine the extent of data entry errors that affected prior Congressional reporting.

9. You testified during the hearing that the FBI has revised its internal policy on NSLs and adopted the recommendations contained in the Inspector General's report. But, in 60 percent of the NSLs that the Inspector General reviewed, he found widespread failure on the part of the FBI to comply with its own internal control policies. Given this track record, how can you assure Congress that the new policies that you are implementing will prevent future abuses of NSLs, when the Bureau clearly failed to follow its own policies in the past?

Response:

The IG did not find that 60 percent of the NSLs reviewed had mistakes. The IG reviewed 293 NSLs and found 22 errors (7 percent) that he classified as potential errors that should be considered for reporting to the President's IOB. Of the 22 errors the IG identified as potential errors, 10 were third party errors (i.e., the recipient of the NSL provided the FBI information that was not requested). The remaining 12 out of 293 NSLs examined (or just 3.4 percent of all NSLs examined) are FBI errors. But even that statistic overstates the number of NSLs that "misused" the NSL authority. Of the 12 errors attributable to the FBI, 2 involved full credit reports in counterintelligence investigations, and 1 involved

information that was arguably content from an electronic communications company. The remainder of the errors did not affect anyone's statutory rights and are best characterized as administrative errors on the FBI's part. Thus, only 3 of the 293 NSLs reviewed (1 percent) contained significant errors.

Nevertheless, the FBI took the IG's findings very seriously. Following the OIG report, the FBI has prepared comprehensive guidance concerning the use of NSLs. Every proposed NSL must be reviewed by the Chief Division Counsel in each FBI field office or by an attorney in OGC's National Security Law Branch (NSLB) at FBIHQ, including review of the relevance of the request to an authorized investigation and the predication for that investigation. In addition, NSLB is developing a training curriculum, which will be mandatory for all employees involved in the NSL process, to address problems created by confusion and lack of familiarity with the provisions and requirements of the various statutes authorizing NSLs. Even before the OIG report was published, the FBI had begun work on a database, based on the successful "FISA Management System," that will permit the electronic transfer of NSL-related data between databases (this transfer is currently being accomplished manually). Finally, the FBI's Inspection Division is investigating in more detail many of the problems identified in the OIG report. This review should identify any areas that require closer scrutiny. Taken together, these measures will both provide a more user-friendly business process for FBI personnel who use NSLs as an investigative tool and enhance management's audit and oversight capabilities. This system will also enhance the accuracy of the NSL reports provided to Congress.

The FBI has also recognized the need to create a compliance program to ensure we have appropriate policies, procedures, audit capabilities, and training for all our activities. The FBI's compliance program will be modeled after similar programs in the public and private sectors. While it is too early to say with certainty what the program will look like, it will most likely incorporate features common to most successful programs, such as a written compliance policy, a central compliance officer and office, a senior-level compliance committee, access to and the ability to draw upon the resources of the organization, and an implementing strategy that adjusts as new threats and programs are identified. Audits of practices, not just procedures, will be an essential component of the program, as will effective "two-way" communication channels. In addition, OGC will continue to meet s regularly with DOJ's National Security Division (NSD) to discuss appropriate policies in the national security arena.

In addition, DOJ's NSD and the FBI's NSLB, along with officials from DOJ's Privacy and Civil Liberties Office, will conduct at least 15 national security reviews of the FBI's field offices in calendar year 2007. Those reviews will

broadly examine the FBI's national security activities, its compliance with applicable laws, policies, and AG Guidelines, and its use of various national security tools, including NSLs. The reviews are not limited to areas in which shortcomings have already been identified; instead, they are intended to enhance compliance across the national security investigative spectrum. At the AG's direction, the NSD will also review all referrals by the FBI to the President's IOB, focusing on whether these referrals indicate that changes in policy, training, or oversight mechanisms are required. The NSD will report to the AG semiannually on such referrals and will inform DOJ's Chief Privacy and Civil Liberties Officer of any referral that raises serious civil liberties or privacy issues.

10. During the hearing, you testified that "[t]he relevant standard established by the PATRIOT Act for the issuance of National Security Letters is unrelated to the problems identified by the Inspector General." Yet, given the broad scope of the abuses uncovered by the Inspector General's report, it appears that there is a need for additional checks and balances on the authority to issue NSLs. Do you believe that an independent check on the NSL process, such as approval of NSLs by a judge, a Justice Department attorney, or an outside review panel, would improve the NSL approval process and prevent future abuses?

Response:

We do not agree that the OIG uncovered "a broad scope" of FBI abuses. On the contrary, the OIG report identified a problem in one FBIHQ unit that used exigent letters. The unreported IOB violations identified by the OIG (at p. X of the report) do not reflect widespread abuse by the FBI; while 22 of the 293 NSLs reviewed by the IG (7.5 percent) were said to indicate some sort of violation, 10 of these 22 NSLs (45 percent) were the result of a third-party error in providing the FBI with material outside of the request. As discussed in response to Question 9, above, of the 12 errors attributable to the FBI, 2 involved obtaining full credit reports in counterintelligence investigations, and 1 involved obtaining information that was arguably content from an electronic communications company. The remainder of the errors did not affect anyone's statutory rights and are best characterized as failures of care on the FBI's part. Thus, only 3 of the 293 NSLs reviewed (1 percent) contained significant errors. We do not minimize those errors, and we recognize that the OIG's follow-up NSL investigation, which is ongoing, may identify additional problems in the FBI's use of NSLs, but we believe that requiring either a court or an AUSA to approve an NSL would be an overreaction to the level of error, and may not have prevented one of these errors. We have taken significant steps to reduce that 1 percent error rate without altering the approval process. For a more complete discussion of the steps the FBI has taken in this regard, please see our response to Question 9, above.

Finally, we note that altering the NSL approval process to require review by a judge, DOJ attorney, or outside panel would largely eviscerate the usefulness of this tool. Such a change would likely result in either a significant slowing of our national security investigations, with possible adverse impact on our national security, or abandoning NSLs in favor of grand jury subpoenas when possible. Grand jury subpoenas are less transparent than NSLs because they include no reporting requirements. Moreover, if we were to lose the efficient use of NSLs in terrorism investigations, we would have the anomalous result that our investigators would have access to more agile tools to investigate narcotics and child pornography (where administrative subpoenas have long been available) than they do to investigate threats to our national security.

LIBRARY RECORDS

11. I appreciate your March 30, 2007, letter responding to my question about how often the FBI has used NSLs to obtain records from libraries and educational institutions. In your letter, you state that the FBI's Office of General Counsel has maintained an informal list of the number of NSLs served on educational institutions or libraries; however, you also state that this list may not be complete or accurate. Given the importance of this issue to Americans' privacy and civil liberties, will the FBI agree to formally track the number of NSLs issued to libraries and educational institutions and periodically report this figure to Congress?

Response:

The FBI will track NSL recipients and will be pleased to address related inquiries by our Congressional oversight committees. It is important to note that the FBI does not serve NSLs on libraries or educational institutions per se, but instead on "electronic communication services" and "financial institutions" as those terms are defined in the statutes authorizing NSLs. Similarly, the FBI would direct a Right to Financial Privacy NSL to an educational institution only if it were providing financial services to its employees or students.

12. During the hearing, you cited the Inspector General's Report on Section 215 of the PATRIOT Act, which found that the FBI rarely used this authority to obtain library records. However, I am concerned that the FBI is using other provisions in the PATRIOT Act to obtain this information, thereby circumventing the safeguards and reporting requirements of Section 215. For example in 2005, the FBI issued NSLs to four Connecticut libraries asking them to surrender "all subscriber information, billing information and access logs of any person" related to a specific library computer during a specific time period, pursuant to Section 505 of the PATRIOT Act. These NSLs also

prohibited the librarians from disclosing the fact that they had received the NSLs or their contents -- the so-called "gag order" under the PATRIOT Act.

a. Please describe the circumstances surrounding the FBI's decision to issue these National Security Letters.

Response:

We believe the report that NSLs were served on four Connecticut libraries is erroneous. The FBI served one NSL on the Executive Director of Library Connections, Inc., an Internet service provider that furnishes computer services to several libraries. No library was served. Three directors of Library Connections, Inc., have apparently described themselves as individual NSL recipients, but the case agent who served the NSL on one official had no contact with the others.

This one NSL was issued in order to follow up on an alleged local connection to international terrorism. The FBI sought subscriber information, toll billing records, and logs relative to those who had access to the communications services during relevant times. The NSL was very narrowly tailored to seek information for only a 45-minute period.

b. Please identify all of the PATRIOT Act provisions that the FBI has used to obtain library records from libraries and educational institutions?

Response:

We understand the term "library records" to mean records of libraries that reflect loans of books, movies, and similar materials to library patrons. We are not aware of any use of the USA PATRIOT Act to obtain such "library records" from educational institutions or libraries. As indicated in the previous response, we are aware that one NSL was served on a company that provides computer services, including Internet access, to several libraries. This NSL was authorized by 18 U.S.C. § 2709, which was amended by section 505 of the USA PATRIOT Act.

c. Is the FBI circumventing the requirements of Section 215 by relying on other provisions in the PATRIOT Act to obtain this information?

Response:

The premise of this question appears to be that the sole authority for obtaining information from a library or educational institution is section 215 of the USA PATRIOT Act. In fact, libraries and schools are subject to grand jury subpoenas

and NSLs under certain circumstances. If a library provides Internet service that meets the definition of an electronic communication service, as defined in 18 U.S.C. § 2510(15), then the library is an electronic communication service provider to which the provisions of 18 U.S.C. § 2709 apply. Similarly, while special rules govern the acquisition of a student's records from a university, an NSL can be used to obtain toll billing records if the school is functioning as a telephone company relative to the provision of campus telephone services.

ARAR/WATCHLIST

13. I have asked before about Maher Arar, a Canadian citizen who when returning home from a vacation in 2002, was detained by federal agents at JFK Airport in New York City on suspicion of ties to terrorism, and was sent to Syria, where he was held for 10 months. After I pressed the Attorney General about the Arar case at a hearing in January, Senator Specter and I were finally granted a classified briefing. After that briefing, we wrote to request a Justice Department investigation into the matter and have learned that the Department's Office of Professional Responsibility is looking into the Department's legal decisions.

a. Is the FBI taking any steps to evaluate whether your agents and officials acted properly in the Arar matter, particularly with regard to the original decision to send him to Syria, rather than to Canada?

Response:

DOJ's OPR opened an investigation based on a referral from the Department of Homeland Security (DHS) OIG concerning the detention and subsequent removal of Maher Arar, a Canadian citizen, to Syria from JFK Airport in New York City. The FBI's Inspection Division conducted an internal review of the actions of FBI personnel with respect to this matter. The FBI will cooperate fully with the DOJ OPR review and will defer final adjudication regarding the of actions of FBI personnel until the DOJ OPR review is concluded.

b. Given that a past OPR investigation of a politically sensitive matter, specifically the NSA's warrantless wiretapping program, appears to have been blocked, will you commit to cooperate with OPR's investigation of the Arar case?

Response:

The FBI cooperates with DOJ's OPR on an ongoing basis, and commits to continuing to do so as appropriate in this matter.

c. What steps has the FBI taken to ensure that you do not participate in sending other people in the future to places where they will be tortured?

Response:

As a signatory to the Convention Against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment ("The Convention Against Torture," or "CAT"), it is the obligation of the United States not to "expel, return ('refouler') or extradite a person to another State where there are substantial grounds for believing that he would be in danger of being subjected to torture." (CAT, Article 3(1).) The department with primary responsibility for knowing the human rights record of foreign countries (and, therefore, knowing whether there should be concern about potential violations of the CAT) is the Department of State. The FBI does not have the authority to deport people from the United States, to determine the country to which a deportee will be delivered, or to ascertain whether such a deportation might run afoul of the CAT. Our role in deportations is to share whatever relevant information we might possess to assist the agencies that do have those responsibilities to fulfill them.

14. Despite having been cleared of all terrorism allegations by Canada, Mr. Arar remains on a United States terror watch list. In fact, *The Washington Post* reported on Sunday that our watch lists keep growing, with the Terrorist Identities Datamart Environment ("TIDE") - the master list from which other lists, like the No Fly list, are taken - now numbering about 435,000 people.

a. Doesn't such a large and constantly growing list actually make it harder for the FBI and others to use the information? Wouldn't the FBI and other agencies be able to do much more to protect us with a more controlled list, focused on serious and proven threats?

Response:

The FBI's counterterrorism watchlisting strategy is designed to enable law enforcement and screening personnel to effectively detect, disrupt, and/or assist national security components in tracking those suspected of involvement in terrorist networks. This strategy empowers Federal, State, local, and tribal security and law enforcement officials, who serve as "first preventors" in the global war on terrorism. The foundation of the FBI's counterterrorism watchlisting strategy is the requirement that the subjects of both preliminary and full-field investigations be watchlisted.

The circumstances in which a preliminary or full-field counterterrorism investigation may be initiated are dictated by the October 31, 2003 AG Guidelines for FBI National Security Investigations and Foreign Intelligence Collection. Because the subjects of these investigations are automatically nominated for inclusion on the watchlist, the value and accuracy of the watchlist depend on the FBI's compliance with these AG Guidelines in initiating counterterrorism investigations. Other United States agencies that submit watchlist nominations are similarly required to ensure their nominations are made pursuant to appropriate guidelines. The Terrorist Screening Center (TSC) reviews all watchlist nominations to ensure they are adequately supported and meet Terrorist Screening Database (TSDB) criteria. The TSC also works hard to ensure that individuals are promptly removed from the watchlist as soon as it receives information indicating removal is appropriate.

It continues to be imperative that TSDB nominations be properly supported and that entries be promptly removed when errors occur or other circumstances warrant deletion. It is accuracy, far more than volume, that defines the value of the TSDB, and the FBI is committed to ensuring that our policies and practices ensure the greatest possible accuracy.

b. *The Washington Post* article also noted the difficulty that people on the list, or with names similar to people on the list, have in getting off of government lists -- which restrict their travel and their lives. The Government Accountability Office issued a report last year setting out some of the failures throughout the government in allowing individuals effective redress if they are wrongly placed on these lists. In light of the Arar situation, Senator Specter and I asked the Government Accountability Office to update their review. What steps has the FBI taken to allow individuals who may be wrongly on watch lists to challenge and correct those designations?

Response:

In January 2005, the TSC established a formal watchlist redress process. That process allows agencies using TSDB data during a terrorism screening process (screening agencies) to refer individuals' complaints to the TSC when it appears those complaints are watchlist related. The goals of the redress process are to provide for timely and fair review of individuals' complaints and to identify and correct any data errors, including errors in the TSDB itself.

The TSC has worked closely with screening agencies and others to develop a redress procedure that receives, tracks, and researches watchlist-related complaints and corrects inaccurate TSDB or other TSC data that is causing an individual hardship or difficulty during the screening process. While the terrorist

watchlist is an effective counterterrorism tool in large part because its contents are not revealed, and the redress process consequently does not inform individuals whether they are on the terrorist watchlist, the TSC's inability to provide transparency to affected individuals means the burden is on the government to perform a critical, in-depth review of the information supporting a person's inclusion in the TSDB to ensure it meets the watchlisting criteria. If sufficient information does not exist to justify a person's inclusion in the TSDB or its subsets (such as the No Fly List), the person will be removed. An enhanced redress process for individuals on the No Fly List provides for an administrative appeal of any adverse redress decision, the ability to request any releasable information, and the ability to submit information for consideration during the appeal.

Those who are misidentified as watchlisted can experience varying levels of difficulty when they fly or attempt to cross national borders. When these misidentified persons file redress complaints, review and any corrective actions are accomplished by the screening agency. The Government Accountability Office (GAO) recently completed a comprehensive review of the ongoing interagency efforts to improve the experience of misidentified persons (GAO Report 06-1031), including efforts by DHS to annotate their record systems to distinguish those persons more quickly in the future. The GAO Report highlights the TSC's significant efforts to improve the redress process and to assist misidentified persons, including a procedure for maintaining records of encounters with misidentified persons and for reviewing records when new encounters occur so the TSC can rapidly identify and clear known misidentified persons during screening. Information regarding the watchlist redress process and how to file a complaint with a screening agency is available to the public on the TSC's website at www.fbi.gov/terrorinfo/counterrorism/tsc.htm. Other agencies that use TSDB data for screening, including the TSA, also provide redress information on their websites.

SENTINEL

15. Now a year into the Bureau's Sentinel computer upgrade program, I remain concerned about the prospect of this program and its ballooning costs to American taxpayers. Earlier this month, the FBI informed the Committee that it had encountered unexpected problems with the deployment of Phase I of the Sentinel program that would delay the program. Even more troubling, the FBI could not tell Committee staff how long it would take to remedy these problems, or how the delay would impact the overall schedule for Sentinel.

a. What is the current status of the Sentinel program and do you anticipate that there will be additional delays in deploying the program or costs overruns?

Response:

The FBI successfully deployed Phase 1 of the SENTINEL system to all Automated Case Support (ACS) system users worldwide on June 18, 2007, two months later than originally planned. Product integration problems and performance issues delayed delivery, and more testing was required to ensure fixes worked to specifications. In addition, the FBI changed the deployment approach to allow for a pilot period to test the system with actual users and ensure an accurate measurement of performance. The program was piloted in the Baltimore, Washington, and Richmond Field Offices and in one Division at FBIHQ. In addition to testing the system's functionality, the pilots also assisted in testing how the system handled the user load and in assessing the adequacy of the training materials.

The SENTINEL Program Management Office and Lockheed Martin prepared users for training and deployment, training nearly 250 field office and FBIHQ users as SENTINEL Training Advisors. This group assisted contract instructors in providing training and will continue to assist users in their divisions when questions arise.

The FBI deferred a total of 57 mostly low-level requirements from Phase 1 to later phases because they were outside of the scope of Phase 1, did not add value to Phase 1, required the modification of ACS, or would duplicate a capability included in a future phase. As a result of a series of contract modifications, some of which pre-purchased software for Phase 2, the cost for Phase 1 development, including award fees, increased from $57.2 million to $59.7 million.

b. What impact have the delays with Sentinel -- and Trilogy before it -- had on the Bureau's ability to fulfill its core mission?

Response:

The delays in updating the FBI's computer systems have had very little impact on the Bureau's ability to fulfill its core mission. All components of the FBI's ACS system have continued to be operational, and this information will be migrated to Sentinel. Phase 1 provides Sentinel's foundational base and enhanced access to the information contained in ACS. Phase 2 will bring the most new capabilities to the users, including automated workflow, document and record management, public-key infrastructure, digital signatures, and role-based access controls.

CIVIL RIGHTS COLD CASES

16. In February 2006, the FBI established a nationwide initiative to re-examine civil rights era cold cases. At a press conference on February 27th, the FBI released a press statement announcing that although 100 cold cases have been referred to the Bureau, the FBI has prioritized only a dozen. I applaud the effort to reexamine these cases, but why has the FBI only prioritized a mere handful of civil rights era cold cases? How many agents, analysts, and other resources has the FBI committed towards this important effort?

Response:

While the FBI initially prioritized 10 cases for immediate assessment, all of the matters referred to the FBI as a result of this initiative have been forwarded to the 17 affected FBI field offices for preliminary investigation. Those offices will review available investigative files, court records, and public source information, determine if identified subjects and witnesses are still alive, and compile comprehensive witness and evidence lists. The facts of each case will be presented to both Federal and local prosecutors to assess possible prosecution potential, and matters identified as having both investigative and legal viability will be pursued. The FBI has 152 SAs assigned to work Civil Rights matters, including this important initiative.

17. Earlier this year, I joined Senator Dodd in re-introducing the Emmett Till Unsolved Civil Rights Crime Act. This bill creates permanent unsolved civil rights crimes units within the FBI and the Civil Rights Division of the Justice Department to investigate and prosecute these crimes. This bill will also give law enforcement the resources to ensure that justice is served. As a former prosecutor, I strongly believe law enforcement should have the necessary tools to aggressively seek those who have committed these crimes, regardless of the time that has passed. Would you support the Emmett Till bill? Do you believe this bill gives the FBI the resources needed to thoroughly investigate unsolved civil rights murders?

Response:

As indicated during the testimony of Deputy Assistant AG Grace Chung Becker in a June 12, 2007 hearing before the House Committee on the Judiciary, Subcommittee on Crime, Terrorism, and Homeland Security, DOJ and the FBI support the goals of the Emmett Till Unsolved Civil Rights Crimes Act, but have offered recommendations to improve its effectiveness.

LOST LAP TOPS/ DATA SECURITY

18. In February, the Inspector General for the Department of Justice released another troubling report finding that the FBI lost 160 laptop computers - including at least ten computers that contained classified information and one that contained sensitive personal information about FBI personnel - during a 44-month period. Even more troubling, the report also found that the FBI could not even account for whether 51 other computers, including seven computers that were assigned to the Bureau's counterintelligence and counterterrorism divisions, might contain classified or sensitive data. What is the Bureau doing to address its problem of lost laptops and lax data security?

Response:

The DOJ OIG recognizes that the FBI has made substantial progress since the OIG initiated its review. The report itself states that "the FBI has made progress in decreasing the rate of loss for weapons and laptops" and notes the positive trend in this direction since the FBI's implementation of corrective actions in 2002. This progress reflects the FBI's commitment to minimizing such losses. The statistics cited in the report reflect a substantial reduction in the average number of laptops lost or stolen in any given month when compared to information in the 2002 OIG report. The report additionally recognizes that "in an organization the size of the FBI, some weapons and laptops will inevitably be stolen or go missing."

The FBI recognizes that more needs to be done to ensure the proper handling of laptop computers (and the information on these laptop computers) to minimize the incidents and ramifications of loss and theft. One of the most important steps to ensuring the security of the information on our laptop computers is the encryption and password protection of this information. To this end, the FBI requires that all FBI laptops be configured to include encryption that protects the sensitive but unclassified information they may contain, such as personally identifying information (PII). The policy requiring this configuration contains a total of nine requirements and recommendations designed to minimize the potential for loss of FBI laptops and information. Additional policies related to the protection not only of PII but also of other information, including National Security information, were promulgated in April 2006 and articulated in the FBI's comprehensive Security Policy Manual.

19. Earlier this year, Senator Specter and I reintroduced our Personal Data Privacy and Security Act, which would, among other things, require federal agencies to give notice to the individuals whose data is lost or stolen, when a data breach occurs. Did the FBI notify

the individuals whose sensitive personal information was lost in the case of the missing laptops? Would you support this legislation?

Response:

The FBI bases its response to a compromise of PII on the circumstances of the breach. In appropriate cases, the affected individuals are notified. However, in some cases notice is deemed unnecessary because the risk of data compromise is almost non-existent (e.g., where an effective security system blocks access to data), in some cases notice may compromise a criminal or national security investigation, and in some cases notice is not possible because there is no way to determine which identities were compromised. The FBI is in the process of developing a formal data breach policy that will comport with guidance provided by the Office of Management and Budget (OMB). The FBI has not taken an official position regarding the Personal Data and Security Act and will defer to DOJ in this regard.

20. After the VA lost a lap top containing sensitive personal information about millions of veterans and active duty personnel, Secretary Nicholson instituted a new policy requiring that all of the VA's computers contain encryption technology to prevent the unauthorized disclosure of sensitive information. Will you make a similar pledge to use encryption technology for all of the Bureau's computers?

Response:

The FBI's security policy requires that FBI-owned and FBI contractor-owned laptop computers used for FBI work be equipped or configured according to Federal Information Processing Standards Publication 140-2, "Security Requirements for Cryptographic Modules," or with National Security Agency-approved encryption if the laptop contains FBI information (including Classified, Sensitive But Unclassified, For Official Use Only, or Law Enforcement Sensitive information), operates in other than a stand-alone mode, or connects to the Internet.

DNA SAMPLING

21. Pursuant to a little noticed provision in the Violence Against Women Act reauthorization bill, the Department of Justice is currently developing new guidelines that would greatly expand the Government's ability to collect DNA samples - which reveal the most sensitive genetic information about an individual - from most individuals who are arrested or detained by federal authorities and to store this sensitive biological information in a federal data base known as the National DNA Index System. This new policy will

allow the Federal Government to collect DNA samples from hundreds of thousands of illegal immigrants who may be detained by federal authorities and from individuals who may be arrested - in essence, making DNA collection as common as fingerprinting. What privacy protections are in place under the Department's new guidelines to ensure that sensitive DNA data contained in the National DNA Index System will not be misused or improperly disclosed by the FBI or other federal and state agencies?

Response:

While the FBI is working with DOJ to finalize the regulations on DNA sample collection relative to Federal arrestees and detainees, there are already a number of protections in place and they are vigorously enforced. When arrestee and detainee DNA samples are collected, they are placed in the National DNA Index System (NDIS) offender database. The offender and crime scene databases are populated by profiles from Federal, State, and local law enforcement agencies. The profiles within the database use only genetic markers that provide identification; no other genetic information, such as medical status, can be gleaned from these markers, and NDIS, which is in essence a pointer system, does not contain any names or personally identifying information. Instead, each profile is associated with a unique identifier that traces back to the laboratory that developed that particular profile and placed it in the database. Once a "hit" occurs and is confirmed, then the two laboratories involved will exchange information regarding the individual involved.

Although all states participate in NDIS, they do not have direct access to the national database. NDIS is searched once a week at the FBI and a hit report is generated. If an individual lab desires to follow up on a particular hit (generally the lab that contributed the forensic sample), it contacts the laboratory that provided the offender information and a confirmation process begins. During that process, the laboratories follow written procedures to ensure the hit is related to the correct offender; these procedures include re-working a portion of the remaining sample and re-comparing results. Under procedures established by the NDIS Board, no names or other personally identifying information may be reported until the confirmation process is complete.

Federal law also provides privacy protections, including criminal penalties for privacy violations. By law, NDIS DNA information must be

> [m]aintained by Federal, State, and local criminal justice agencies (or the Secretary of Defense in accordance with section 1565 of Title 10) pursuant

to rules that allow disclosure of stored DNA samples and DNA analyses only –

(A) to criminal justice agencies for law enforcement identification purposes;
(B) in judicial proceedings, if otherwise admissible pursuant to applicable statutes or rules;
© for criminal defense purposes, to a defendant, who shall have access to samples and analyses performed in connection with the case in which such defendant is charged; or
(D) if personally identifiable information is removed, for a population statistics database, for identification research and protocol and development purposes, or for quality control purposes.

(42 U.S.C. § 14132(b)(3).) These protections are further bolstered by provisions that reiterate these protections and provide criminal penalties for individuals who knowingly disclose DNA information from the database to a person or agency not authorized to receive it. (See, for example, 42 U.S.C. § 14133© and 42 U.S.C. § 14135e©.)

22. I am also concerned about this new policy because the new DNA evidence collected by the Government will add to the already notorious backlog at the Bureau's laboratory. According to press reports, the FBI acknowledges that this new policy will result in an increase of as many as 1 million additional DNA samples a year. Is the Bureau's laboratory equipped to handle this additional workload? What steps are you taking to make sure that the FBI's laboratory can keep up with the demand for DNA samples?

Response:

The FBI's Federal Convicted Offender (FCO) Program is responsible for collecting and processing DNA samples collected from those convicted of Federal felonies for the purpose of retention and cataloging in the FBI's National DNA Database. The FCO Program receives samples from over 500 collection sites across the country. Since the program's inception in June 2001, over 225,000 samples have been received, with 7,000 to 8,000 samples currently received monthly. To date, the FCO Program has uploaded over 34,000 samples into the National DNA Database, resulting in over 600 hits. While the volume of sample submissions to the FCO Program has increased dramatically since 2001, the FBI Laboratory has received no additional resources to support this work.

While much of the DNA analysis process has been automated, the volume of sample submissions to the FCO Program has increased dramatically since 2001. A bottleneck continues to exist at the DNA data review stage, which is currently conducted manually. To alleviate this bottleneck, the FBI is evaluating data analysis software packages and expert systems to automate this part of the process. Once implemented, the resulting system would be able to assess 85 percent to 90 percent of the convicted offender data without manual intervention, reducing data analysis time from approximately 60 minutes (per 80 samples) to less than 15 minutes. The FY 2008 budget request also includes $15 million to address the workload increases for the FCO Program.

IMPROPER REPORTING OF TERRORISM STATISTICS

23. The Department of Justice Inspector General found in another recent report that the FBI failed to accurately report eight of the ten terrorism statistics that it reviewed for this report - that is an 80% failure rate. Among other things, the FBI overstated the number of terrorism-related convictions for 2004, because it included cases where no terrorism link was actually found. This is no simple matter -- the Congress relies upon these statistics to conduct oversight and to make funding and operational decisions regarding the Bureau. What steps have you taken to address the problems with reporting of terrorism statistics at the FBI?

Response:

The FBI has modified and substantially improved the systems and internal controls related to terrorism reporting. Following the attacks of September 11, 2001, the FBI underwent a substantial reorganization and restructuring, and many of the apparent weaknesses in statistical reporting discussed in the OIG report entitled, "The Department of Justice's Internal Controls over Terrorism Reporting" occurred during, and were a result of, that reorganization and restructuring. The backbone of the FBI's statistical reporting system is the case management system, along with its supporting information technology systems. These systems were not originally designed to capture or report on the enhanced requirements developed as part of the FBI's post-9/11 reorganization and restructuring. The FBI recognized this challenge in 2002 and began a concentrated effort to build supporting systems that include additional internal controls to ensure that we accurately capture and report on the activities involved in our post-9/11 intelligence mission. The FBI has made significant progress in the development and implementation of these systems, which are being upgraded as part of the FBI's Sentinel project.

Also since the time period examined by the OIG Report, the FBI has made significant strides in the development of a new central management information system known as the Comprehensive Operational Management Plan Advancing Specific Strategies (COMPASS). COMPASS accumulates statistical accomplishments from various stand-alone systems and presents the information in a unified format available to all senior managers both at FBIHQ and in FBI Field Offices. COMPASS is one example of the FBI's commitment to improving and sharing statistical reporting with FBI senior managers. The bulk of the information captured in COMPASS is used internally to identify trends and to evaluate progress against the FBI's defined strategic objectives. The FBI continues to make extensive efforts to refine performance metrics that measure the FBI's achievements against strategic outcomes.

STAFFING

24. I also remain concerned about staffing at the Bureau. In January, your Deputy, John Pistole, told the Senate Intelligence Committee that the FBI expects to lose 400 agents and 400 intelligence analysts this year, due to retirement or attrition. Mr. Pistole also stated that approximately 20% (370) of the FBI's intelligence analysts have less than a year of experience with the Bureau. I cannot help but worry that the Bureau will not have the staffing and expertise that it needs to carry out its counterterrorism and counter-intelligence mission, given these figures on staffing. What are you doing to address the shortage in intelligence analysts and agents? How many agents and analysts do you expect to hire by the end of 2007?

Response:

The FBI's top priority for Fiscal Year (FY) 07 was to recruit highly qualified, diverse applicants targeting specific critical skills and backgrounds, including foreign languages, intelligence, computer science/information technology, accounting/finance, engineering, law enforcement/law/military, and science.

The FBI employs several recruitment strategies to support the recruitment of SAs, IAs, language analysts, and others possessing critical skills and backgrounds, including minorities, women, and those with disabilities. The most effective strategies have included the following.

- National advertising, including television, radio, Internet, billboards, airport dioramas, and print media.

- Participation in over 900 national and local targeted career fairs and conferences annually to maximize the FBI's access to high-quality, diverse applicants with critical skills.

- Partnering with diverse organizations such as the U. S. Copts' Association, American-Arab Anti-Discrimination Committee, Sikh Foundation of Virginia, Sikh Council on Religion and Education, Kaur Foundation, Intelligence Analyst associations, National Society of Black Engineers, Black MBA Association, American Arab Institute, and U. S. Arab Economic Forum.

- Targeted intern and co-op programs.

- Continuation of the FBI's EdVenture Partners Collegiate Marketing Program.

- Expanded partnership with the Faith-Based Council on Law Enforcement and Intelligence.

- Using recruitment contractors whose missions focus on the recruitment of applicants possessing such expertise as intelligence, foreign languages, information technology, and middle eastern cultures.

- Featuring onboard employees with critical experience and education in line with the FBI's targeted hiring goals and objectives in all new recruitment media (such as advertisements, brochures, exhibits, and videos), clearly demonstrating the FBI's diversity.

- Continued participation in the Intelligence Community Recruiting Group, which meets monthly, includes all recruitment chiefs in the Intelligence Community (IC), and engages in joint recruitment, training, and diversity seminars.

The FBI's Hiring Plan provides for the addition of 287 SAs and 112 IAs in FY 2007. We have been successful in recruiting IAs with the specialized skills needed to build our Intelligence Program, hiring 1,448 IAs in the past 3 years, including a mix of IAs who have either specialized skills that target specific knowledge or general analytic skills. In order to recruit and hire IAs with the skills and educational backgrounds needed to meet our national security mission, the FBI developed a targeted recruitment strategy that identifies the critical skills required by the FBI to satisfy its current mission as well as those needed to address the organization's future challenges. The FBI is updating the recruitment

strategy to reflect the current hiring environment for the intelligence workforce and anticipates releasing a modified version of this strategy by the end of 2007.

25. I was disappointed to learn that the FBI has not met several of its goals to improve FOIA processing under the President's Executive Order 13,392, including the important goal to complete all FOIA requests that are more than two years old by August 2006. What is the current status of the FBI's FOIA backlog?

Response:

The FBI identified 24 goals designed to improve our efficiency in processing requests under the Freedom of Information Act (FOIA), the professionalism of staff employees, and customer service, establishing an ambitious multi-year plan for implementing these improvements. The FBI met its interim and completion targets with respect to all but eight goals, and continues to work on these remaining goals.

Despite a 40 percent increase in FOIA requests (from 10,873 in FY 2005 to 15,349 in FY 2006), the FBI met or surpassed its goals related to the time required to process requests. The median time for processing small requests (those of less than 500 pages) decreased by 10 percent (the goal was a 10 percent reduction) and the median time for processing medium requests (500 to 2499 pages) decreased by 16 percent (this goal was also a 10 percent reduction). The median time required to process all pending requests decreased by 36 percent (the goal was a 20 percent reduction).

Although not among our designated goals because of the difficulty in predicting the volume of incoming requests, we also worked hard to reduce the number of requests pending at any given time. Overall, we reduced the number of pending requests from 1,796 at the end of FY 2005 to 1,750 at the end of FY 2006. This included a 58 percent reduction in the number of pending large requests (those of 2,500 pages or more) from the end of FY 2005 to the end of FY 2006 (a reduction from 122 to 51), and this number continued to decrease, with 42 requests pending on April 1, 2007. The number of pending medium requests also decreased, from 691 at the end of FY 2005 to 203 on April 1, 2007, with a corresponding decrease in the median amount of time for which medium requests were pending (from 556 days at the end of FY 2005 to 273 days on 4/1/2007).

Contrary to the indication in the question, the FBI's goal was not to "complete all FOIA requests that are more than two years old by August 2006." The FBI's goal was to "continue emphasis on completing requests over two years old." Even before development of the FBI's Improvement Plan, the FBI had identified 74

requests (approximately 320,700 pages) received by the FBI before August 14, 2003 and was developing a plan to complete them. The FBI successfully met its August 15, 2006 interim goal of developing a plan for processing older requests. As of September 1, 2007, 72 of these requests had been closed by reviewing 290,300 pages. As part of the continuing emphasis on requests over two years old, on August 15, 2006 the FBI identified 36 pending requests (an estimated 72,000 pages) received between August 15, 2003 and August 15, 2004. As of September 1, 2007, 34 of these requests had been closed by reviewing 68,670 pages. The FBI continues to both process and provide interim releases with respect to the remaining open requests.

26. After the horrific attacks of September 11th, I worked very hard with others in Congress to give the FBI the tools that it needed to combat terrorism and carry out its domestic intelligence functions. Given what we have learned about the widespread misuse of National Security Letters and chronic staffing problems in the Bureau's counterterrorism and counterintelligence offices, some are calling for the Congress to put the Bureau's domestic intelligence operations in a new MI5-styled domestic intelligence agency. Do you believe that Congress should create a domestic intelligence agency to carry out the Nation's domestic counterterrorism activities?

Response:

The FBI believes there is no reason to separate the functions of law enforcement and domestic intelligence, as would occur if the MI-5 model were adopted. On the contrary, combining law enforcement and intelligence affords us ready access to every weapon in the government's arsenal against terrorists, allowing us to make strategic and tactical choices between the use of information for law enforcement purposes (arrest and incarceration) or intelligence purposes (surveillance and source development).

The benefits of this approach have been clearly borne out. Since September 11, 2001, the FBI has identified, disrupted, and neutralized numerous terrorist threats and cells, and we have done so in ways an intelligence-only agency like the United Kingdom's MI-5 cannot.

Because of its personnel, tools, and assets, the FBI is uniquely suited for the counterterrorism mission. These resources include:

- A worldwide network of highly trained and dedicated SAs;
- Intelligence tools to collect and analyze information on threats to national security;

- Law enforcement tools to act against and neutralize those threats;

- Expertise in investigations and in the recruitment and cultivation of human sources of information;

- Longstanding and improving relationships with those in state and local law enforcement, who are the intelligence gatherers closest to the information we seek from these communities; and

- Nearly a century of experience working within the bounds of the United States Constitution.

For these reasons, the FBI believes the United States is better served by enhancing the FBI's dual capacity for law enforcement and intelligence gathering/analysis than by creating a new and separate domestic intelligence agency, which would constitute a step backward in the war on terror, not a step forward.

That said, the FBI is in the process of adopting some aspects of MI-5. One of the benefits inherent in an intelligence organization like MI-5 is its ability to establish a "requirements" process where current intelligence requirements are reviewed (whether they be terrorism, international crime, cyber crime, or otherwise) and knowledge gaps are identified. The next step is to get the intelligence collectors (in this case, FBI SAs from around the country) to fill in those gaps. The FBI has adapted and is incorporating this kind of intelligence requirements process, not just with respect to terrorism but for all programs. This process is invaluable in helping to better prioritize FBI resources and to identify the gaps in understanding.

Both the National Commission on Terrorist Attacks Upon the United States (the 9/11 Commission) and the report of the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction (WMD Commission) agree that the FBI should retain its domestic intelligence responsibility. Similarly, in its March 2005 report entitled, "Transforming the FBI: Progress and Challenges," a panel of the National Academy of Public Administration wrote: "This Panel, like the 9/11 Commission, is convinced that the FBI is making substantial progress in transforming itself into a strong domestic intelligence entity, and has the will and many of the competencies required to accomplish it. That Panel recommended that the FBI continue to be the key domestic intelligence agency responsible for such national security concerns as terrorism, counterintelligence, cyber, and transnational criminal activity."

The WMD Commission also examined the FBI's intelligence program and concluded in March 2005 that it had been significantly improved since September 11, 2001. The commission rejected the need for a separate agency devoted to internal security without any law enforcement powers, recognizing that the FBI's hybrid intelligence and investigative nature is one of its greatest strengths and emphasizing the importance of the ongoing effort to integrate intelligence and investigative operations. At the same time, the commission noted that the FBI's structure did not sufficiently ensure that intelligence activities were coordinated with the rest of the IC. Accordingly, the commission recommended the creation of a "National Security Service." In response to the President's directive endorsing that recommendation, the FBI created the National Security Branch, which combines under one leadership umbrella the capabilities, resources, and missions of the Counterterrorism Division, Counterintelligence Division, Directorate of Intelligence, and WMD Directorate. The structure offered by the National Security Branch ensures the integration of national security intelligence and investigations, promotes the development of a national security workforce, and facilitates a new level of coordination with our partners in the IC.

Questions Posed by Senator Kennedy

27. The Hate Crime Statistics Act requires the Justice Department to publish an annual summary of crimes which "manifest prejudice based on race, religion, sexual orientation, disability, or ethnicity," based on data from law enforcement agencies across the country. In 2005, there were 7,163 such crimes. 3,919 were motivated by racial bias; 1,227 by religious bias; 1,017 by sexual orientation bias; 944 by ethnicity/national origin bias; and 53 against disabled individuals. 12,417 law enforcement agencies in the United States participated in this data collection effort. Only a small percentage of law enforcement agencies in the nation participated, and only 16% of the participating agencies reported even a single hate crime.

a. What steps is the FBI currently taking to increase participation in the data collection effort?

Response:

The FBI's hate crime data collection effort is part of the Uniform Crime Reporting (UCR) program, which is a nationwide, cooperative statistical effort that depends on the voluntary reporting of Federal, state, tribal, city, county, and university law enforcement agencies. In 2005, the reporting agencies represented more than 245 million inhabitants, or 82.7 percent of the nation's population, including reporting from 49 states (hate crime information is not received from Hawaii) and the District of Columbia. Though the published 2005 UCR statistics did not include hate crime data for New York City or Phoenix, the FBI's UCR program has worked with these cities and has obtained their data for inclusion in the 2005 hate crime database.

The UCR program relies on the good faith reporting by its participating agencies of bias-motivated crime. Periodically, the UCR program forwards to state UCR program managers quality reviews that identify reported hate crimes by reporting agency, listing those agencies for which no information is received. At that time, the FBI encourages the submission of any missing or incomplete information. The UCR program has strongly endorsed the collection of hate crime statistics in electronic format. Currently, 73 percent of the hate crime statistics are submitted in electronic format, typically by using the National Incident-Based Reporting System (NIBRS) and interactive online communications through Law Enforcement Online (LEO).

b. How much training is the FBI currently providing to state and local law enforcement authorities to improve identification, reporting, and response to hate crimes nationally?

Response:

The FBI's UCR program provides training materials in print, online, and, when funding permits, on site for the agencies that request it. During the last three fiscal years, the FBI's UCR program has provided almost 6,000 printed hate crime training manuals to law enforcement. In addition, the UCR program has conducted on-site training for 63 agencies regarding issues specific to hate crimes, and web-based hate crime training is available to law enforcement through LEO. The UCR program also provides training regarding hate crime reporting when it trains law enforcement personnel regarding Summary reporting and NIBRS. UCR program contributors and stakeholders are informed of hate crime reporting procedures and training opportunities through the UCR *State Program Bulletin* and *UCR Newsletter*, among other means.

28. Attached is a June 26 letter signed by 42 national civil rights, law enforcement, civic, and religious organizations which includes recommendations, prepared in response to the 71 FR 24869 request for comments on improving the Act. In meetings with government officials and community-based organizations, FBI representatives have indicated that an interagency hate crime working group was created to revise and update FBI resources under the Act.

a. What is the current status of this Hate Crime Working Group?

Response:

Former Attorney General Reno convened a Hate Crime Working Group at DOJ in May 1997. The Working Group was initially chaired by David W. Ogden, Counselor to the Attorney General, and met approximately weekly. Members of the Working Group included interested components throughout DOJ and the FBI. The Working Group examined five principal areas related to hate crime: legislative initiatives, data collection, community outreach, prosecution and enforcement, and coordination. The Working Group developed a number of specific recommendations, including the formation of local hate crime working groups in Federal judicial districts under the leadership of or with the participation of each U.S. Attorney's Office. The local working groups were envisioned as including local community leaders and educators, as well as Federal, State, and local law enforcement officials, and were to be the primary mechanism for evaluating and addressing the hate crime problem in the local community.

The FBI defers to DOJ regarding the current status of this Working Group.

b. What is the status of plans to revise and update the FBI's Hate Crime Incident Report forms to provide space to encourage additional narrative about the bias motivation?

Response:

The UCR program is evaluating the current Hate Crime reporting program and exploring opportunities for program enhancement, including the possible inclusion of narrative comments or structured narrative fields. This evaluation must include consideration of how to ensure the value of subjective, unstructured narrations and how to limit the burden on those drafting the narratives to accurately and succinctly depict incidents. Once the FBI has evaluated this issue, recommendations will be provided to the FBI's Criminal Justice Information Services (CJIS) Advisory Policy Board (APB) for review and recommendation to the FBI Director.

c. What is the status of plans to revise and update the Bureau's 1999 training materials on how to identify, report, and respond to hate crimes to reflect post-9/11 realities?

Response:

The FBI is reviewing all training materials, including both hard copy and web-based materials, to ensure law enforcement has the tools it needs to accurately and efficiently report hate crimes. Recommendations based on this review will be presented to the CJIS APB to ensure consensus within the law enforcement community.

29. Attached is an exchange of letters between 51 national organizations and your office. On October 23, 2006 these groups wrote to you to express concerns that the 2005 edition of the comprehensive FBI crime data compendium, *Crime in the United States,* was published without a summary of hate crime data for the first time since 1996. The FBI Assistant Director in charge of the Criminal Justice Information Services Division, Thomas E. Bush, III, responded in the attached November 30 letter, stating:

> **"Although the decision to exclude preliminary hate crime data from *Crime in the United States* was well thought out and thoroughly reviewed, we understand the concerns expressed in your letter. In response, the FBI will work to better align hate crime statistics with *Crime in the United States,***

2006, **thus giving hate crime data more visibility in conjunction with this publication."**

What is the status of efforts to integrate data from the Act into *Crime in the United States, 2006?*

Response:

A link to hate crime statistics is provided on the main navigation page of the electronic version of the UCR (www.fbi.gov/ucr/ucr.htm). This link connects to the hate crime statistics for the selected year.

30. Professor Jack McDevitt, Director of The Center for Criminal Justice Policy Research at Northeastern University in Boston, has emphasized the need for an expanded narrative in reporting hate crimes. In his September 2002 report, *Improving the Quality and Accuracy of Bias Crime Statistics Nationally,* funded by the Justice Department's Bureau of Justice Statistics, Professor McDevitt suggested that more detailed reporting can reduce the occurrence of "information disconnect" between the investigating officer and Uniform Crimes Report reporting officials.

The current reporting form provides boxes only for "Anti-Hispanic" and "Anti-Other Ethnicity." In light of the disturbing number of post-9/11 "backlash incidents" in the aftermath of the September 11th terrorist attacks, do you believe that the form should include additional boxes for "Anti-Arab," "Anti-Muslim," and "Anti-Sikh" crimes, among others?

Response:

The FBI's UCR program collects hate crime data in accordance with the Hate Crime Statistics Act of 1990, as amended, and in compliance with the standards for race and ethnicity designations established by OMB. The current Hate Crime Incident Report Form collects "Anti-Islamic (Muslim)" data under the category of "religious bias motivation." The FBI recognizes the possible value of establishing separate categories for "anti-Arab" and "anti-Sikh," but there is no current consensus on how to define these terms (for example, should they be based on geography, culture, religion, or native language). Therefore, absent a consensus on definitions for these categories, the FBI does not intend to include "Anti-Arab" or "Anti-Sikh" bias motivation types.

31. As states continue to enact hate crime statutes, the clear trend has been to include gender-based crimes in these laws. In 1990, only seven of the statutes in the thirty-one states with hate crime laws included gender. Today, including the District of Columbia,

twenty-eight of the forty-five states with penalty-enhancement hate crimes statutes include gender-based crimes. Eight states now include gender in their hate crime data collection mandate. Gender-based crimes are subject to federal sentencing enhancements under 28 U.S.C. § 994.

a. Do you believe that the FBI's Hate Crime Incident Report should include a box in the Bias Motivation section for gender-based hate crimes?

b. Is there a legal impediment to making that change, or could the Bureau take this step on its own?

Response:

The categories of bias reported in the UCR are based on the Hate Crime Statistics Act of 1990, as amended, and OMB's minimal standards for race and ethnicity designations. While the FBI does not anticipate revising the bias motivation categories absent revision of these authorities, there is no legal impediment to seeking additional voluntary reporting from law enforcement. If the FBI were to contemplate this, we would seek consideration of the proposal by the CJIS APB.

32. In your March 9, 2007 press conference after the release of the Inspector General's report, you were asked if any FBI personnel would face criminal sanctions for their conduct relating to the FBI's misuse of its National Security Letter authority. You said the IG report found no criminal misconduct, so your inspection division review of this matter is "to determine whether or not there should be any administrative actions taken." When questioned again you actually quoted from page 124 of the IG report, where the IG stated "we also did not find any indication that the FBI's misuse of NSL authorities constituted criminal misconduct." But the IG backed off from this definitive statement in his congressional testimony in the House of Representatives last week, saying "we did not do a thorough review of what people up and down the line knew and did," and later that "we didn't do a review where we asked each individual, "What did you do and why?" The IG suggested that you were going to conduct that sort of review: "The FBI is looking at the evidence right now to see what people knew and what they did." Since you now know that the IG didn't look for criminal misconduct during his audit, will you expand your review to investigate the possibility of criminal misconduct?

Response:

On March 9, 2007, the FBI Director directed the Inspection Division to thoroughly investigate concerns raised by the DOJ OIG. Thereafter, the OIG announced it would initiate a review of the FBIHQ unit in question. The Inspection Division is working jointly with the DOJ OIG in its review, with

DOJ's OIG designated as the lead agency. In addition, former Attorney General Gonzales asked an Associate Deputy Attorney General and DOJ's OPR to examine the role FBI attorneys played in the use of exigent letters. The FBI Director will review the results of all such inquiries when available and take appropriate action.

33. In fact, there is ample evidence that this misconduct was intentional. The Inspector General's report confirms that the Office of General Counsel knew of the FBI's misuse of National Security Letter authorities. In fact, OGC was put on notice of problems with NSLs a[s] late as 2004, yet did nothing to stop the abuses and in some cases, sanctioned them:

a. At least one OGC procurement attorney reviewed contracts between the Communications Analysis Unit and three phone companies, which were the basis for illegal "exigent" letters (p. 88-89);

b. Field agents complained about improper Communication Analysis Unit requests to the OGC's National Security Law Bureau as long as two years ago (p. 93);

c. NSLB attorneys gave improper advice to the Communications Analysis Unit and told them it was proper to issue exigent letter in true emergencies, despite any statutory grant to do so (p. 93);

d. NSLB attorneys discovered they were misled by Terrorist Financing Operations Section supervisors on the use of "Certificate Letters," yet the letters continued to be used[;]

e. FBI lawyers in the field, Chief Division Counsels, reported that they felt intimidated by their Special Agents in Charge and would approve NSL requests when they would have preferred to reject them out of fear of challenging their Special Agents in Charge.

Are you concerned that FBI attorneys were so intimately involved in this illegal conduct and allowed it to continue despite their reservations? Doesn't the involvement of attorneys in this misconduct make the illegal activity appear intentional? Have you reported these attorneys to the bar?

Response:

Without concurring with the premises or asserted factual representations within this question, please see the response to Question 32, above. The FBI Director

will review the results of the referenced inquiries when available and take appropriate action.

34. FBI General Counsel Valerie Caproni also testified before the House of Representatives last week. In response to questioning about the inability of the FBI to tie the use of NSLs to criminal terrorism prosecutions, Ms. Caproni said that "It is my belief that virtually every counterterrorism case that began in its normal course of affairs is likely to have a national security letter used sometime during it."

a. Does that mean every FBI terrorism prosecution used evidence obtained with NSLs? If this is so, why can't the FBI demonstrate it with data supporting this claim?

Response:

NSLs, which are an essential tool in national security investigations, are used to obtain basic information for use in national security investigations, similar to that routinely obtained through grand jury subpoenas for use in criminal investigations. Just as no prosecutor or investigator tracks the usefulness of grand jury subpoenas in criminal investigations or prosecutions (although all would say grand jury subpoenas for documents can be critical to investigations), the FBI has not tracked the usefulness of NSLs in national security investigations. Moreover, while some national security investigations ultimately result in criminal prosecutions, disruption through arrest is only one of many appropriate responses the FBI may have to a national security threat.

b. Has evidence obtained with NSLs been entered into evidence in any criminal proceeding? Was the fact that the evidence was obtained with an NSL disclosed to the court, or to defense counsel?

Response:

It is certainly possible that records initially obtained through the service of NSLs have been introduced into evidence during criminal trials. There is no legal obligation to disclose the manner in which documents are obtained before introducing them in evidence. See, for example, Federal Rule of Criminal Procedure 16.

c. If evidence obtained with NSLs is used to support wiretap requests or search warrants, is that fact disclosed to the defense counsel at trial, and does the defense counsel have an opportunity to challenge that evidence for legal insufficiency?

Response:

Generally, the means used to obtain evidence that is used to support a wiretap request or a search warrant is not disclosed to defense counsel as a part of normal criminal law discovery practice. However, a criminal defendant always has the opportunity to challenge the sufficiency of incriminating evidence introduced by the prosecution at trial. A criminal defendant also may contest the *legality* of a search or seizure of evidence under the Fourth Amendment. And, as a statutory matter, a defendant also may challenge the legality of certain surveillance activities that are within the scope of either Title III or the Foreign Intelligence Surveillance Act (FISA). It should be noted, though, that records obtainable by an NSL are third-party records in which individual customers have no constitutionally protected privacy interest (see *United States v. Miller*, 425 U.S. 435 (1976); see also *Smith v. Maryland*, 442 U.S. 735 (1979) and which are not covered by either Title III or FISA. Therefore, we believe it is unlikely that a criminal defendant would be successful in suppressing a wiretap or search because it was based in some fashion on information obtained through an NSL.

d. Can you assure Congress that no evidence obtained with an "exigent letter" or with an improper or illegal NSL request was ever used in evidence in any criminal proceeding, or used to support a search warrant or wiretap that was later used as evidence?

Response:

Please see the responses to Questions 6 and 34c, above.

35. General Counsel Caproni also said she could not confirm any instance in which information gathered with NSLs was used to prevent a terrorist attack. Can you confirm such an instance? Why should Congress accept that NSLs are "indispensable," when no data support such a claim?

Response:

Just as it would be difficult to demonstrate that information obtained through a grand jury subpoena had been used to prevent a murder, it is difficult to point to the use of an NSL to prevent a terrorist attack. NSLs are used to gather very specific types of third-party records that are used to identify and understand the adversaries who seek to do us harm. Once this information is obtained, other investigative tools may be used to disrupt the plans of terrorists, saboteurs, and spies.

For example, during the investigation of a terrorist financier and recruiter, NSLs for financial records and telephone toll billing records helped the FBI identify banks and accounts that were used to facilitate his terrorist fund-raising efforts. He was eventually identified as having provided instructions for terrorist activities in the United States. Although this financier and recruiter was not prosecuted, he was deported based upon the information developed during the investigation - information attributable in part to the information received through the use of NSLs.

In another case, the FBI received information from a foreign government indicating that individuals using e-mail addresses in the United States were in contact with an e-mail address belonging to a suspected terrorist. The FBI served NSLs on the relevant Internet service providers, and the investigation that followed indicated that these individuals were involved in plots against the United States, leading to indictments on various terrorism-related charges.

36. A March 20, 2007 Washington Post article suggested that the FBI will continue to use "emergency" requests to obtain records in advance of issuing NSLs or grand jury subpoenas.

a. Under what authority would the FBI use an emergency request?

Response:

Emergency disclosures are authorized by 18 U.S.C. § 2702(c)(4), which provides that an electronic communications service provider may voluntarily disclose to a governmental entity a record or other information (other than the contents of communications) pertaining to a subscriber or customer if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay. Pursuant to this provision, the FBI may present a service provider with information indicating the existence of an emergency and ask the provider to produce records or other non-content information in accordance with the provisions of the statute, recognizing that the statute authorizes the provider to make the determination and that production of the requested information would be voluntary on his or her part. A good example of when such a need might arise is as follows. Suppose a child is kidnapped, her parents receive a ransom call, and their telephone's caller ID function identifies the telephone number from which the ransom call was placed. In that circumstance, the FBI has a need to obtain telephone information immediately, but the facts underlying the emergency circumstance are unknown to the

telephone company at that point. Pursuant to section 2702(c)(4), if the FBI provides the facts to the telephone company, that company may provide the requested records if it decides that those facts justify an emergency disclosure of customer records. Such a need could also arise in the national security arena. Suppose, for example, the FBI receives a call anonymously warning that a bomb has been placed in the Sears Tower. The FBI would want to immediately identify the individual who placed the call and to determine others to whom the caller is related. That investigation would start by quickly gathering the telephone records of the telephone from which the anonymous call was placed.

b. The article said that under FBI policy, these requests could even be oral. Is there such a policy? Given what we have learned about the FBI's mismanagement of the NSL authority, and the lack of internal controls, why is it appropriate to use oral requests for documents?

Response:

An oral request would be entirely appropriate in an emergency in which delay could endanger lives. FBI policy requires documentation of the basis for an oral request and the service provider's response "forthwith." FBI policy also requires approval by an Assistant Special Agent in Charge (ASAC) in the field or a Section Chief at FBIHQ before a service provider may be asked to consider voluntarily disclosing the requested information pursuant to these provisions. Examples of when an oral request would be appropriate include the examples discussed above.

c. How does the FBI define an "emergency" as it pertains to a request for documents? What are the criteria? Is this a written policy, or does each agent decide on his own whether an emergency exists?

Response:

The statute requires "an emergency involving danger of death or serious physical injury to any person" requiring disclosure without delay. The FBI has not further defined this language. Under FBI policy, as indicated in the preceding response, a judgment call about whether to present information concerning such an emergency to an electronic communications service provider would be made by ASACs in FBI field offices or Section Chiefs at FBIHQ. Ultimately, the statute requires the service provider, with the information provided by the FBI, to make a good faith determination whether there is an emergency that justifies its voluntary release of this information.

37. The FBI has no policy on retention of improperly collected records, and does not require the purging of records of individuals proved not to be linked to terrorism.

a. Why was there no guidance to field agents on when or how to store and access information before November 2006?

Response:

The FBI has long had a records management plan, approved by the National Archives and Records Administration, for general record keeping. All FBI files are subject to a record-keeping plan which, among other things, provides for the preservation or destruction of records under specified circumstances. Materials obtained pursuant to NSLs were treated no differently than documentary materials obtained pursuant to other legal processes.

b. Field agents were asking for guidance on ad hoc basis, so the Office of General Counsel knew there was confusion in the field. Why didn't you develop a policy?

Response:

As noted above, there was a general records keeping plan in place and, as noted below, policies were developed as the need arose.

c. Why was an OGC guidance issued in November 2006? Was the guidance issued to mute the IG's criticism?

Response:

The issuance of guidance in November of 2006, which relates to the reporting of potential IOB matters, was not tied to any particular event. Since September 11, 2001, the mission of the FBI had expanded exponentially in the intelligence arena, and large numbers of FBI personnel were working intelligence issues for the first time. The cumulative effect of questions from the field and our own assessment of IOB matters coalesced in a determination that the issuance of comprehensive guidance would be appropriate.

The FBI's response to the recent IG report concerning NSLs demonstrates the willingness of the FBI to accept constructive criticism, incorporate lessons learned, and improve our policies and procedures.

d. The guidance issued by OGC in November 2006 is for field agents to send documents to OGC to determine what to do with them. If there's no overarching policy, how does OGC know what to do with them?

Response:

The November 2006 guidance concerned the reporting of potential IOB violations, not the retention of potentially improperly received information per se. The guidance provides that documents or records that are the subject of a potential IOB violation should be sequestered with the Chief Division Counsel (CDC) pending adjudication of the potential IOB matter. The import of that guidance was not that OGC would retain improperly obtained documents, but that OGC would, as required by Executive Order 12863, make the determination as to whether a potentially improper receipt of documents should be reported to the IOB. OGC has long advised that field offices should *over-report* rather than *under-report* potential IOB matters; that advice is based on the premise that, when there is any doubt as to whether a particular incident constitutes a violation of any requirement under the cognizance of the IOB, it is better to report it than not. Regardless of whether an overproduction of material is reported to the IOB, if the material is not relevant to an authorized investigation, it will be destroyed.

e. If field agents determine documents they received were improperly collected and they send them to OGC, on what possible grounds could OGC decide to retain them?

Response:

Please see the response to subpart d, above.

f. The IG report indicated the information gathered with NSLs is often used to close FBI cases by proving the subject has no links to terrorism. Yet the FBI does not have a policy of purging this data from FBI databases. Why not?

Response:

The FBI has legitimate investigative reasons for retaining information properly collected during the course of authorized investigations, even if the data pertains to individuals who are ultimately determined not relevant to the investigation (for example, the target called a telephone number ten times, but the contact is determined to be innocuous).

The FBI retains such information for at least two investigative reasons. First, by retaining the records that form the basis for our determination that a person is not of investigative interest, we ensure ourselves of an audit trail so we do not re-investigate the person each time he or she appears in an investigation. Instead, our agents and analysts can simply revisit the information previously collected and satisfy themselves that the judgment previously made, that this person is not of concern to the FBI, is still valid. That can generally be done without intruding again on the person's privacy and without again collecting personal information about the individual. In contrast, if we were to destroy the data, we would have to re-investigate the person each time he or she became pertinent to an investigation. Accordingly, retaining information is more protective of privacy interests than would be a policy mandating destruction.

The second reason to retain information is equally important: in order to fulfill our mission of keeping the country safe, we have been exhorted by Congress, the 9/11 Commission, the WMD Commission, and the American public to "connect the dots." The reality of analysis and investigative work is that connections between people that may seem entirely innocuous today can seem anything but innocuous when additional information is obtained. For that reason, we need to retain data and analysis regarding individuals so that, should the factual background change, we still have the lawfully obtained information regarding those individuals. In short, using the jargon that has become prevalent, we cannot "connect the dots" if we do not maintain the "dots" to connect.

For these reasons, the FBI does not support a policy that requires the destruction of data merely because, upon initial analysis, the person to whom it relates appears irrelevant to national security concerns.

g. If agents aren't reviewing the material they receive from NSLs, and are uploading that data into FBI databases, how can the FBI be certain its databases aren't bloated with records of totally innocent Americans? Why would the FBI want this information in its databases in the first place? How is it being used?

Response:

We do not read the IG's report as indicating that FBI Agents are not reviewing the material produced pursuant to NSLs. Rather, we believe the IG was concerned that the FBI may not be verifying that the records received were those requested from the provider before uploading them for analysis. This concern was addressed in a January 3, 2007 electronic communication (EC) that reiterated the

need to review results before uploading to ensure the correct results are being received.

38. With respect to NSLs being used to collect intelligence rather than as investigative tool:

a. The IG report reveals that field agents are not even reviewing data received in response to an NSL, which indicates they are not using the data to pursue investigative leads. What can you do about this?

Response:

Please see the response to Question 37g, above.

b. Under the current system, the FBI can't document how useful NSLs are, because it intentionally does not keep records on how these authorities are used. There were more that 140,000 NSL requests in two years, and the IG confirmed only one conviction for material support for terrorism and 152 "criminal proceedings." Considering the 87% declination rate by the Department of Justice for actual prosecutions, how significant are NSLs?

Response:

Please see the response to Question 35, above.

c. The FBI uses control files to issue NSLs where no authorized investigation exists. Why would the Office of General Counsel allow this, much less suggest it when the law clearly says that the NSLs must be relevant to an *authorized* investigation?

Response:

The premise upon which this question is apparently based is erroneous. While a control file was cited in the issuance of NSLs in a compartmented investigation, these NSLs were relevant to an authorized investigation. It is erroneous, therefore, to conclude that investigative activity was conducted under the auspices of a control file and in the absence of an authorized investigation. The use of a control file under these circumstances may have made auditing difficult, but it was not unlawful. Under the circumstances, the need to protect sensitive intelligence sources and methods fully justified this measure.

Notwithstanding the fact that the use of a control file under the circumstances described above was not unlawful, the FBI has adopted a policy pursuant to which

NSLs should not be issued under control file numbers and investigative activity should not be conducted based on a control file. The February 23, 2007 EC publishing this policy also reiterates that "NSLs are authorized only when the information sought is relevant to an existing national security investigation."

d. The Communications Analysis Unit is clearly not an investigative unit. Why would it be contracting with telephone companies to receive records, and why would the Office of General Counsel approve such contracts?

Response:

The functioning of the Communications Analysis Unit as an investigative unit or an analytical unit does not affect the propriety of issuing an NSL or receiving information in response to an NSL, provided the data sought is relevant to an authorized investigation.

39. In your testimony before the Senate Judiciary Committee, you testified that "We do not have an enforcement mechanism for national security letters." In response to a subsequent media inquiry by the Associated Press, FBI spokesman John Miller indicated the following about your testimony: "He misspoke. He was operating on the standard that existed before the renewal where the enforcement mechanism was not clearly defined." The article then states, "Miller added that Mueller knows the law was changed, but "it just slipped his mind for that moment."

a. Can you please clarify your testimony for the Committee?

Response:

In the USA PATRIOT Act Improvement and Reauthorization Act (Pub. L. 109-177), Congress enacted 18 U.S.C. § 3511(c) to enable the AG to seek from the United States District Court in an appropriate jurisdiction an order directing the NSL recipient to comply with the NSL request. Any failure to comply with such an order from a district court may be punished by the court as contempt.

b. In addition, can you describe in detail the procedures for the FBI to follow the enforcement mechanism for National Security Letters as established by the reauthorization of the PATRIOT Act in the 109th Congress?

Response:

Since enactment of the Reauthorization Act, we are unaware of any NSL recipients who have failed to comply with NSLs. When that occurs, the FBI will work with the appropriate DOJ attorneys to enforce the NSL.

40. I am very concerned that Iraqis who have worked with the U.S. government and military are targeted for assassination by terrorists and insurgents. The United States has a moral obligation to assist those whose lives are in danger because of their close association with us. State Department Assistant Secretary Sauerbrey recently testified that Iraqi employees who fear for their lives and already received security checks as part of their employment will nevertheless have to wait six months for the Department of Homeland Security to run an additional security clearance before they are allowed to resettle here.

a. What role does the FBI play in supporting Department of Homeland Security background checks for refugees?

b. What can you do to speed up the clearance process for Iraqis who have a target on their backs because of their association with the U.S. government?

Response:

It is our understanding that DHS does not submit to the FBI name check requests related to background checks for refugees.

41. My constituents frequently write to me with concerns over lengthy times for immigration and naturalization processing. This leaves families separated for months. It also means that thousands of elderly and disabled refugees lose subsistence benefits because they cannot complete naturalization within the seven years for which they are able to receive SSI. I understand that background and other security checks are a big cause of the backlog.

a. What role does the FBI play in this process, especially in the name check process? What are you doing to speed up the FBI's part of the process?

Response:

Through its National Name Check Program (NNCP), the FBI disseminates information from its files in response to requests submitted by Federal agencies, such as the U.S. Citizenship and Immigration Services (USCIS). From the

beginning of FY 2007 through July 31, 2007, the FBI has received over 3.2 million name checks (with over 1.6 million coming from USCIS) and has completed over 3.3 million (with over1.6 million of these belonging to USCIS). Additionally, USCIS submits criminal check requests (the fingerprint portion) to the FBI's CJIS Division for processing.

The FBI is seeking a number of improvements to its process, in the near term, mid-term, and long term.

Near Term

- Working creatively in partnership with other Government agencies to streamline the process. Some agencies have provided employees and/or contractors to assist in the processing of name checks.
- Continuing the development of a computer database that works with the current name check system to eliminate paper processes and the duplicate preparation of reports.
- Completing a new employee development program to streamline the training of new employees in the name check process.
- Scanning all paper files to produce machine-readable documents to build an electronic records system.
- Working with customers to streamline incoming name check requests and automate the flow of information between the FBI and its customer agencies.
- Adjusting the fee schedule to reflect the actual cost of providing name check services. This will provide the FBI with additional resources to address workload demands.

Mid-Term

- Procuring textual analysis software and investigating other ways to further automate the name check process.

Long-Term

- Developing a Central Records Complex to create a central repository of records. Currently, paper files/information must be retrieved from over 265 locations throughout the FBI. The Central Records Complex will address this issue and will create a central document repository and scanning facility.

b. What happens to people who have very common names?

Response:

The processing of common names requires extensive analysis to ensure that any information provided to USCIS pursuant to a name check request is attributed to the correct person.

c. What process exists for expediting completion of the name check process in appropriate cases?

Response:

Name check requests are expedited at the request of the submitting agency.

d. What kinds of changes would you recommend that we make to the current clearance process to allow greater efficiency?

Response:

The FBI is currently implementing several improvements to the Name Check process. Many of these efforts are being undertaken with the USCIS, which is the FBI's largest customer for this service. These improvements, coupled with the additional resources to be provided by the new user fee currently under development, should substantially improve the process.

e. What kinds of changes would you recommend that we make to the current clearance process to allow greater transparency?

Response:

The FBI is committed to working with the USCIS and its other (over 70) customers to provide the information needed for clearance adjudication. The FBI,

USCIS, and DHS have recently agreed to improvements in the process that will support a reduction in the name check backlog that is consistent with our shared national security and public safety goals.

Questions Posed by Senator Biden

Personnel Issues at the FBI and Their Impact on National Security

1,000 ADDITIONAL FBI AGENTS

42. I noted that in answers to written questions from Senator DeWine you discussed an issue that we discussed privately several years ago - the reprogramming of FBI agents from crime to terrorism. In fact, you indicated that you have lost 994 FBI criminal case agents since September 11th. And, because of this "the FBI has made difficult choices on how to most effectively use the available agents."

My view is that Public safety should be our number one priority, and I think of all the challenges that you are facing with reforming the FBI shortages of agents should not be one. Quite simply, you must have the resources to respond to terrorism AND crime. To this end, I introduced a bill that would authorize an additional 1,000 agents to fill this gap.

Do you view the FBI's responsibility to prevent and respond to crime and would 1,000 additional agents ultimately assist you in meeting the dual challenges of addressing crime and terrorism in the post 9-11 era.

Response:

The FBI's post-September 11, 2001 reallocation of SAs previously assigned to its criminal program did not diminish the FBI's commitment to criminal matters, but it did reduce the number of FBI SAs available to prevent and respond to crime. For a substantial increase in SAs to be fully effective, such an increase should also address the corresponding need for additional equipment and other infrastructure, as well as support employees. If these needs are not addressed, the effectiveness of any additional SAs will not be fully realized.

UP AND OUT POLICY

43. In addition to needing more agents to meet the challenges of crime and counterterrorism, I am concerned that your personnel decisions are compounding the problem. Last year the Bureau began implement a personnel policy related to the Supervisory Special Agents (SSA) wherein SSA with many years of experience supervising investigations are being forced to choose between re-locating to FBI headquarters in Washington or

accepting a decrease in compensation and giving up their supervisory duties under the so-called "up or out" policy.

Based upon the most recent information, 162 SSA's that were subjected to the "up or out" policy last yea[r], and many of these agents made the decision to leave the bureau rather than [being] re-located to headquarters or give up their supervisory positions. In addition, this year there are roughly 255 SSAs who will be subject to the policy and to this point four have resigned, 15 have stepped down, and 41 have retired.

These SSAs have developed extensive expertise and relationships in their field offices, and I am very concerned that a policy that increases the early retirement of agents with supervisory experience[] harms national security and further exacerbates personnel problems at the FBI.

Are you concerned that losing this many supervisory agents to earlier retirement due to the enforcement of this policy harms counter-terrorism efforts and criminal law efforts within the FBI field offices?

Response:

The Field Office Supervisory Term Limit Policy (FOSTLP) was designed to better position the FBI for the challenges of the future. As the FBI evolves toward a global intelligence-driven agency with increased focus on counterterrorism, hostile intelligence services, and international criminal enterprises, it is important to ensure that our front-line leaders develop a broad base of experience and progress as managers. The FOSTLP promotes the growth and diversification of experience in the supervisory ranks through a strong emphasis on continued career development.

When the FOSTLP was being developed, the FBI considered allowing those SSAs promoted prior to June 2004 to remain in their positions but, given the terrorist threat level and the escalating complexities of criminal conspiracies, the FBI could not afford the luxury of waiting five years before realizing the benefits of this policy. Based on our recognition that those SSAs affected by this policy were among our most experienced mid-level managers, though, a grace period ranging from two to three years based on tenure was established to allow these SSAs an extended opportunity to advance their careers, and several options were made available to accomplish this intent.

Although some of the field SSAs subject to the FOSTLP have relinquished their managerial positions, and some have retired, these results are in line with

historical data and therefore have not been substantially affected by implementation of the FOSTLP. In addition, many field SSAs have advanced their careers as a result of the FOSTLP rather than returning to investigative duties. For example, the candidate pool for ASACs has increased dramatically since the implementation of the FOSTLP, and field SSAs are filling critical FBIHQ positions such as Unit Chief, Assistant Section Chief, Legal Attaché, and Assistant Inspector. Field SSAs are also participating in other career enhancing opportunities, such as the Alternate Headquarters Credit Plan and the Inspection Team Leader Pilot Project, which are designed to provide experienced field SSAs with the critical FBIHQ experience needed for career advancement.

44. Have you taken any steps to address this problem?

Response:

Please see the response to Question 43, above.

RETENTION OF AGENTS IN HIGH COST CITIES

45. Director Mueller: I am also concerned that the high cost of living is impacting staffing levels and morale of field agents our big cities, where it is imperative we focus our efforts on crime and terrorism. Indeed, assignment of agents to our high-threat cities should be a high priority. I realize that Congress provided pay increases to agents assigned to certain high-cost cities back in 1991.

Is it your view that the parameters of this program are suitable to meet the needs of your work force and to enhance retention in high cost cities?

Response:

The reference to 1991 legislation appears to relate to the New York demonstration project, the authority for which expired many years ago. The FBI does, though, use several other statutory authorities to address the impact of the high cost of living experienced in some of our cities.

The Federal Workforce Flexibility Act of 2004 allows the FBI to offer retention or relocation bonuses in appropriate cases, and the Consolidated Appropriations Act of 2005 (CAA) affords to the FBI specific authority to address the impact of living in high cost areas. The CAA allows the FBI Director to offer bonuses of up to 50 percent to retain FBI employees with unusually high or unique qualifications or to relocate FBI employees to areas with higher costs of living

than their current residences (as determined by the Director). Although the FBI has used both of these authorities to assist our SA retention efforts, the language of the CAA regarding relocation bonuses is limiting, because it applies only to individuals "transferred to a different geographic area with a higher cost of living." This language does not allow the FBI to offer relocation incentives to those SAs needed in many high cost areas. For example, the CAA does not allow the FBI to offer a relocation bonus to an SA relocating from New York City or Los Angeles to Washington, D.C., because it is not clear that the cost of living in Washington, D.C., is higher than it is in New York City or Los Angeles. In addition, the CAA expires on December 31, 2009, so we cannot build a retention program on which SAs can rely into the future.

46. The use of housing allowances have been used effectively by other agencies, such as the Department of Defense, have you taken any steps towards establishing a housing allowance or other steps to help ensure retention in high-threat, high-cost cities?

Response:

We have considered various means of improving our retention of SAs in high cost areas. A housing allowance would require statutory authority, since the FBI does not currently have the authority to offer housing allowances. We would be pleased to work with OMB, Congress, and others in DOJ to evaluate housing allowances and other incentives to encourage our SAs to relocate to, or remain in, high-threat, high-cost cities.

Questions Posed by Senator Schumer

47. John McKay, the former U.S. attorney in the Western District of Washington, reportedly faced complaints about his decision not to prosecute allegations of election fraud in Washington's 2004 gubernatorial election. Did the FBI agree with Mr. McKay's decision not to prosecute allegations of election fraud in Washington's 2004 gubernatorial election, discussed above?

Response:

Pursuant to a citizen's complaint, the FBI's Seattle Division reviewed allegations of voter fraud in Washington State's 2004 gubernatorial election. The Seattle Division and the U.S. Attorney's Office for the Western District of Washington agreed that the information presented and the substance of the allegations did not merit a Federal investigation. The alleged voter fraud appeared to be individual voter misconduct, which would fall under the jurisdiction of Washington State authorities.

48. David Iglesias, the former U.S. attorney from New Mexico, was also reportedly criticized for his handling of allegations about flawed voter registration cards in the 2004 election. Did the FBI agree with Mr. Iglesias's decision not to prosecute any case about flawed voter registration cards in the 2004 election, described above?

Response:

The FBI's Albuquerque Division agreed with DOJ, including the United States Attorney's Office (USAO) for the District of New Mexico, that there was insufficient evidence to support Federal charges of election fraud in that case.

49. In the judgment of the FBI, was there sufficient evidence to support any federal charge of election fraud in the matters handled by Mr. McKay and Mr. Iglesias?

Response:

The FBI agreed with the decisions of United States Attorneys McKay and Iglesias regarding the election fraud matters at issue.

50. In the judgment of the FBI, were there any election fraud allegations that merited federal charges, but were not pursued, in the jurisdiction of any of the U.S. attorneys asked to resign in 2006?

Response:

The FBI is not aware of any 2004 election fraud allegations that merited Federal charges but were not pursued in the jurisdictions of the United States Attorneys asked to resign in 2006.

I also ask that you provide the following:

51. Copies of any documents in the custody, control or possession of the FBI regarding the allegations of election fraud in Washington discussed above and the FBI's recommendations in that matter;

52. Copies of any documents in the custody, control or possession of the FBI regarding the allegations of voter registration fraud in New Mexico, described above, and the FBI's recommendations in that matter;

53. Copies of any documents in the custody, control or possession of the FBI regarding allegations of election fraud that were investigated by any other U.S. attorney who was asked to resign in 2006, and the FBI's recommendations in those matters; and

54. Any other documents in the custody, control or possession of the FBI that are relevant to election fraud matters handled by any of the U.S. attorneys who were asked to resign in 2006.

Response to Questions 51 through 54:

These documents were also requested pursuant to a letter from Senator Schumer to Director Mueller dated April 2, 2007 and will be addressed separately.

Questions Posed by Senator Specter

FUNDING FOR NATIONAL SECURITY MATTERS

55. At the hearing, I asked you whether the FBI has sufficient funding for intelligence and counterintelligence matters to protect the nation from another terrorist attack. You replied, "We have requested funds that we have not received, whether it be through the Department of Justice or through the budget process. So there are items we need and would want that would enhance our ability to protect the American public."

a. Please explain what funding the FBI has requested for these priority programs and not received.

b. Also, please respond in writing to my follow-up question at the hearing: "How much additional funding does the FBI need on intelligence and counterintelligence matters to protect the nation from another terrorist attack?"

Response:

The FBI continues to work with OMB and others in DOJ to identify areas of future investment necessary to support both the national security and law enforcement missions of the Bureau.

JUSTICE DEPARTMENT INSPECTOR GENERAL'S REPORT ON NATIONAL SECURITY LETTERS (NSLs)

56. The Inspector General's report on NSLs states that, when the FBI's Office of General Counsel learned of the problems with the "exigent" letters in 2004, it began to implement corrective measures such as "discontinuing the use of exigent letters except in true emergencies." In contrast, reports in the *Washington Post* and the *New York Times*, as well as testimony before the House Judiciary Committee by FBI General Counsel Valerie Caproni, suggest that the FBI was not fully aware of the problem until 2006. Furthermore, the *Washington Post* and the *New York Times* have reported that Bassem Youssef - who currently heads the FBI unit that improperly used the exigent letters - raised concerns about the improper use of exigent letters when he took office in early 2005. The reports say that his concerns were ignored. According to his lawyer, Steve Kohn: "He discovered [the exigent letter procedures] were not in compliance, and then he reported that to his chain of command. They defended the procedures and took no action ... their initial response was to deny the scope of the problem."

a. When did the FBI's Office of General Counsel first become aware of the problem with so-called "exigent" letters?

Response:

As noted in the response to Question 32, above, multiple reviews of the exigent letter matter are currently underway. It appears that some FBI OGC attorneys may have become aware of aspects of the exigent letter practice sometime in late 2004.

b. When were corrective measures taken?

Response:

Upon learning of the exigent letter practice, and continuing into 2006, OGC attorneys offered a series of recommendations concerning this practice, among which were that exigent letters were inappropriate in the absence of a true emergency. As noted in the response to Question 32, above, multiple reviews of the exigent letter matter are currently underway.

c. Were the concerns of Mr. Youssef ignored?

Response:

As noted in the response to Question 32, above, multiple reviews of the exigent letter matter are currently underway. It should be noted, however, that the IG has testified that SSA Youssef did not raise the exigent letter with the IG when he was interviewed and that Youssef, himself, signed at least one exigent letter.

57. You have said that the FBI plans to remedy many of the problems addressed in the NSL Report. With regard to the misuse of exigent letters, in your written testimony, you said that the General Counsel's office "has been working with the affected unit to attempt to reconcile the documentation and to ensure that any telephone record we have in an FBI database was obtained because it was relevant to an authorized investigation and that appropriate legal process has now been provided." You also said that, at last count, "there were still a small handful of telephone numbers that had not been satisfactorily tied to an authorized investigation. If we are unable to determine the investigation to which those telephone numbers relate, they will be removed from our database and destroyed."

a. Other than removing improperly obtained information from the database, what is the remedy for those people whose privacy was violated by improperly used exigent letters?

Response:

There is no statutory remedy for individuals whose records may have been improperly obtained through the use of exigent letters. That said, it should be noted that telephone information obtained by the FBI pursuant to NSLs is normally received in bulk on computer disks and consists largely of dates, times, and durations of calls. No person's privacy is invaded beyond the bare receipt of this telephone record information unless link analysis or other investigation reveals that the communications are of legitimate investigative interest.

b. Although the IG "did not find any indication that the FBI's misuse of NSL authorities constituted criminal misconduct," will you hold FBI personnel who signed exigent letters accountable if you find they knew there were no exigent circumstances or they knew there was no contemporaneous intention to seek legal process (such as a subpoena)?

Response:

The DOJ IG and the FBI's Inspection Division are conducting a joint investigation into the use of exigent letters. When those inquiries are complete, the Director will determine what steps should be taken.

58. In years past, you have asked this Committee to consider authorizing the FBI to issue administrative subpoenas in counterterrorism cases. Given the lack of internal controls identified in the Inspector General's report on NSLs, why should Congress consider giving the FBI even greater authority to obtain records and other materials unilaterally, without court supervision?

Response:

If we are to be able to protect the United States from terrorist attacks, we must have access to the kinds of information obtainable by NSLs or administrative subpoena. As discussed in response to Question 35, above, the kind of data obtainable by NSL is mission essential, serving as a critical factor in our ability to produce leads that help identify terrorist networks. While NSLs are extraordinarily useful, they do have limitations. Unlike administrative subpoenas, NSLs reach only a narrow type of third-party records. The concerns voiced by

the IG indicate confusion on the part of some FBI agents regarding the technical requirements imposed by the NSL statutes. The IG did not identify any intentional FBI misuse of its investigative authorities or indication that the FBI was engaging in investigations based solely on the exercise of First Amendment rights or other prohibited criteria. The FBI's response to the IG's concerns shows its willingness to address any perceived gaps in training or errors in the implementation of its lawful authorities.

U.S. ATTORNEY DISMISSALS AND FBI POLICY OF NOT RECORDING INTERVIEWS

59. The FBI has a policy of not recording its interrogations electronically, in contrast to the more than 500 police departments in all 50 states that now make electronic recordings of at least some interrogations. This policy has received publicity in connection with the dismissal of U.S. Attorney Paul Charlton and the trial of I. Lewis "Scooter" Libby. Specifically, a March 4, 2007 *New York Times* story states that Charlton "annoyed Federal Bureau of Investigation officials by pushing for confessions to be tape-recorded." With respect to the Libby trial, a February 12, 2007 *New York Times* op-ed by Adam Liptak observes that jurors in the Libby case had to "rely on an F.B.I. agent's recollection, based on notes," because key interviews were not recorded. The author asks: "Why is the Federal Bureau of Investigation still using Sherlock Holmes methods" in the age of computers?

a. Did the FBI complain about Paul Charlton's efforts to require the recording of interviews?

Response:

In a letter dated February 9, 2006, then United States Attorney Paul Charlton advised Federal law enforcement agencies in the District of Arizona that beginning March 1, 2006, the Arizona USAO would require law enforcement agencies to record, by either audio or audio and video, the statements of all criminal suspects. On March 1, 2006, Charlton advised that he was delaying implementation of this policy while DOJ reviewed it in conjunction with law enforcement agencies to determine whether it should be a pilot project for the broader implementation of this policy. Under the policy, the Arizona USAO would not pursue prosecution if investigative interviews were not recorded, with limited exceptions, even if other evidence supported criminal charges. The policy permitted reasonable exceptions at the sole discretion of the AUSA assigned to the case and that attorney's supervisor.

Because this policy created a requirement not recognized in the Rules of Evidence, and imposed on the government a penalty not applied to other similarly situated parties, the FBI sought DOJ review before implementation. Specifically, the FBI disputed United State Attorney Charlton's claim that the lack of a recorded confession was a key factor in the negative outcomes in three criminal cases, noting that a number of other factors had contributed to those outcomes. The FBI also disputed Charlton's description of FBI policy as prohibiting the recording of interviews or confessions, noting that the FBI's Phoenix Division was already recording many such statements and that other FBI field offices also record subject interviews. Pursuant to the FBI's current policy, which has been in effect since 1998, Special Agents in Charge (SAC) can authorize the recording of confessions and witness interviews in all types of cases, ranging from traditional criminal investigations to national security investigations. The FBI's policy recognizes that many factors are considered when deciding whether to record a confession or interview, and that a blanket requirement mandating recording in all cases would be unnecessarily burdensome. SACs receive substantial guidance regarding the relevant factors and are afforded the discretion to weigh these factors in making their decisions.

b. Do you believe the FBI's policy complicated the Libby prosecution?

Response:

As indicated in response to subpart a, above, the FBI's policy does not preclude the electronic recording of interviews. Instead, this decision is made on a case-by-case basis, and the determination not to record the interviews in this case was made because it was believed that doing so would chill the fact-gathering process, hampering the investigation rather than forwarding it. In this case, in particular, the absence of recordings had no adverse impact on the Libby prosecution because Libby and other critical witnesses were examined during the grand jury process, so a word-for-word transcript of their testimony was created at that time.

c. Why does the FBI maintain this policy?

Response:

The FBI's practice of recording some, but not all, interviews is consistent with the practice of many other law enforcement agencies. While the policies of law enforcement agencies vary widely in this regard, they rarely mandate the recording of all interviews. The FBI's policy of permitting the SAC to authorize recording as required by investigative needs recognizes that local policies vary

and that recording does have some investigative and practical disadvantages. For example, a requirement to record all interviews would be quite expensive, would create significant logistical challenges, and may create obstacles to the admissibility of lawfully obtained statements that are not recorded through either inadvertence or circumstances beyond the control of the interviewing agents. In addition, the very presence of recording equipment may actually undermine the FBI's highly successful rapport-building interview technique.

Additional information responsive to this request is provided separately.

INTELLIGENCE ANALYSTS

60. At a January 2007 Intelligence Committee hearing, Deputy Director John Pistole said the FBI has hired roughly 2200 intelligence analysts. At the same hearing, Dr. John Gannon stated that FBI analysts are "given minimal training and deployed into organizations that are managed by agents." He then compared this unfavorably to how analysts are treated in the CIA and DIA.

a. Please describe the general experience and background of the analysts hired by the FBI.

Response:

In the past 3 years, the FBI has been successful in recruiting and hiring 1,488 Intelligence Analysts (IA) with the skills and backgrounds needed to build the FBI's intelligence program, including those with general analytic skills, those with particular specialized skills, and those with the specific knowledge needed to understand and analyze particular types of information. The FBI's IAs come to us from various positions and backgrounds, including other Intelligence Community (IC) agencies, academia, state and local law enforcement, the United States military, and the private sector, and have a wide range of critical skills in such subject areas as regional studies, international security, law, computer engineering, computer science, engineering, financial security, international banking, international migration, Islamic studies, physical science, religious conflict, and weapons of mass destruction (WMD).

This successful recruitment effort was conducted pursuant to a targeted recruitment strategy that identifies the critical skills the FBI needs to satisfy its current responsibilities as well as those required to address its future needs. The FBI is updating its IA recruitment strategy to reflect the current hiring

environment within the intelligence workforce and anticipates releasing a modified version of this strategy by the end of 2007.

b. What training are they provided by the FBI?

Response:

The FBI's intelligence training is designed to align with IC standards for content and tradecraft, addressing the policy, authorities, and oversight requirements relevant to a robust domestic intelligence mission, augmented as appropriate by material uniquely relevant to the FBI's dual missions of intelligence and law enforcement. To ensure that training remains a top FBI priority, the FBI's Directorate of Intelligence (DI) has established a special assistant position specifically focused on training. Below are descriptions of the courses and training initiatives designed to meet the needs of the FBI's IAs.

Intelligence Analyst Courses

- Intelligence Basics Course (IBC) – In collaboration with the FBI's Training Division (TD), the DI is currently redesigning the entry level course for new analysts. This course will emphasize the three tradecraft skills (thinking, expository writing, and briefing) critical to an analyst's professional success and necessary to the production of more sophisticated, forward-leaning analysis and to its effective delivery to a range of consumers. The IBC will give students a solid foundation for their continued professional development by exposing them to a variety of techniques and exercises that will improve their ability to: think creatively but check the insights they develop with rigorous, structured, and skeptical scrutiny; craft accurate, concise, and comprehensible written products for consumers who have very little time to read and understand them; and deliver the same high quality analysis orally under a variety of circumstances. Students who finish the IBC will be better prepared to fulfill a variety of roles at the FBI and to contribute to the success of its unique intelligence mission. This 10-week course will be comprised of modules that can be used in various combinations to provide tailored training to a field office or to groups of field offices.

- Managing Analysis Course - In coordination with the TD, the DI has conducted the Managing Analysis Course, which was piloted in August 2006, on two additional occasions. This course was developed to enhance the effectiveness of those responsible for supervising analysts; many

supervisors are not, themselves, analysts. The workshop, which will be presented over days using a variety of exercises, provides supervisors with a set of tools and management techniques they can use to enhance the rigor and quality of the analytic products generated by their offices. The workshop addresses such issues as the role of analysis in the intelligence cycle, categorizing various types of analysis, how to avoid analytic traps and mind sets, selecting and characterizing evidence, meeting the needs of various customers, elements of effective warning, and understanding analysts and their core competencies. The last half day will be taught by DI personnel and will include discussions of the intelligence production and review process and of the promotion process. Feedback regarding this course, which requires both pre-workshop and evening homework, continues to be positive, and we are making adjustments to optimize the value of the course. To date, 115 students have received this training.

Reports Officer Course - In coordination with the TD, the DI ran a pilot of the newly developed one week basic Reports Officer (RO) course in January 2007. This course was designed to give entry-level ROs a clear idea of their responsibilities and to enable them to achieve greater consistency in their duty performance. Participants will learn about RO roles and responsibilities, the national requirements structure and collection requirements process, what intelligence is and how to discern intelligence information from operational information, the importance of Intelligence Information Report (IIR) follow-up, and the legal authorities that govern collection and reporting. The course will teach students how to refine techniques for drafting various intelligence products, including division-specific IIRs, teletype memos, requests for information, and responses to *ad hoc* requirements. Additionally, participants will benefit from a panel discussion with experienced ROs and be challenged by an intensive IIR practical writing exercise. Feedback from the pilot course has been very positive and we are in the process of making appropriate changes suggested by developers, instructors, and the pilot's students.

Collection Management Course - This course provides overviews of intelligence collection requirements management, collection operations management, and the national intelligence prioritization and needs process, and provides familiarization with open source intelligence, the Open Source Requirements Management System, imagery intelligence, signals intelligence, measurement and signature intelligence, and human intelligence. The course will be taught at Quantico by a mobile training

team from the Defense Intelligence Agency (DIA) Joint Military Intelligence Training Center (JMITC).

- Counterdrug Intelligence Analyst Course - This course will examine the nature of organized criminal activity in drug trafficking and serves as a baseline for understanding the techniques, tools, and procedures used to analyze these organizations and derive intelligence. It will be taught at Quantico by a mobile training team from DIA's JMITC. Additional iterations will be offered based on demand.

- Counterintelligence Analytic Methods Course - This course provides a counterintelligence foundation for IAs who work strategic and operational-level all-source analytic issues. The analyst will also be able to demonstrate a counterintelligence methodology that accurately evaluates assets, threats, vulnerabilities, and risks associated with FBI counterintelligence support activities. The counterintelligence analyst's relationships with collectors and customers are continually examined and emphasized during the four day course. This course will be taught at Quantico by a mobile training team from DIA's JMITC. Additional iterations will be offered based on demand.

- Counterterrorism Analyst Course - This course introduces new counterterrorism analysts to the nature and extent of the terrorism threat and associated analytical challenges and techniques. Emphasis is placed on student collaboration and multiple exercises. This course will be taught at Quantico by a mobile training team from DIA's JMITC.

- WMD Terrorism Course - This workshop provides a basic overview of the technical and terrorist threat aspects of nuclear, chemical, and biological weapons. Participants will be introduced to counterterrorism policy and to the various Federal Response Elements and the role each plays when responding to a WMD event.

- Financial Intelligence Seminar (DIA) - This seminar provides analysts with the basic tools needed to uncover the trails of money that support terrorist activity, are generated by narcotics cartels, or result from other international crimes. The goals of the course are to apply financial analysis techniques, in the context of critical thinking and structured analytic techniques, to improve the quality of financial analyses and assessments of intelligence target operations. The seminar provides tools and techniques for analyzing financial networks and developing actionable

intelligence. It focuses on how money moves through banks, money services businesses, and informal value transfer systems (such as hawalas), examining the impact this movement has on operational decisions. The seminar includes learning blocks on money laundering schemes and indicators, terrorism financing, financial critical thinking, and trade-based transfer systems. In the financial analysis section, the students will study sources of information, bank record analysis, financial patterns, financial data charting, and financial profiles. The course is capped by a three and a half hour interactive exercise involving multiple bank accounts. Financial experience or background is not a prerequisite for taking the course.

Domain Management

- Fundamentals of Geographic Information Systems – As part of DI's effort to implement domain management practices and methodology, the DI has, in partnership with the National Geospatial-Intelligence Agency, tailored a one week course that teaches basic applications of geographic information systems in FBI domain management. During FY 2007, DI will host seven such classes. These classes have been attended by both FBIHQ and field SAs and IAs.

Tools and Techniques

- Analyst Notebook - The Analyst Notebook training will be presented over four and a half days using a variety of exercises. Students will learn the fundamental concepts and features necessary to create and analyze Association and Timeline charts. Using scenario-driven exercises, students will learn how to: manually create charts and import structured data to make charts; use basic functional tools with the software to query, find, and analyze data within the charts; switch a chart from association to temporal or vice versa; merge and combine charts; use attributes in charts; and set up charts for presentation.

- Pen-Link - The three day Pen-Link course provides instruction regarding various Pen-Link databases, including Calls, Subscribers, Events, Seizures, Case Management, City-Link, and International, as well as multi-media storage and Title III (wiretap) information. Students will become familiar with basic configuration options, manual data entry, Pen-Tran, built-in database reports, built-in frequency reports, built-in special reports, graphic analysis, and custom reporting.

- Denial and Deception - This course discusses methods used by foreign governments and groups to deflect and distort intelligence collection and analysis. The course, which will be taught at Quantico by a mobile training team of DIA's JMITC, will provide an introduction to the methods and tools available for identifying and neutralizing foreign denial and deception tactics. Additional iterations will be offered based on demand.

- Open Source Intelligence Course (Hidden Universes) - This three day course, which will be taught by Open Source Academy instructors, will offer a baseline understanding of the rich, complex, and dynamic world of open-source information as leveraged by the IC. The course will also introduce the latest tools and strategies that help IC personnel exploit open sources quickly, efficiently, and knowledgeably, and will familiarize students with the basic elements of a robust open source acquisition, exploitation, and dissemination process.

- Advanced Tools and Techniques - This course engages analysts in a highly interactive, hands-on environment and covers some 20 tools and techniques that can enhance the sophistication and rigor of finished analytic products. Analysts participate in numerous practical exercises using tools such as argument mapping, brainstorming, key assumptions check, red cell analysis, analysis of competing hypotheses, social network analysis, advanced devil's advocacy, risk security analysis, and others. In addition, students will engage in interactive discussions of analytic traps and mind-sets, how to collaborate more effectively in virtual environments, how best to use these tools and techniques in written products, and how to integrate these advanced tools and techniques into their daily work process.

c. How does the training provided to analysts by the FBI, in terms of curriculum, duration, and similar factors, compare to the training provided by the CIA and DIA?

Response:

The FBI is orienting its training for new analysts to mirror the CIA's new analyst training. After reviewing other organizations' courses for new analysts, including those run by the CIA, DIA, and NSA, the FBI determined that the CIA's Career Analyst Program (CAP) was most closely aligned with the FBI's intelligence

requirements. In revising our basic intelligence training for new analysts and developing the new IBC, we have been using the CAP as a template.

The FBI's 10-week IBC is designed to introduce our new analysts to the world of intelligence and analysis while focusing on three fundamental skills: critical thinking, expository writing, and briefing. We have developed a close working relationship with the CIA's Kent School and are adapting a number of the CIA's core modules and exercises for use in the IBC.

Immediately following the restructuring of the IBC curriculum, the FBI will begin adapting key modules for delivery to FBI employees who supervise analysts. We anticipate a three to five week "Developing Analysts" course that will help ensure that analysts and supervisors, regardless of position, have the same vocabulary and are on the same analytic page conceptually.

d. To what extent has the Director of National Intelligence implemented standardized training for analysts in the Intelligence Community?

Response:

While the Office of the Director of National Intelligence (ODNI) has not required that the FBI conform its training to an ODNI standard, it has offered guidance through the provision of training competencies, the Intelligence Community Officer Certification Program, ODNI-sponsored training and programs, and presentations by various leadership speakers. Below are some examples of ODNI-sponsored initiatives in which the FBI is actively engaged.

Intelligence Community Training Initiatives

- Intelligence Community Officer Training (ICOT) - The ODNI-sponsored ICOT certification requires 400 hours of training in the following seven categories: National Security and Intelligence Issues; Leadership and Management; Counter Intelligence (CI), Security, Information Assurance, Denial and Deception; Production and Analysis of Intelligence; Collection, Sources, and Processing of Intelligence; Impact of Intelligence across the IC; and the IC Officer Course. While training may be obtained from a variety of sources, including IC classes, the FBI, or universities, course objectives must relate to at least one of the aforementioned categories to receive credit for ICOT certification purposes. To date, one FBI IA has earned IC Officer certification.

- Intelligence Community Assignment Program (ICAP) – ICAP, a structured rotational program within the IC, is designed to provide intelligence professionals (GS-13s, 14s, and 15s, as well as highly qualified GS-12s) with the opportunity to gain IC experience through rotational assignments in intelligence or intelligence-related positions associated with the participants' parent organizations. Two FBI employees have completed ICAP tours and are eligible for ICAP certification pending completion of end-of-tour surveys. Two more candidates are expected to complete ICAP tours next year and would then be eligible for ICAP certification in 2008.

- Summer Hard Problem Program (SHARP) – SHARP is a four week program sponsored by the Office of the Deputy Director of National Intelligence for Analysis. Students in this program investigate the intelligence implications of the factors that cause individuals and communities of interest to coalesce into pro-social, antisocial, terrorist, or extra-legal movements. FBI participation in the 2006 initial offering was praised, and the FBI has been encouraged to nominate candidates for upcoming programs.

- Rapid Analytic Support and Expeditionary Response (RASER) Team - Four FBI IAs joined other IC colleagues in the two year ODNI-sponsored RASER program. The purpose of the RASER team is to establish a group of multidiscipline, highly-trained analysts ready to deploy worldwide on demand. ODNI tasked each of the IC agencies to nominate five candidates for the 12 positions; all five of the FBI's applicants were awarded positions on the team.

- ODNI Leadership Day Speakers Series - The FBI hosted ODNI's first annual Intelligence Community Leadership Day. Presenters from the FBI included the FBI's senior leadership, as well as leaders from across the IC. The FBI will continue to participate in this series and plans to send approximately 30 senior-level employees to the next ODNI Leadership Day.

TERRORIST IDENTITIES DATAMART ENVIRONMENT (TIDE) AND THE TERRORIST SCREENING CENTER (TSC)

61. The *Washington Post* has reported that, each day, thousands of pieces of intelligence information from around the world are fed into a central list of terrorists and terrorism suspects known as TIDE, which is maintained by the National Counterterrorism Center.

According to the *Post*, TIDE has "[b]alloon[ed] from fewer than 100,000 files in 2003 to about 435,000." Moreover, "the growing database threatens to overwhelm the people who manage it." According to the article, "The bar for inclusion is low, and once someone is on the list, it is virtually impossible to get off it. At any stage, the process can lead to 'horror stories' of mixed-up names and unconfirmed information." The article even quotes Russ Travers, the official in charge of TIDE, as saying: "The single biggest worry that I have is long-term quality control."

The article adds, "Every night at 10, TIDE dumps an unclassified version of that day's harvest -- names, dates of birth, countries of origin and passport information -- into a database belonging to the FBI's Terrorist Screening Center." The article acknowledges that, for inclusion in the FBI's database, the "bar is higher than TIDE's," leading to total listings of about 235,000. Nevertheless, the article raises several issues:

a. Do you have concerns that these lists are growing too large to manage?

Response:

The FBI pursues a counterterrorism watchlist strategy designed to enable law enforcement and screening personnel to effectively detect, disrupt, and/or track those suspected of participating in terrorist networks, requiring that the subjects of both preliminary and full-field investigations be watchlisted. The FBI's TSC continues to monitor the growth of the Terrorist Screening Database (TSDB) to ensure that its collection strategy is appropriate, that it is maintained consistent with the policy set forth in Homeland Security Presidential Directive 6, and that it serves the needs of its customer agencies. In collaboration with these customer agencies, TSC continues to examine the data collection methodology to ensure the terrorism screening process is as efficient and effective as possible.

b. Given the problems with internal controls elsewhere at the FBI, are you confident that these systems are not infringing on the privacy rights of innocent people?

Response:

The TSC has a robust privacy compliance program in place, led by a full-time Privacy Officer, to ensure the personal information TSC maintains is protected by strong privacy and security policies and practices. The TSC Privacy Officer reports to the TSC Director and is responsible for establishing internal policies and procedures to ensure the TSC complies with the laws and policies regulating the handling of personal information and to recommend additional policies that would enhance compliance with information privacy principles.

Following are examples of the TSC's efforts to ensure privacy rights are protected.

- The TSC has implemented quality controls at the various stages of the watchlist process to increase the quality of TSDB data. For example, in March 2006, TSC began to use a newly developed business process (known as the Single Review Queue) to ensure every new nomination or modification of a watchlist record is reviewed for quality by a member of TSC's Nominations Unit before inclusion in the TSDB. TSC analysts review the nominations to ensure, to the extent possible, the accuracy of biographical data and the sufficiency of the derogatory information supporting the watchlist nomination. Nominations are refused if they are not supported by adequate biographical information or derogatory information indicating a nexus to terrorism.

- The TSC's redress process provides for timely and fair review of individuals' complaints and the correction any data errors, including errors in the terrorist watchlist itself.

- The TSC's Data Integrity Unit is continually reviewing TSDB data to ensure it is accurate, thorough, and current. Examples of efforts by the Data Integrity Unit are the recently completed 100 percent review of the No Fly List and the ongoing 100 percent review of the Selectee List.

- The TSC has developed procedures to ensure that, every time a possible encounter with a watchlisted person is phoned into the TSC, an Operations Specialist assigned to the Terrorist Screening Tactical Operations Center reviews the relevant entries in the TSDB and other relevant data systems for completeness and accuracy. If a record is determined to be accurate and complete, it is maintained. If, however, modification or removal appear to be necessary, the TSC coordinates with the nominating agency and the National Counterterrorism Center to ensure the record is adjusted or removed, as appropriate.

- The TSC has performed privacy impact assessments of its information technology systems in compliance with the e-Government Act of 2002 and has published a Privacy Act notice describing its system of records in compliance with the Privacy Act of 1974.

- The TSC has integrated privacy risk assessments into various parts of the information technology system development life cycle to ensure privacy risks are identified early and mitigated appropriately.

- The TSC has developed and applied to the TSDB technology-oriented business rules designed to identify records that appear to have erroneous, inconsistent, or otherwise discordant data and to ensure prompt correction of this information.

- The TSC is reviewing staffing needs to ensure the availability of adequate staff to conduct audits and internal compliance reviews to improve both data quality and the efficiency of business processes.

DOMESTIC SPYING BY THE NEW YORK POLICE DEPARTMENT

62. The *New York Times* has recently reported that the New York Police Department (NYPD), in preparation for the 2004 GOP Convention, gathered and disseminated intelligence information on what appeared to be lawful political activity: "In hundreds of reports stamped 'N.Y.P.D. Secret,' the Intelligence Division chronicled the views and plans of people who had no apparent intention of breaking the law ... These included members of street theater companies, church groups and antiwar organizations, as well as environmentalists and people opposed to the death penalty, globalization and other government policies."

I understand that an April 2006 Inspector General report titled "Review of the FBI's Investigative Activities Concerning Potential Protesters at the 2004 Democratic and Republican National Political Conventions" cleared the FBI of similar allegations. Nevertheless, the recent reports about the NYPD raise new questions:

a. Did the FBI collaborate with, or give guidance to, the NYPD with respect to intelligence gathering prior to the GOP Convention?

Response:

Along with the Secret Service and the New York Police Department (NYPD), the FBI served on a committee focused on the responsibilities and mechanics of intelligence dissemination during the Republican National Convention (RNC). The committee did not provide guidance regarding intelligence gathering. Instead, the committee focused its efforts on the dissemination of intelligence related to the existing international terrorism threat through the Joint Terrorism Task Forces (JTTFs), in large part based on the fall 2004 threat concern.

In response to a request from Congress, DOJ's OIG reviewed the FBI's investigative activities with respect to potential protestors at the 2004 Democratic and Republican national political conventions. The OIG conducted over two dozen interviews of FBI personnel, including those assigned both to field offices (including New York) and to FBIHQ (including the Counterterrorism Division, Counterintelligence Division, and OGC). The OIG also examined approximately 10,000 pages of documents produced by the FBI in response to the OIG's document requests. Among the documents analyzed by the OIG were FBI investigative case files, information retrieved from FBI databases, correspondence, guidance memoranda, and manuals. The OIG concluded that the FBI's investigative activities were based on the threat of criminal activity and that its investigative conduct was consistent with the applicable Attorney General Guidelines.

b. Did the FBI receive any intelligence information on lawful political activity from the NYPD?

Response:

The FBI's New York Field Intelligence Group (FIG) had SAs and Task Force members embedded in the NYPD Intelligence Fusion Center and elsewhere during the RNC. During this event, the NYPD prepared and disseminated to both the FIG and the FBI's Joint Operations Center (JOC) daily situation reports concerning RNC activities, including arrests, demonstrations, and delegate and VIP movement. The situation reports provided information regarding both legal and illegal demonstrations focusing on location, direction of movement, time, arrests, and participant numbers. The FIG and JOC received real-time intelligence from the NYPD concerning information included in the daily situation reports, and FIG members participated in the formal daily briefings to law enforcement agencies. The FIG assessed this and other information and provided to appropriate customers intelligence related to potential international and domestic terrorism threats both to the United States generally and to New York City and the RNC specifically. This information was included in the NYPD situation reports, which were intended to provide situational awareness for all law enforcement agencies involved with the RNC and were provided to multiple law enforcement agencies. The FIG received the NYPD situation reports and disseminated them internally to JTTFs and FBI personnel involved with the RNC.

c. In your view, does the fact that the NYPD felt a need to engage in such far-reaching intelligence gathering reflect a lack of confidence in the FBI's ability to provide local law enforcement with necessary information?

Response:

The FBI's mission during National Security Special Events is to support local law enforcement efforts to identify terrorism threats, and it works closely with the JTTFs, which include local law enforcement representatives, to do so. The FBI highly values the contributions of the NYPD and other State and local law enforcement agencies to the JTTF and to other task forces, and strongly believes the JTTF partnership is the most effective way to prevent terrorist attacks.

The relationship between the FBI and NYPD has continued to grow and evolve. The FBI and NYPD have worked together closely to prevent attacks, and both have adjusted operations to address the threat in a manner consistent with their respective authorities. In his September 12, 2006, prepared statement to the Senate Committee on Homeland Security and Governmental Affairs, the NYPD Deputy Commissioner for Counterterrorism, Richard A. Falkenrath, stated: "[T]he NYPD's most important federal partner in the field of counterterrorism [is] the Federal Bureau of Investigation. The NYPD has an excellent partnership with the FBI's field office in New York. . . . [O]ver 100 NYPD detectives are assigned full-time to the Joint Terrorism Task Force in New York City. The JTTF permits the awesome power of the federal government's national intelligence capabilities to be brought to bear against any particular terrorism case. . . ."

LEAK INVESTIGATIONS

63. There was a leak three weeks before the last election about an investigation into Congressman Curt Weldon, who represented Delaware County in the Philadelphia suburbs. The following week, there was a search and seizure at the property of Congressman Weldon's daughter. At your December 2006 hearing, you stated that you were conducting an ongoing investigation of this leak. Can you provide an update on the status of this investigation?

Response:

The FBI has interviewed 121 personnel, 85 of them FBI, as well as a number of other individuals, and analyzed internal records in furtherance of this investigation. The investigators were unable to identify a suspect or substantially

narrow the pool of possible suspects. Accordingly, the investigation was closed on October 1, 2007.

Questions Posed by Senator Grassley

MICHAEL GERMAN TRANSCRIPT

64. through 83.

As Congress has previously been advised, the contents of the transcript are highly sensitive because a person with knowledge of these circumstances could identify the parties from the context provided. Similarly, many of the questions based on the transcript provide sufficient details to permit this identification. The transcript excerpts, the questions, and the FBI's responses are, consequently, provided separately.

JANE TURNER VERDICT

84. Former FBI agent Jane Turner recently won a $565,000 verdict from a federal jury in Minnesota. The jury found that her supervisors had made false and misleading statements in her performance reviews in retaliation for her for filing an Equal Employment Opportunity claim. I recently wrote asking what steps the FBI is going to take to discipline the supervisors responsible for the retaliation. However, all I got back was a letter saying that you don't comment on personnel matters.

a. You say you won't tolerate retaliation, but what are you doing about this? A jury found that FBI supervisors retaliated against someone, why can't you at least tell us whether the FBI is taking any action to consider holding accountable the people who did it?

Response:

The jury found that two of Jane Turner's former supervisors in Minneapolis retaliated against her for her complaints of discrimination. One of them, former Supervisory Senior Resident Agent (SSRA) Craig R. Welken, retired from the FBI in 2001 and the other, former ASAC James H. Burrus, Jr., retired on May 1, 2007.

Some media accounts have incorrectly identified James Casey as one of the FBI supervisors who retaliated against Ms. Turner. Mr. Casey was not assigned to the Minneapolis Division and his only involvement arose from his participation in the October 1999 inspection of the Minneapolis Division, which included the Minot Resident Agency (RA), Ms. Turner's office of assignment. That inspection resulted in Ms. Turner's "loss of effectiveness" transfer from the Minot RA back

to the Minneapolis headquarters office, which the jury specifically found did not constitute retaliation.

b. I understand the FBI may appeal the decision. Why is that a wise use of FBI resources? Do you think the jury got it wrong? If so, why?

Response:

After careful consideration by the FBI and DOJ, the judgment was not appealed. In light of the jury's verdict, DOJ determined that an appeal was not in the best interests of the United States.

DeVECCHIO CASE

85. As you know, I've previously expressed my concerns about the appearance given by current and former FBI agents who are publicly supporting Lindley Devecchio. He is a former agent currently charged with four counts of murder in New York, under circumstances similar to the scandals exposed a few years ago in the Boston FBI office. You have assured me that the FBI takes no position and that you will let the legal process play-out in court. However, recently I learned that the Justice Department is paying at least part of Devecchio's legal bills and that the prosecutor's requested documents that the FBI has not provided. For example, the prosecutors in New York would like to see the entire informant file for the mob informant that Devecchio allegedly helped in a mafia war in the 1980's.

a. In order to approve paying his legal bills, did the FBI make any determination or certification that Devecchio acted lawfully and within the scope of his employment?

Response:

Pursuant to regulations governing the representation of Federal employees by DOJ attorneys or by private counsel furnished by DOJ (28 C.F.R. § 50.15), the FBI submitted to DOJ a statement containing its findings as to whether DeVecchio was acting within the scope of his employment and whether such representation would be in the best interest of the United States. This statement was accompanied by all relevant information available to the FBI. All material prepared by FBI and DOJ personnel in this regard is protected by the attorney-client and attorney work-product privileges.

b. Why is the FBI withholding evidence from local prosecutors in a murder trial?

Response:

The FBI is not withholding evidence from the prosecution. Pursuant to applicable Federal law (see, for example, *United States ex rel. Touhy v. Ragen*, 340 U.S. 462 (1951), and 28 C.F.R. § 16.21, *et seq.*), the numerous requests of the Kings County District Attorney (DA) for FBI and other Federal records and information in this case have been handled by the USAO for the Eastern District of New York. The USAO reviewed related FBI records and information in order to properly respond to the DA's requests, proffering the testimony of FBI personnel having first-hand factual information and authorizing the release to the DA of thousands of pages of FBI records. These records included all relevant portions of the informant file of Gregory Scarpa, Sr., the informant with whom DeVecchio is accused of having conspired, and records of all FBI payments made to Scarpa during the relevant time period. To the extent that any related FBI records or information were not produced, this was based upon the USAO's determination that such information was not relevant and that production should therefore not be authorized pursuant to the *Touhy* regulations set forth at 28 C.F.R. § 16.22(d). It is the FBI's understanding that the production of FBI records and information was acceptable to the DA's lead prosecutor, and that the DA's office has made no requests for additional FBI information since August 2006.

c. I understand that the FBI's General Counsel, Val[e]rie Caproni, had some involvement in the underlying facts when she was at the U.S. Attorney's Office in New York. What role, if any, has she played in the decision to withhold documents from the local prosecutors?

Response:

General Counsel (GC) Caproni has played no decision-making role regarding the DA's requests for production of FBI records and information. Pursuant to applicable Federal law, and as discussed further in response to subpart b, above, such decisions have been made by the responsible USAO.

d. Have you analyzed whether it might be appropriate for her to recuse herself from any such decisions?

Response:

GC Caproni recused herself from decision-making in this case in April 2006. As discussed in response to subparts b and c, above, decisions regarding disclosures to the DA of FBI and other Federal records and information in this case have been made by the responsible USAO pursuant to applicable Federal regulations.

AMERITHRAX

86. I recently learned from depositions in the lawsuit that Stephen Hatfill filed against the FBI, that you denied the lead investigator's request to polygraph FBI agents. He said he wanted to do that in order to get to the bottom of who in the FBI was leaking information about the case to the press. I also learned that instead, you ordered the three squads working on the case not to talk to each other - to put up stovepipes to prevent sharing information.

a. Why wouldn't you allow the investigators to do what they felt was necessary to find out who at the FBI was leaking?

Response:

The FBI Director has a clear policy against the leaking of confidential law enforcement information, and his communications with those involved in the anthrax investigation were consistent with this policy. As indicated in the Director's deposition, he generally believes that the use of polygraph examinations is productive in investigations involving a narrow universe of individuals to be examined. That was not the case regarding the anthrax investigation leaks, where the universe of possible leak sources included the FBI, DOJ, the U.S. Postal Service, Congress, and others. More central to this particular case, though, is that the leak investigation was handled by DOJ's OPR, not by the anthrax investigation team. In fact, we presume DOJ's OPR would have objected to outside activities that might impact their investigation.

b. Did the FBI take any other steps to find out who was responsible? For example, were the telephone records of agents with access to the information examined to find out if they had been talking to the reporters who published sensitive information? If not, why not?

Response:

The FBI cooperated fully with the investigation by DOJ's OPR. We defer to DOJ's OPR with respect to the acquisition of telephone records and other investigative steps.

c. Rick Lambert, the former lead investigator, testified that putting up walls between the investigators working different aspects of the case risked keeping the FBI from "connecting the dots" like before 9/11. Given his strong concerns, why did you overrule him and direct that he "compartmentalize" the case?

Response:

It is critical that investigators have access to all relevant information when they are seeking to identify relationships among various facts. Particularly since the attacks of September 11, 2001, the FBI has placed great emphasis on information sharing, and has instituted numerous mechanisms to ensure that we "share by rule and withhold by exception." One "exception" (meaning, one circumstance in which information sharing is not appropriate) is when such sharing would not benefit the investigation at issue, such sharing may adversely affect that investigation (such as by encouraging or contributing to information leaks), and the absence of such sharing is not likely to adversely affect other investigations. This was such a case.

87. Also in the deposition transcripts in the Hatfill lawsuit, there is an indication that the FBI did some kind of background records check on constituents who wrote to their member of Congress about the case and whose letter had been referred to the FBI for comment by the Member of Congress.

a. Does the FBI routinely do these records checks on citizens who contact their elected representatives to inquire about an FBI matter?

Response:

According to the referenced transcript, the deposition witness indicates that when we receive constituent and similar inquiries the FBI queries "ACS." Although the witness indicates that ACS is "the system that the FBI employs and generates peoples' criminal background history," this is not the case. The FBI's Automated Case Support (ACS) system contains FBI-generated documents, including investigative information and other FBI documents uploaded pursuant to FBI policy. While ACS is queried by those familiar with its contents and uses to

address the substance of an inquiry (typically by obtaining either substantive case information or the identity of a subject-matter expert who can assist in responding to the inquiry), FBI practice is not to use ACS to obtain information regarding the person making the inquiry, such as a constituent.

b. Were records checks performed on all constituent mail referred to the FBI, or only on those involving the Amerithrax investigation? Were records checks performed only on authors of letters critical of the FBI or supportive of Stephen Hatfill?

Response:

ACS queries are conducted for the purpose of obtaining substantive information to respond to constituent inquiries, not to obtain information about the constituents themselves. This is the case regardless of whether the inquiry concerns the anthrax investigation.

c. Are Members of Congress given any notice that referring a constituent letter to the FBI may result in an FBI records check on their constituent?

Response:

Referring a constituent letter to the FBI does not result in an FBI records check on the constituent.