U.S. Department of Justice

Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

June 14, 2007

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

Dear Mr. Chairman:

Enclosed please find responses to questions posed to FBI Director Robert S. Mueller III, following Director Mueller's appearance before the Committee on December 6, 2006. The subject of the Committee's hearing was "Oversight of the Federal Bureau of Investigation." We hope this information is helpful to the Committee.

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 these responses. If we may be of additional assistance in connection with this or any other matter, we trust that you will not hesitate to call upon us.

Sincerely,

Richard A. Hertling
Principal Deputy Assistant Attorney General

Enclosure

cc: The Honorable Arlen Specter
Ranking Minority Member

Responses of the Federal Bureau of Investigation
Based Upon the December 6, 2006 Hearing Before the
Senate Committee on the Judiciary
Regarding FBI Oversight

Questions Posed by Senator Specter

TERRORIST SURVEILLANCE PROGRAM

1. I understand that you are bound by the constraints of information classification when speaking about particulars of the Terrorist Surveillance Program (TSP). However, could you respond to the following questions about the efficacy of the TSP?

a. Has the FBI made any arrests as a result of a lead generated from the TSP?

i. If so, how many?

ii. Can you provide a general description about the circumstances of the arrest(s)?

b. Have any terrorist plots targeting the United States been foiled through the TSP?

i. If so, how many?

ii. Can you provide a general description of the plot(s) being planned?

c. Have any FISA orders been sought by the FBI after and/or granted as a result of a TSP intercept? If so, how many?

d. Have any FBI cases been opened as a result of a TSP intercept?

i. If so, how many?

ii. Can you provide a general description of the case(s) opened following the TSP intercept?

Response to subparts a through d:

A full briefing on all aspects of the Terrorist Screening Program as it affects the FBI was provided to the Senate Select Committee on Intelligence.

As Director Mueller has testified, leads from that program have been valuable in identifying would-be terrorists in the United States and providing us leads concerning other individuals who warrant investigation.

REFORMING THE FBI IN THE MOLD OF BRITAIN'S MI5

2. A May 2005 Justice Department Office of Inspector General survey of more than 800 FBI analysts (two thirds of the total employed by the FBI at the time) found that, on average, analysts were spending only half their time doing analytical work (Audit Report 05-20).

a. What is being done to better utilize intelligence analysts both within the FBI's National Security Branch and in criminal cases?

Response:

The FBI's National Security Branch (NSB) is developing a workforce environment with defined career paths that will attract and retain intelligence personnel with critical skills and competencies needed to protect the nation against current and emerging threats. Currently, the FBI has more than 2,200 Intelligence Analysts (IAs), who are assigned across the FBI. Career paths that reward and develop technical experts in intelligence operations are essential to our ability to retain a world-class national intelligence workforce. In developing career paths for Intelligence Career Service (ICS) members, the FBI is using a competency-based approach to drive the intelligence workforce human resources continuum of selection and hiring, training and development, performance management, career progression, retention, and Intelligence Officer Certification.

Part of our strategy began with a snapshot of the current NSB workforce and an assessment of what the workforce must look like in the future. The NSB is working with the FBI's Human Resources and Training and Development divisions, and with other appropriate FBI divisions and the Office of the Director of National Intelligence (ODNI), to reengineer and refine an overall workforce, which will integrate ODNI human resource standards and processes and fill gaps to meet future needs.

We are conducting an ICS Competency Model/Job Task Analysis for each of the three job series that make up the FBI's ICS: IAs, language analysts, and investigative specialists. These analyses, which began in October 2006, are based on an employee's job series, grade, and work assignment, and are being conducted in accordance with the Uniform Guidelines on Employee Selection Procedures. For each competency developed, we will identify proficiency levels, measurable behavioral indicators, and related developmental opportunities. The contract to conduct this analysis was awarded to a firm that specializes in conducting human resource evaluations to establish business processes. We are committed to enhancing career paths for our ICS personnel, and the ongoing analysis is the first step in this complex process. Contract deliverables for FBI ICS competencies and their developmental opportunities are expected in 2007. The contractor has consulted with the Office of Personnel Management and ODNI regarding competency development; ODNI's common set of core competencies for analysts and collectors will inform the entire process of competency development and job task analysis. The NSB will use these results, in conjunction with the FBI's human resources and training components, to further develop our analytic cadre.

The FBI will develop specific performance measures after completion of both the SA and IA competency profiles, ensuring that they reinforce and are integrated with the ODNI's efforts to establish core competencies applicable throughout the Intelligence Community (IC). As part of the overall career development model for the NSB workforce, the FBI completed an inventory of career development opportunities, and identified gaps are being addressed based on this survey. The FBI will coordinate these profiles with the IC Chief Human Capital Officer.

The FBI is implementing several workforce programs to build its national security capabilities. These programs, which are designed to establish and enhance national security workforce specialties and to create training and developmental opportunities for IAs, will be developed in close coordination with the ODNI, to ensure that IC joint duty requirements and other functionally specific cross-community career paths are addressed. During 2006, the number of IAs in each Field Intelligence Group (FIG) was reviewed and recommendations were made for the assignment of the appropriate number of Supervisory Intelligence Analysts (SIAs), leading to the use of 25 IA positions for SIAs. A support relief position for SIAs is being established that will parallel the relief position for SAs. In 2006, 53 IA positions were added to FIGs to provide essential administrative support.

In addition to these initiatives, we are providing numerous training opportunities to elevate the stature of our intelligence professionals and to acknowledge the importance of our intelligence mission. Mirroring the successful SA hiring process, the FBI has implemented an aggressive schedule for hiring IAs and having them enter on duty at Quantico. We have also developed a course for supervisors assigned responsibility for the FIGs. The first FBI Managers of Analysts Course, a four-day workshop, was held at the National Academy in Quantico, Virginia, in August 2006. This workshop provides managers with a set of tools and managerial techniques they can use to enhance the quality of the analytic products they generate. It addresses such issues as the role of analysts in the intelligence cycle, categorizing various types of analysis, how to avoid analytic traps and mindsets, selecting and characterizing evidence, meeting the needs of various customers, elements of effective warning, and understanding analysts and their core competencies. Directorate of Intelligence (DI) personnel will hold discussions on the intelligence production and review process and the promotion process during the final portion of the workshop. The second iteration of this class, which was renamed "Managing Analysis," was held in November 2006. We plan on significantly increasing training for this critical group during the next six months.

Through the Kellogg School of Management, we have implemented joint-training seminars with SAs, IAs, language analysts, and surveillance specialists, entitled Navigating Strategic Change. The major theme for these seminars is accelerating the FBI's integration of the intelligence process into FBI operations. Topics discussed include strategic leadership, change implementation, and the role of intelligence in criminal as well as counterterrorism and counterintelligence cases. We identified 3,011 eligible FBI participants at the start of the program and, halfway through the program, 1,511 SAs, IAs, language analysts, and surveillance specialists had completed the 2.5-day Navigating Strategic Change course and 42 senior and mid-level executives had completed the five-day Leading Strategic Change course.

The FBI also continues to offer to our employees the opportunity to participate in Joint Military Intelligence College (JMIC) courses, and 43 employees are currently active in the JMIC program. Each academic year, 20 to 40 employees are enrolled in JMIC courses part-time and IAs are invited to pursue the Master of Science in Strategic Intelligence (MSSI) Program. Two employees are currently attending the full-time MSSI Program, which began in August 2006, and one employee is pursuing a bachelor of science in Intelligence Program full time. In addition, we are partnering with the University Education Program for future academic semesters in order to include the field divisions.

b. What is being done to ensure analysts have a stake in the work conducted by FBI Special Agents and JTTF officers?

Response:

Many of the efforts of the past several years have focused on building a team environment for SAs and IAs. Because training has played a key role in helping SAs and IAs understand their integrated roles, we have established several opportunities for joint training. Joint exercises between new IA and new SA classes emphasize that both play key roles in executing the FBI's intelligence mission. As we mentioned in response to subpart a, above, mid-level management SAs and IAs also participate together in the 2.5-day seminar on Navigating Strategic Change at the Kellogg School of Management and in a Managing Analysis course, which emphasizes the role of IAs and their core competencies.

This training has enhanced the collaboration between SAs and IAs outside of the classroom. Increasingly, SAs in field offices and at FBI Headquarters (FBIHQ) are paired with IAs on some of our most critical programs, and IAs sit side-by-side with SAs on field office squads and in the FIGs embedded in each field office.

As the FBI's Intelligence program matures, the role of the IAs continues to increase. IAs are now tasked with duties that go far beyond "supporting" SA's investigations and are, instead, part of a team that is identifying threats and driving our investigations. This IA role ensures that FBI analysts have a stake in the FBI's mission.

c. Do you agree with the findings of the May 2005 OIG audit? Have you conducted additional surveys to determine whether its conclusions are accurate? If so, what were the results? Do you intend to conduct further audits?

__Response__:

Even prior to the review of our analyst program by the Department of Justice (DOJ) Office of the Inspector General (OIG), the FBI had underway efforts to enhance and strengthen our analytic capabilities. Much of our work over the past several years has been aimed at addressing the concerns that were raised in this review. Specifically, we have worked to improve recruitment, hiring, and retention. We are also working to enhance the IA career path. As part of this effort, we have hired the Human Resources Research Organization to develop and validate a set of competencies for the IA position. This work will allow us to further refine our training, performance, and promotion measures for the IA position. We believe this will have a far-reaching positive impact on the FBI's IAs.

While we have not conducted any additional surveys, we have participated in the ODNI's Climate Surveys in 2005 and 2006. The 2005 survey revealed the commitment of FBI employees to the FBI's national security mission and to protecting the country. This survey also demonstrated that, while FBI IAs still experience some degree of frustration with their work environment, most are satisfied with the organization and its mission and remain committed to the FBI. Additionally, this survey indicated that IAs are very satisfied with their co-workers (both agent and non-agent) and believe the FBI provides an opportunity to contribute to a larger, well-defined mission, with 87% indicating that the work they do is important and 84% saying, "the people I work with cooperate to get the job done."

The FBI will continue to address the concerns raised in the 2005 survey. The results of the 2006 survey should be available in the next few months, and we will analyze those results to identify areas for improvement. We will continue to participate in this survey process and are committed to developing an intelligence workforce that is ready to meet the challenges facing the FBI.

3. On November 9, 2006, Dame Eliza Manningham-Buller, Director General of Britain's MI5 gave a detailed account of the terrorist threat facing Britain. She revealed that MI5 is currently investigating "some 200 groupings or networks, totaling over 1600 identified individuals" who are believed to be involved in nearly 30 plots to attack Britain. Given this recent statement, please describe to the committee [the following.]

a. [T]he number of groups or individuals being investigated by the FBI in terrorism cases.

b. [T]he number of suspected plots known to the FBI.

c. [T]he kinds of groups being investigated-e.g., fundraisers versus operational cells, or Al Qaeda affiliates versus homegrown groups.

Response to subparts a through c:

The responses to these questions are classified and are, therefore, provided separately.

IMPACT OF CHANGES IN SUPPLEMENTAL PATRIOT BILL

4. During the debate over reauthorization of the PATRIOT Act, I introduced a bill (S.2369) along with Senator Leahy to correct some of the provisions contained in the conference report negotiated with the House of Representatives. One provision of concern was the provision governing challenges to the so-called "gag" or non-disclosure requirement that accompanies National Security Letters and orders issued pursuant to Section 215 of the Patriot Act. Under the conference report, the recipient of an NSL or a Section 215 order can challenge the "gag," but there is a conclusive presumption requiring courts to uphold the "gag" if the government makes a good-faith certification that disclosure may endanger the national security of the United States or interfere with diplomatic relations. Our bill eliminates this "conclusive presumption" to give courts more discretion in reviewing the "gag" requirement.

a. Why shouldn't we trust Article III judges to make sound decisions about disclosure or nondisclosure?

Response:

The provisions adopted in the USA Patriot Act Improvement and Reauthorization Act of 2005 (the Act) to modify the so-called "gag" provisions of the National Security Letter (NSL) statutes and Section 215 of the PATRIOT Act were not the result of any distrust of Article III judges. To the contrary, they are carefully crafted provisions that conform to constitutional allocations of power. When the Executive Branch certifies that there should be non-disclosure of an NSL or a 215 order because disclosure would interfere with a criminal, counterterrorism, or counterintelligence investigation or endanger the life or physical safety of any person, that certification is fully reviewable by an Article III judge because the judiciary is fully competent to evaluate those possible harms. On the other hand, when the Executive Branch certifies (via a high level executive official) that disclosure of an NSL or 215 order might endanger national security or interfere with diplomatic relations, the Executive is making an assessment in an area that is at the core of the Executive Branch's Constitutional authority. In those instances (i.e., national security and foreign relations), the Executive Branch is better able to assess the risk caused by disclosure.

b. Would this change negatively impact the FBI's use of NSLs or Section 215 orders?

Response:

As indicated above, we believe the Executive Branch is best able to assess the harm to national security or to diplomatic relations that could be caused by disclosing the existence of an NSL or a 215 order, and that the statute should not be further amended.

SEAPORT PROTECTION

5. In your response to submitted questions from our May 2, 2006 hearing, you indicated that the FBI is working with the Coast Guard to alleviate coordination issues in the protection of our nation's seaports.

a. Have the FBI and the Coast Guard completed a new Memorandum of Understanding (MOU) regarding counterterrorism responsibilities in costal and littoral regions of the United States?

b. If not, is it in progress and are you confident that, in the meantime, should exigent circumstances occur, you and the Coast Guard could effectively work together to mitigate the threat?

c. Are you currently working under any documented guidance?

<u>Response to subparts a through c</u>:

The Maritime Operational Threat Response (MOTR) Plan was signed by the President on 11/8/06 and has been employed during maritime threat responses and fused into applicable training exercises at the national, state, and local levels with success. The FBI and United States Coast Guard agree that the MOTR Plan's coordination mechanisms have dramatically improved the operational response to maritime threats and incidents. In completing their preliminary analysis of the MOTR Plan's implementation, the Center for Naval Analysis noted that operations under the Plan have demonstrated increased unity of effort and interagency coordination.

RENDITIONS

6. The FBI's Inspection Division has conducted an internal review of the FBI's role in the Arar case and concluded that the FBI was not involved in the decision to remove Arar to Syria. In a response to a question posed by Senator Leahy during our hearing, you said, "...we did participate here in the questioning of Mr. Arar. We did not make the decision as to which country he should be deported to."

a. While your answer to Senator Leahy suggests the FBI may not have made the final decision concerning Mr. Arar's deportation, was the FBI involved in any way in the decision to send Mr. Arar to Syria?

b. If so, in what capacity was the FBI involved?

c. Which agency made the final decision in Mr. Arar's deportation?

<u>Response to subparts a through c</u>:

DOJ responded to this inquiry during a classified briefing on 2/1/07. In addition, a report by the Department of Homeland Security (DHS) OIG is pending.

7. At our hearing, you indicated the FBI has participated in the rendition of suspects removed from other countries and returned to the U.S. to face charges here. Can you confirm that the FBI has not participated in the rendition of any suspects to third countries for purposes of interrogation or detention?

<u>**Response**</u>:

The FBI has not participated in the rendition of suspects to third countries.

TECHNOLOGY UPGRADES/SENTINEL PROGRAM

8. In a previous appearance before the committee, you discussed the timing of completion of the Sentinel project. It is supposed to be completed by 2009. Is that still the anticipated date of completion?

<u>**Response**</u>:

Yes. The anticipated completion date for the development of the Sentinel System is still the end of 2009.

9. At our hearing, you discussed the potential impact of the lack of appropriations on the FBI's ability to keep Sentinel within its projected cost and timeframe. Please elaborate on the potential problems created by a failure to appropriate current funds for this project.

<u>**Response**</u>:

Under the third Continuing Resolution (Pub. L. No. 109-383), the FBI had neither funding nor authority to proceed with Phase 2 of Sentinel. Sentinel is estimated to cost $157 million in Fiscal Year (FY) 2007. The FBI requested $100 million for Sentinel in the FY 2007 budget, and has identified the remaining $57 million from prior year funds that remain available.

On 2/15/07, the President signed into law Pub. L. 110-5, 121 Stat. 8, "Revised Continuing Appropriations Resolution, 2007," which will provide for full funding of the FY 2007 request. Given this funding, the Sentinel program will proceed on schedule.

TRAC STUDY

10. The Transactional Records Access Clearinghouse (TRAC) at Syracuse University recently found that federal prosecutors "rejected" 87% of the international terrorism cases referred to them by the FBI in the first 9 months of FY 2006. It is my understanding that the FBI and the DOJ have challenged this claim.

a. Would you please explain your objections to the TRAC study?

Response:

The FBI objects to the methodology of the Transactional Records Access Clearinghouse study because it uses inaccurate figures, relies on a faulty assumption that every referral from an investigative agency should result in a criminal prosecution, and ignores the reality of how the war on terrorism is being conducted, particularly regarding the value of early disruption of potential terrorist acts with proactive investigation and prosecution. For example, the report criticizes the number of international terrorism referrals from the FBI that were not prosecuted, based on the apparent assumption that all referred cases should lead to prosecution. Often, in fact, matters are referred to prosecutors to assist in further investigation through the use of criminal investigative tools that require legal process such as subpoenas and surveillance orders.

b. Do you keep your own statistics on these international terrorism cases?

Response:

The FBI investigates Federal criminal violations, while DOJ attorneys prosecute these violations. The FBI has been advised by DOJ's National Security Division (NSD) that, after the attacks of 9/11/01, DOJ's Criminal Division and Executive Office for United States Attorneys began maintaining statistics concerning terrorism and terrorism-related cases with an international nexus. The statistics formerly maintained by the Criminal Division are now maintained by DOJ's NSD.

c. If not, what metrics do you use to measure success in combating international terrorism?

Response:

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

TERRORIST SCREENING EFFORTS

11. Multiple watchlists that existed before 9/11 have now been consolidated into the terrorist screening database (TSDB) maintained by the FBI's Terrorist Screening Center (TSC). Nevertheless, Inspector General Glenn Fine has identified inherent problems with the master list such as missing names and incomplete/inaccurate data. With this in mind, please answer the following questions:

a. How accurate and complete is the consolidated terrorist screening database?

Response:

The Terrorist Screening Database (TSDB) contains data on known or appropriately suspected terrorists that is provided to the Terrorist Screening Center (TSC) by either the National Counterterrorism Center (NCTC) (for international terrorists) or the FBI (for purely domestic terrorists). The TSC is not in a position to validate the derogatory information that justifies placement of an individual on the TSDB. For example, TSC has no ability to verify whether information in an intelligence cable is accurate or was obtained from a reliable source. TSC must rely upon the agencies that investigate terrorism and gather and analyze intelligence to provide accurate, complete, and current information to support terrorist watchlist nominations. Clearly, the agencies that nominate individuals to the watchlist are in the best position to ensure the adequacy of the quality controls employed to ensure the underlying intelligence and investigatory data support the inclusion of nominated individuals.

TSC has developed quality controls for the various stages of the watchlist process to increase the quality of the TSDB. First, since March 2006, TSC has used a software application called the Single Review Queue (SRQ) to ensure that every new nomination or modification of a watchlist record is reviewed by a TSC subject matter expert. TSC analysts review the nominations to ensure, to the extent possible, that the derogatory information supporting the watchlist nomination based upon a terrorism nexus is sufficient and accurate. TSC has developed technology business rules in TSDB to enforce minimum data and export requirements in order to identify and correct records that appear to have erroneous, inconsistent, or otherwise discordant data.

The TSC established an interagency working group to review the nominating criteria, finding that the criteria were valid but the guidelines for implementing them required revision. Based on this finding, TSC will conduct record-by-record reviews of the Transportation Security Administration (TSA) No Fly list and Selectee list, including thorough examination to identify records no longer meeting the criteria so they may be removed from the list.

TSC has also developed procedures to ensure that every time a possible encounter with a watchlisted person is phoned into the TSC, the TSC's call center staff will review the TSDB and other relevant data systems to identify records in which an individual's status has changed or other updates are required. If modifications or removals are required, TSC coordinates with the nominating agency and the NCTC to ensure that records are appropriately adjusted or removed.

As discussed below, TSC's redress process is also an important part of ensuring the accuracy and completeness of the TSDB.

b. What mechanisms or processes are afforded to those individuals incorrectly placed on the TSDB, or those whose name is confused with that of a suspected terrorist, who seek to challenge the accuracy of the government's information?

Response:

In January 2005, TSC established a formal watchlist redress process. The process allows agencies that use watchlist 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 terrorist watchlist itself.

The redress process consists of procedures to receive, track, and research watchlist-related complaints and to correct watchlist and other information causing an individual unwarranted hardship or difficulty during the screening process. TSC has worked closely with screening agencies to establish a standardized process for referral of and response to redress requests from the public. TSC also works with federal law enforcement agencies and the IC, which nominate individuals to the watchlist, to review redress complaints, evaluate their validity, and make appropriate corrections (including removal from the watchlist when warranted).

The terrorist watchlist would not be an effective counterterrorism tool if those who are watchlisted were able to learn the basis for their watchlist status. Consequently, to maintain the confidentiality of the watchlist, the redress process does not inform individuals, either orally or in writing, whether they have been watchlisted. The redress process also does not reveal the final determination of the redress matter, including whether the individual was removed from the watchlist. The TSC believes that the inability to provide transparency to affected individuals places on the TSC the burden to perform a critical, in-depth review of the information supporting each person's inclusion on the watchlist to ensure it meets the watchlist criteria. There is an enhanced redress process for individuals on the No Fly list, providing for an administrative appeal of any adverse redress decision that includes the ability to request any releasable information and to submit information for consideration during the appeal.

Those who are erroneously identified as watchlisted individuals (misidentified persons) often file redress complaints and corrective action is usually taken by the screening agency. The Government Accountability Office (GAO) recently completed a comprehensive review (GAO Report 06-1031) of the ongoing interagency efforts to improve the experience of misidentified persons, including efforts by DHS agencies to annotate their record systems to distinguish the individuals more quickly in the future. TSC's efforts to assist misidentified persons include recording encounters with misidentified persons and check these records when a new encounter occurs so TSC can rapidly identify and clear known misidentified persons.

Information regarding the watchlist redress process and how to file a complaint with a screening agency is available to the public on TSC's website at www.fbi.gov/terrorinfo/counterterrorism/tsc.htm. Other agencies that use TSDB data for screening, such as TSA, also have redress information on their web sites.

FBI NAME CHECKS

12. The FBI's National Name Check Program (NNCP) reportedly receives between 60,000 and 70,000 name check requests every week (3.3-3.5 million annually). Of these, over 28,000 (1.5 million annually) are related to immigration cases from U.S. Citizenship and Immigration Services within DHS, followed in volume by OPM and the State Department.

Although 68% of name checks are processed within 48 hours and 90% are completed within 30-60 days, the remaining 10% can take years to complete. The committee has been advised the FBI has contracted a comprehensive fee study to analyze how name checks are processed and measure direct and indirect costs.

a. What is the status of this study?

Response:

The National Name Check Program (NNCP) process is comprised of four steps: 1) batch, 2) name search, 3) file review, and 4) dissemination. The four steps vary in terms of automation levels and processing times.

- **Batch** - Most name check requests are received from customers on data tapes. Each data tape can contain up to 10,000 different name check subjects. These tapes are electronically checked against the FBI's Universal Index (UNI). UNI is an electronic subject/case index of all investigative and administrative matters that indexes names to cases. If the FBI's UNI database contains no identifiable information regarding a particular individual, the name is returned to the customer as having "No Record" (NR). Historically, 68 percent of the name check requests submitted by United States Citizenship and Immigration Services (USCIS) return no records in FBI files during batch and are completed within 48 to 72 hours, with the results returned to USCIS. The remaining name check requests are passed to the next step, which is "name search."

- **Name Search** – Analysts view each UNI record using a specialized computer application called the Name Check Program (NCP) to further refine the search and determine if any potentially valid file references pertaining to the name check subject exist. If no valid file references pertaining to the name check subject exist, the NCP returns an NR response to the customer agency. Historically, approximately 22 percent of the original name check requests submitted by USCIS are completed in this step within 30 to 60 days, with the results returning to USCIS. If potentially valid references still exist, the name check request proceeds to the "file review" phase.

- **File Review** - FBI files may exist in electronic or paper form. The file review staff attempts to locate paper files for review to determine applicability to the name check subject. Those name check requests not identified with an FBI file receive a final designation of NR and the results are forwarded to the customer agency. The remaining name check requests are passed on to the "dissemination" step.

- **Dissemination** - Research analysts examine each file to determine what information, if any, is pertinent to the customer agency, and then provide a response to the customer. If the FBI's information is derogatory, the NNCP provides this information to the customer as allowed by various laws, policies, and court orders that dictate the content of the response. The "dissemination" phase can take from 90 days to more than a year to complete.

In accordance with Office of Management and Budget (OMB) Circular A-25, the FBI is currently conducting a NNCP fee study. The study will be finalized within the next several months, at which time the FBI will pursue a rule change to update the current fee structure, which was put in place over 10 years ago.

b. What efforts are you taking to address the name check backlog?

Response:

The current backlog is due in part to a change in the name check process. In a pre-terrorism environment, only a "main" file name indexed in UNI that could be positively identified with a name check request from USCIS was considered responsive to that request. A "main" file name is the name of an individual who is, himself or herself, the subject of an FBI investigation. Because that approach ran the risk of missing a match to a possible derogatory record, the FBI and USCIS agreed that the FBI would alter its search criteria to include "reference" file names as well. A reference file name is the name of an individual whose name appears as part of an FBI investigation, but who is not the subject of the investigation, such as a witness interviewed by the FBI or an associate of a main subject. This change led to the resubmission in November 2002 of 2.7 million names *at one time*, which created an immediate backlog that is still impacting the processing of name checks. Currently, over 480,000 name check requests have been in process at the FBI for over 30-days, of which over 345,000 belong to USCIS. The FBI is currently revising the process to eliminate the backlog by increasing its capacity to process name checks and handle broader customer requirements.

The following short-term improvement efforts are in progress to address the name check backlog:

- The NNCPS is partnering with its customer agencies to provide contractor and/or personnel support. For example, in July 2006, OPM provided Top Secret cleared contractors to work on OPM's name check requests. To date, over 70 percent of the name checks that were considered to be a part of the backlog at the start of this initiative have been completed. NNCPS is working closely with USCIS to develop a similar strategy to reduce its backlog.

- NNCPS continues to make process improvements to its Name Check Dissemination Database (NCDD). The NCDD is an automated system that eliminates manual and duplicate preparation of reports to other agencies, providing opportunities for further automation of the name check process.

- NNCPS has implemented a new NNCP Employee Development Training Program to establish standard operating procedures and decrease the time it takes new employees or contractors to learn name check program processes.

- NNCPS has begun to build an Electronic Records System through the scanning of paper files. This process will enable employees to electronically access required files.

- The NNCPS is continually exploring innovative ways to streamline the incoming product and to automate the exchange of data with our customers in an effort to ensure a more secure and timely method of sending and receiving data.

Regarding a long-term improvement, the FBI is developing a Central Records Complex in order 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 scanning facility and document repository.

TURNOVER OF TOP COUNTERTERRORISM MANAGEMENT

13. Previously, you have attributed your high turnover rate of top level management personnel to their years of experience and the high level of demand in the private sector, coupled with their eligibility for retirement. That being said, in order to become an effective intelligence agency, consistency within your top-level managers is critical.

a. What steps are you taking to address this?

Response:

For the past ten years, retirement has accounted for approximately 85 percent of the attrition in the Senior Executive Service (SES) ranks. Since 9/11/01, we have targeted the best qualified personnel for promotions earlier in their careers in order to have a younger workforce entering the SES ranks. As a result, significantly fewer individuals currently in the SES ranks are eligible to retire than in the past several years.

b. Have you created any incentives encouraging top-level managers to stay with the FBI once promoted?

Response:

In May 2005, the FBI implemented new authorities for the payment of retention pay to those executives eligible to retire or considering leaving Federal service for other reasons. Since then, we have provided retention pay to approximately 30 SES officials as an incentive to remain with the FBI.

c. In your response to submitted questions from our May 2, 2006 hearing you argue that turnover in the EAD position for Counterterrorism and Counterintelligence has not harmed efforts to improve that division. Is continuity in this position not necessary? What impact has the high level of turnover had in your ability to meet your objectives in counterterrorism?

Response:

While continuity in all FBI executive positions is preferable, individual employees may elect to retire once they reach eligibility. Therefore, we have developed a strong team of professionals at the highest levels of the FBI to ensure that the departure of any one individual does not negatively impact our ability to meet our objectives in any FBI program. Recently, the FBI began developing a formalized Succession Plan for executive positions.

TRANSLATIONS

14. At our hearing, you indicated that the FBI has 33 agents proficient in Arabic at level two and 52 total in Middle Eastern languages (including Arabic, Turkish, Farsi, Urdu, etc.).

a. How many FBI agents are higher than level two in proficiency in Middle Eastern languages?

Response:

There are 37 SAs at the 2+ or higher proficiency level in Middle Eastern languages (see the breakdown below). The FBI considers SAs at level 2 proficiency to be productive linguists. At a level 2, the speaker is able to fully participate in casual conversations, express facts, give instructions, describe, report on, and provide narration about current, past, and future activities, and discuss family, interests, work, travel, and current events.

	Proficiency Level						
Language	**2+**	**3**	**3+**	**4**	**4+**	**5**	**Total**
Arabic	12	2	2	4	3	0	23
Hebrew	2	0	0	0	0	0	2
Farsi	4	3	1	1	0	1	10
Punjabi	1	0	0	0	0	0	1
Turkish	1	0	0	0	0	0	1

b. We understand the FBI has worked hard to expand the number of linguists in its analytical corps, however, are you concerned that the lack of language proficient agents may hinder your ability to interview and interrogate suspects and witnesses?

Response:

While the FBI is aggressively pursuing an increased population of SAs with proficiency in Arabic, we do have 267 linguists who are proficient in Arabic and who support our SAs. The FBI's language analysts and contract linguists are assigned to more than 100 locations throughout the world. Within the United States, the heaviest concentrations of the FBI's linguists are found in major metropolitan areas at our largest field offices. These offices have been the greatest consumers of the foreign language interpretation and translation services provided by the Bureau's Language Services Section. In these locations, language analysts routinely serve as interpreters accompanying SAs who conduct interviews or interrogations.

Used in this way, SAs benefit not only from the language analysts' native-level language abilities, but also from the linguists' native knowledge of history, culture, religion, and geography. Further, as native speakers, these linguists are often more adept at identifying non-verbal cues that a non-native speaker might not recognize. SAs also often rely on the language interpreting process itself - even when the SA has a working level of proficiency in the required language - as part of interrogation or interview tactics designed to elicit specific information from subjects or witnesses.

15. In your written response to questions submitted for the record from our May 2, 2006 hearing, you indicate that in the past 5 years, attrition for language analysts has ranged between 5 and 8 percent. You cite competition with private sector salaries as the principal factor in this level of attrition. What additional resources would be necessary to prevent the flight of skilled analysts?

Response:

The FBI would be pleased to work with DOJ, OMB, and the Congress to identify the appropriate resources.

16. In your written response to questions submitted for the record from our May 2, 2006 hearing, you indicate that 46.1 percent (3,240 hours) of the total backlogged audio recordings that need translation (7,028 hours) is due to obscure languages and unfamiliar dialects. What progress has been made in recruiting the necessary linguists to address this need?

Response:

The FBI continually recruits for all necessary languages, and attempts to address all work possible. The chart provided as Enclosure A reflects the hiring in recent years up to 12/31/06 in the critical counterterrorism languages. When the FBI does not have the language resources for a particularly rare language, we work with contractors and with the National Virtual Translation Center (NVTC) to address those needs. In one situation, the FBI used Department of Defense (DoD) contracts to provide cross-training for FBI Arabic linguists on an unusual dialect of Arabic that was needed. These resources provide a surge capacity in the FBI's most critically needed languages as well as a pool of linguists in less commonly needed languages that are important to the FBI's mission. Contract linguists must pass the same language test batteries and security vetting as full-time employees. Their Top Secret clearances, native-level proficiency in the foreign language, high-level of skill in English, and knowledge of the target culture make FBI contract linguists a highly desirable commodity in the IC. Many of the FBI's contract linguists provide support in languages that the full-time linguist staff does not cover. The FBI depends on the contract linguists and NVTC for a substantial amount of the needed support in many languages critical to the FBI's mission.

While the FBI continues to hire new contract linguists, it is currently converting many of the talented contract linguists hired since 9/11/01 to full-time language analysts, with the goal of maintaining a language workforce composed of one-third contract linguists and two-thirds FBI language analysts. This ratio will enable the FBI to maintain a stable workforce and will provide greater job security and benefits for the linguists proficient in the languages most needed to meet ongoing national security requirements.

Since May 2006, the FBI has made a special effort to focus on the backlog and has decreased the unaddressed counterterrorism work in the most critical languages to less than 1,000 hours. While the figures referenced in the May 2006 hearing pertain to counterterrorism cases only, audio backlog continues to be a concern for the FBI. In general, audio collection in the difficult and unusual languages represents only about 1% of the FBI's total audio collection in the past four years.

WHISTLEBLOWERS

17. Whistleblower Mike German has alleged that the FBI failed to investigate a potential terrorist link between white supremacist and Islamic extremists. During our investigation

of this case, our staff received two different versions of a crucial transcript. Neither version of this transcript was complete.

a. Can you explain the apparent discrepancies in the two versions of the transcript?

<u>Response</u>:

In connection with its investigation of this matter, by letter dated 2/3/06 the Committee requested from the DOJ OIG copies of documents the OIG relied upon in preparing its reports. The document request included the transcript of the 1/23/02 tape-recorded meeting between members of the foreign and domestic terrorist groups, which German had provided to the OIG in February 2003, and any other transcripts made of that meeting. By letter dated 7/27/06, the FBI provided the Committee with copies of the FBI documents responsive to this request, including copies of two transcripts of the 1/23/02 meeting.

One version of the transcript, identified with the text marking "037eb01.t3" at the top left of each page, was obtained from German on 2/12/03 during his interview by investigators from DOJ's OIG and FBI. German produced and referenced portions of this transcript in support of information he provided in his signed, sworn statement, and this version was attached to and made a permanent part of German's sworn statement. This version of the transcript is a rough draft of the transcription of a consensually monitored conversation that occurred on 1/23/02; it contains several instances of "unintelligible" conversations on the recording and abruptly ends on page 126. On page 49, the construction of this document changes from a rough draft format to FBI FD-302a format, and continues sequentially but displays the page number starting at 46. This "combination" document submitted by German contains duplicative pages of the rough transcription and the FD-302a, so that pages 46, 47, 48, and 49 are misnumbered yet sequential. It is unknown why German provided to OIG and FBI interviewers only 126 pages of a total 167 pages or why this document has a combination of transcript formats.

The second version of the transcript, identified with the marking "FD-302a" at the top left of each page, represents the draft of the entire transcription in the official FD-302a format. Because the header and footer on each page of an FD-302a reduce the remaining printing surface, the pages of this FD-302a draft do not line up exactly with the pages of the rough draft portion of the version obtained from

German. In the FD-302a draft, many, though not all, of the "unintelligible" portions that appear in the rough draft have been clarified. This FD-302a version is a complete transcription of the 1/23/02 conversation at 167 pages, or 31 pages more than the version provided by German.

b. Which of the two transcripts do you consider most accurate?

<u>Response</u>:

For the reasons discussed above, the version identified with the FD-302a marking at the top left of each page is the most accurate.

c. Will you provide the committee with the tape that this transcript is based on, in its complete form? If not, why not?

<u>Response</u>:

The Committee has not previously requested a copy of the tape in connection with its oversight investigation of this matter. Should we receive a Committee oversight request from the Chairman regarding this matter, we would be pleased to consult with DOJ as to the appropriate response.

<u>Questions Posed by Senator Grassley</u>

AMERITHRAX INVESTIGATION

18. a. Why was Richard Lambert removed as the head of the Amerithrax investigation?

<u>Response</u>:

Richard Lambert served as the Inspector in Charge of the Amerithrax investigation from 9/20/02 to 9/16/06. On 5/22/06, he applied for promotion to the position of Special Agent in Charge (SAC) of the FBI's Knoxville Division. The Senior Executive Career Board reviewed the qualifications of the interested candidates and recommended Richard Lambert for selection. On 6/16/06, Director Mueller announced the selection of Mr. Lambert as the Knoxville SAC.

b. Was it related in any way to disagreements between him and others working on the investigation about the proper scope and focus of the FBI's inquiry? If so, please explain.

Response:

Mr. Lambert applied for and was selected as Knoxville SAC based on his qualifications for the position.

c. Please identify and describe any and all documents related to Richard Lambert's transfer.

Response:

The FBI's Human Resource Division prepared the routine transfer orders reassigning Mr. Lambert from the Washington Field Office to the Knoxville Field Office.

19. a. Has the FBI been able to narrow the possible source of the anthrax used to a finite number of labs? If so, how many?

b. What basis, if any, does the FBI have to believe that the anthrax was obtained directly from a lab by the terrorist?

Response to subparts a and b:

Pursuant to the longstanding DOJ policy against disclosing non-public information concerning pending law enforcement and litigation matters, we are unable to provide a response at this time.

20. a. How many "persons of interest" other than the Dr. Stephen Hatfill are still of interest to the FBI?

b. How many, if any, individuals have been removed from the "persons of interest" list in the last five years?

c. Describe what criteria, if any, are used to determine when someone is removed from the "persons of interest" list.

Response to subparts a through c:

Pursuant to the longstanding DOJ policy against disclosing non-public information concerning pending law enforcement and litigation matters, we are unable to provide a response at this time.

21. **a. What has been the total cost of the investigation so far?**

b. Of the 9,100 interviews, 67 searches, and 6,000 grand jury subpoenas in the Amerithrax investigation, how many were unrelated to Dr. Stephen Hatfill?

c. How many were related to the potential that foreign-born terrorists were involved in the attacks?

d. How many were related to leads not consistent with the initial FBI suspect profile?

e. Has the FBI altered its initial suspect profile in any way in the last 5 years? Please explain why or why not.

Response to subparts a through e:

Pursuant to the longstanding DOJ policy against disclosing non-public information concerning pending law enforcement and litigation matters, we are unable to provide a response at this time.

22. Are the public reports true that Dr. Christos Tsonas at Holy Cross Hospital in Fort Lauderdale, Florida treated Ahmed al-Haznawi, one of the 9/11 hijackers for a lesion that he thought "was consistent with cutaneous anthrax" and that a 2002 memorandum prepared by experts at the Johns Hopkins Center for Civilian Biodefense Strategies concluded that the diagnosis of cutaneous anthrax was "the most probable and coherent interpretation of the data available?"

Response:

Pursuant to the longstanding DOJ policy against disclosing non-public information concerning pending law enforcement and litigation matters, we are unable to provide a response at this time.

23. In March 2002, John E. Collingwood, an FBI spokesman, was quoted dismissing the possibility that the 9/11 hijackers handled anthrax, saying: "This was fully investigated and widely vetted among multiple agencies several months ago. Exhaustive testing did not support that anthrax was present anywhere the hijackers had been."

a. Has exhaustive testing been conducted where Dr. Stephen Hatfill has been?

b. Did those test results support that anthrax was present in any of those locations?

c. If not, then please explain why those test results have not been announced publicly, just as the 9/11 hijacker test results were four years ago?

<u>Response to subparts a through c</u>:

Pursuant to the longstanding DOJ policy against disclosing non-public information concerning pending law enforcement and litigation matters, we are unable to provide a response at this time.

24. **a. What are the names of the officials responsible for determining that the anthrax attacks would be treated solely as a criminal law enforcement matter and not as an intelligence matter?**

b. On what date was that decision made?

c. Please describe what criteria are used to classify a case as a criminal matter rather than an intelligence matter.

d. Please identify and describe any and all records, documents, or memoranda related to that decision.

<u>Response to subparts a through d</u>:

Pursuant to the longstanding DOJ policy against disclosing non-public information concerning pending law enforcement and litigation matters, we are unable to provide a response at this time.

25. **a. Please describe the procedures for sharing information about the anthrax investigation with the rest of the intelligence community.**

b. Please describe the types and volume of information about the anthrax investigation that has been shared with the intelligence community.

c. Please describe the types and volume information about the Anthrax investigation withheld from the intelligence community, including a description of each occasion in which another government agency has requested information about the investigation and the request was declined.

Response to subparts a through c:

Pursuant to the longstanding DOJ policy against disclosing non-public information concerning pending law enforcement and litigation matters, we are unable to provide a response at this time.

26. **a. On how many occasions, and with what agency, has grand jury or other information gathered during the Amerithrax investigation been shared outside the Justice Department pursuant to Section 203 of the USA PATRIOT ACT?**

b. On how many occasions has information gathered during the course of the Amerithrax investigation been shared outside the Justice Department pursuant to Section 905(a)(1) of the USA PATRIOT ACT?

c. On how many occasions has information gathered during the course of the Amerithrax investigation been withheld under Section 905(a)(2)?

Response to subparts a through c:

Pursuant to the longstanding DOJ policy against disclosing non-public information concerning pending law enforcement and litigation matters, we are unable to provide a response at this time.

27. **a. Other than the FBI's Amerithrax investigative team, is there anyone else in the U.S. government tasked with examining the anthrax attacks and making a judgment about their likely origin?**

b. If so, please explain. If not, why not?

<u>Response to subparts a and b</u>:

Pursuant to the longstanding DOJ policy against disclosing non-public information concerning pending law enforcement and litigation matters, we are unable to provide a response at this time.

28. a. Has the FBI ever employed a "red-teaming" strategy in which a second group of investigators is tasked with looking at the evidence with the freedom to pursue alternative theories of the case?

b. If so, please explain. If not, why not?

<u>Response to subparts a and b</u>:

Pursuant to the longstanding DOJ policy against disclosing non-public information concerning pending law enforcement and litigation matters, we are unable to provide a response at this time.

29. a. What are the names of the officials responsible for the decision to impose a blanket prohibition on all Congressional briefings related to the Amerithrax investigation?

b. On what date was that decision made?

c. What is the legal justification for such a decision?

d. Please identify and describe any and all records, documents, or memoranda related to that decision.

<u>Response to subparts a through d</u>:

There is no blanket prohibition on all Congressional briefings related to the Amerithrax investigation. In fact, after receiving DOJ approval, the FBI contacted Chairman Leahy and offered to provide a briefing to him.

30. a. What steps have been taken to determine who was responsible for the alleged Congressional leak?

b. Did the alleged Congressional leak involve the disclosure of classified information?

c. Did it involve the violation of an agreement not to further disseminate the information?

d. If the FBI believes that a Congressional leak damaged its investigation, as was implied it its September 28, 2006, letter, what steps, if any, has it taken to describe tbe nature of the damage and communicate its concern to the appropriate leadership or other authorities in Congress?

e. If none, then please explain why not.

Response to subparts a through e:

Pursuant to the longstanding DOJ policy against disclosing non-public information concerning pending law enforcement and litigation matters, we are unable to provide a response at this time.

31. **a. On how many occasions have Justice Department and/or FBI personnel leaked investigative information about Stephen Hatfill or the Amerithrax case?**

b. What steps have been taken to investigate those leaks and discipline those responsible?

c. Please provide a list of the names of each government official interviewed, questioned under oath, or subjected to a polygraph examination regarding Amerithrax-related leaks, along with the dates of their testimony and the results of any polygraphs.

d. How many Justice Department and FBI personnel have been reprimanded or punished for leaking such information?

e. If any, please provide a detailed explanation of each instance.

f. What steps have been taken to prevent or deter future leaks by DOJ or FBI personnel of information related to the Amerithrax investigation?

__Response to subparts a through f__:

Pursuant to the longstanding DOJ policy against disclosing non-public information concerning pending law enforcement and litigation matters, we are unable to provide a response at this time.

32. Please explain why the reasons given now for refusing to brief Congress on the Anthrax case (that it is a pending matter and that it involves grand jury information), did not prevent the FBI from briefing Congress on the case three years ago.

__Response__:

Please see our response to Question 29, above.

33. According to public reports, two FBI agents were the anonymous sources for the *New York Times* stories implicating Stephen Hatfill as a "person of interest" in the investigation.

a. Is the FBI aware of aware of the identities of those two agents?

b. Did any other FBI official approve or have contemporaneous knowledge of their communications with the *New York Times*?

c. Will those two agents face any disciplinary action for unauthorized contact with the press? If not, why not?

__Response to subparts a through c__:

Pursuant to the longstanding DOJ policy against disclosing non-public information concerning pending law enforcement and litigation matters, we are unable to provide a response at this time.

d. If so, what is the range of potential punishment for such a violation?

__Response__:

The FBI's Penalty Guidelines set forth the range of disciplinary sanctions available in and applicable to employee misconduct cases. An employee who engages in the unauthorized disclosure of information may receive a disciplinary sanction ranging from a letter of censure to dismissal.

e. In your view, what would be an appropriate punishment under these circumstances?

<u>Response</u>:

It would be inappropriate to speculate on the appropriate disciplinary sanction without knowing the specific facts and circumstances of this case. OPR, the entity in the FBI charged with making these decisions, will review the investigative file, including witness statements, documentary evidence, and prior employment history, before making a final decision. As with all Federal agencies, the FBI decides an appropriate disciplinary sanction on a case-by-case basis, taking into account mitigating and/or aggravating circumstances.

FBI LEAKS

34. Just before the midterm elections, the FBI executed search warrants for properties owned by the daughter and an associate of Congressman Curt Weldon. The timing of the public disclosure of those searches left the FBI open to criticism and speculation about whether there was an attempt to influence an election.

An *Associated Press* story (10/16/06) said: "The search warrants were executed, in part, because of news reports over the weekend exposing the investigation, according to a senior Justice Department official[.] Typically, such searches are sped up to prevent any evidence from being destroyed." It appears that the FBI would not have executed these search warrants until after the election except for the fact that someone -- possibly an employee of the Justice Department or the FBI -- leaked the fact of the investigation to the media.

a. Does the FBI know the identity of the person who apparently leaked it to the media, and if not, have you initiated an investigation to find out?

<u>Response</u>:

An internal review of this matter is being conducted at the request of Director Mueller.

b. Has the FBI investigation into the House page scandal identified the person or people who apparently sat on former Congressman's Mark Foley's potentially criminal emails until their disclosure would have the maximum impact on an election?

Response:

This matter is addressed in the January 2007 report issued by DOJ's OIG.

c. Does the FBI know whether any DOJ or FBI employees have disclosed nonpublic information to a nonprofit group called Citizens for Ethics and Responsibility in Washington (CREW), and if not, has the FBI initiated an investigation to find out?

Response:

The involvement of the Citizens for Ethics and Responsibility in Washington in the matter relating to former Congressman Mark Foley is addressed in the January 2007 OIG Report.

HEDGE FUND DIRTY TRICKS

35. This past Summer a civil lawsuit was filed by a publicly-traded company alleging that it had been attacked by operatives of a hedge fund that was attempting to profit from selling the stock in the company short. The attack is alleged to have included a campaign of dirty tricks and harassment, including, in one instance, the mailing of a harassing package to the Pastor of the company's CEO. After the suit was filed, one of the defendants allegedly responsible for these activities went to the press, claiming to have been "deputized" by the FBI, and an FBI spokesperson was reported to have confirmed this. Recently, that gentleman, Spyro Contogouris, was charged and arrested by the FBI for wire fraud, on charges that I believe are unrelated to the civil suit.

a. Please explain what happened in this case and what the FBI has learned about Contogouris and his activities?

b. Please describe the nature of the interactions and relationship between Contogouris and the FBI. Was he at any time a cooperating witness and/or a confidential informant for the FBI or for any other federal law enforcement agency?

Response to subparts a and b:

Contogouris was arrested on 11/13/06 and is charged with one count of wire fraud. Consistent with longstanding DOJ policy regarding the disclosure of information concerning pending cases, the FBI declines to provide further information on this matter.

The FBI does not "deputize" members of the general public.

c. Related to that, how does the FBI screen and monitor confidential informants in non-terrorism, cases? What does the FBI do to ensure that a confidential informant or an FBI agent is not profiting from his or her knowledge of an ongoing investigation?

__Response__:

Criminal and internal FBI checks are conducted to baseline the history of a potential source at the time the potential source is identified, after which a source may be approved for continued recruitment. A source is then advised of the applicable Attorney General (AG) Guidelines and specifically cautioned against involvement in criminal activity other than that which is specifically approved by the FBI. Recruitment is followed by a suitability assessment during which we determine whether the source will be capable of performing the tasks desired by the FBI, as well as whether the individual will function in accordance with taskings, limits, and required controls. The operation of the source will be reviewed by a Supervisory Special Agent (SSA) at least once every 90 days while the source's relationship with the FBI continues and the source will be annually re-advised of the AG Guidelines. In addition, the responsible SAC is required to review a source who has been operated by the same Special Agent (SA) for an extended period and determine whether the SA will continue to operate the source. If the source should be arrested and entered into National Crime Information Center (NCIC), the FBI will be notified and will determine whether the operation of the source should be discontinued. Greater oversight is afforded for sources whose operations pose significant risk due to source's sensitive position and/or operational or investigative needs, such as those approved to conduct otherwise illegal activities (actions that would be illegal if not sanctioned by appropriate authority, as discussed further below) or used in undercover operations.

The FBI's newly established practice of validation provides for a separate review of the accuracy, reliability, and relevance of the source's information. The validation process also addresses the control we maintain of the source, including review to determine whether a source may be operating at the direction of a third party or manipulating the operation for his/her own benefit and against the interests of the FBI or the U. S. Government. A confidential source's improper use of information gained by virtue of his relationship with the FBI may constitute a violation of the law. A discovery that the source had disclosed FBI investigative information would result in a review to determine the damage to the pertinent investigation and the extent of wrongdoing on the part of the source, including whether the source had engaged in unauthorized illegal activity.

If an operation requires the source to engage in otherwise illegal activity, the FBI requires that the activity be supervised and approved in advance, and the AG Guidelines require that the relevant Chief Prosecuting Official, the responsible FBI SAC, and FBIHQ be notified. Continued operation of a source who has participated in unauthorized illegal activity requires the review and approval of the SAC and the concurrence of FBIHQ.

In order to protect against the improper use of FBI information for profit by FBI SAs, the FBI administers a comprehensive program of security awareness, education, and training with respect to all employees. The program provides explicit instruction on the proper handling and use of FBI information, as well as the potential penalties for noncompliance. In addition, the FBI's Enterprise Security Operations Center (ESOC) monitors FBI information technology systems to deter their misuse and to prevent other insider threats, such as hacking, malware, and unauthorized access. However, misuse of <u>authorized</u> access to FBI information is much more difficult to detect and prevent. Currently, the ESOC supports counterintelligence, criminal, and other serious misuse cases through the review, analysis, and correlation of many disparate sets of FBI business process data. In the near future, ESOC will implement a system that allows more effective detection of anomalous activity, further helping to prevent the misuse of FBI information. This system will use FBI business process data to automate both analysis and the development of leads, incorporating relevant security data from FBI operational databases, facility access databases, personnel databases, and other user activity logs to provide a complete picture of a user's behavior. By quickly and effectively collecting, sorting, and examining relevant data, the FBI will be able to rapidly identify indicators of misuse and other inappropriate activity.

Along with these technology-driven innovations, the FBI will continue to use regular personnel reinvestigations, including reviews of employees' financial circumstances, to detect willful and/or potentially criminal misconduct.

d. What guidelines and training govern how agents deal with potential informants who may be engaged in trading or short-selling securities or may be selling information to hedge funds?

Response:

The FBI has instituted a new comprehensive informant validation process for use by field offices and FBIHQ. The validation process includes quarterly SSA reports addressing the sources' motivation, access, timeliness, corroboration, and history. As discussed above, AG Guidelines address unauthorized criminal activity by confidential sources. These AG Guidelines are covered in the New Agent core-training received at the FBI Academy and reinforced through regular legal training provided in field offices during the remainder of an SA's career.

e. In October of this year, a former FBI agent Jeffrey A. Royer was sentenced to six years in prison for racketeering and securities fraud. According to witnesses at trial, the agent provided non-public FBI information to an outside party who used the information to spread negative publicity about companies and profit from short-selling their stock. What lessons can the FBI learn from this case?

Response:

In response to a recommendation in the March 2002 Webster Commission report, the FBI's Security Division (SecD) developed and implemented a comprehensive security awareness, education, and training program for all persons with access to FBI information. This comprehensive approach included the development of a professional cadre of highly trained Chief Security Officers, who now provide FBI personnel with the most up-to-date security policy, training, lessons learned, and best practices.

SecD uses a variety of educational methods, to include formal classroom training, web-based training, written guidance, and mentoring, to enhance the security awareness and education of the entire FBI population. Formal classroom instruction has included: the authorized procedures for releasing information to the public; refresher courses on establishing an information recipient's "need-to-know"; and the potential penalties for deviating from established procedures. Instruction is also provided in the form of "Non-disclosure and Releasability briefings," during which all personnel execute a "Classified Information Non-disclosure Agreement" and "FBI Rules of Behavior" form acknowledging their responsibility to protect and properly handle FBI information. SecD also provides a host of additional training opportunities and materials, each of which serves to reinforce security awareness throughout the FBI.

While this approach will not stop a trusted insider intent on disclosing information for improper purposes, it ensures the employee is educated on proper information handling techniques and encourages each employee to report others who violate the rules. In other words, FBI employees now better understand their role in protecting and ensuring the security of FBI information, personnel, and facilities.

f. What safeguards exist to prevent agents like Royer from similarly profiting on non-public information about ongoing investigations?

__Response__:

Please see our responses to subparts c and e, above.

USE OF GOVERNMENT-OWNED OR LEASED AIRCRAFT

36. I understand that the FBI operates a number of executive jets as part of its aviation program for both operational use and for official travel by senior FBI officials.

a. Please identify the number, type, and cost of aircraft owned and/or leased by the FBI and used for both operational purposes and travel by senior FBI officials.

__Response__:

The FBI reads this question as distinguishing between aircraft used to meet "mission requirements" of the FBI and those used for the "official travel" of "senior Federal officials" in the FBI other than to meet mission requirements, as those terms are defined in OMB Circular No. A-126.[1] While the vast majority of

---

[1] Paragraph 5 of OMB Circular No. A-126 (5/22/92) includes the following definitions:

b. **Mission requirements** means activities that constitute the discharge of an agency's official responsibilities. Such activities include, but are not limited to, the transport of troops and/or equipment, training, evacuation (including medical evacuation), intelligence and counter-narcotics activities, search and rescue, transportation of prisoners, use of defense attaché-controlled aircraft, aeronautical research and space and science applications, and other such activities. For purposes of this Circular, mission requirements do not include official travel to give speeches, to the FBI's flight capability is used for operational purposes (including criminal investigative purposes, counterterrorism, counterintelligence, and other operations), this distinction is important because senior FBI officials are often aboard FBI aircraft to conduct these mission requirements; to a far lesser extent these officials may use FBI aircraft for "required use" or other non-mission "official travel."

The FBI owns or leases 133 aircraft, including 3 that may be considered "executive jets." Two of these "executive jets" are leased by the FBI and are used for both mission requirements and other official travel by the AG, the FBI Director, and other senior Federal officials. The costs of these aircraft are as follows:

1. Gulfstream V aircraft – leased for $1.00 per year from the U.S. Air Force. The FBI pays the costs of fueling and maintaining this aircraft, which is $3,720.00 per flight hour.

2. Citation X aircraft – leased for $3.0 million per year from the Cessna Aircraft Corporation. The FBI pays the costs of fueling and maintaining this aircraft, which is $2,840.00 per flight hour.

The third is owned by the FBI, is configured with sensitive surveillance equipment, and is not used for executive transportation. This is a Citation Encore, which costs $1,497.00 per flight hour to fuel and maintain.

---

attend conferences or meetings, or to make routine site visits.

c. **Official travel** means (i) travel to meet mission requirements, (ii) required use travel, and (iii) other travel for the conduct of agency business.

d. **Required use** means use of a government aircraft for the travel of an Executive Agency officer or employee, where the use of the government aircraft is required because of bona fide communications or security needs of the agency or exceptional scheduling requirements.

b. Of the aircraft used for both purposes, please identify the number of flights and the percentage of total flight hours devoted to travel by senior FBI officials in the last four years?

Response:

In the last four years the FBI has flown a total of 52,408 flights for a total of 154,570.4 hours. Of these, 534 flights (2171.8 hours) were for non-mission official travel by senior Federal officials of the FBI, which is 1.4 percent of the total flight hours during this period.

c. On how many occasions in the last four years has the FBI used short-term leased aircraft operated by outside companies for particular trips by senior FBI officials rather than FBI-operated aircraft owned or under long-term lease? Please identify particular examples, explain the reasons for not using FBI-operated aircraft, and describe any additional costs associated with such arrangements.

Response:

The FBI maintains a full-time international aviation response posture in furtherance of the FBI's mission to conduct counterterrorism, counterintelligence, and other investigations, relying solely on its owned and leased aircraft except for one period in the past four years. From November 2005 through February 2006, the FBI's only aircraft capable of such international missions was required to undergo scheduled maintenance and receive a communications upgrade. Because it was anticipated that this maintenance would take 3 months, the FBI entered into a three-month contract with an "on-demand" aircraft charter company listed on the General Services Administration (GSA) schedule so it could continue to meet its international mission and official travel requirements. When it was determined that the maintenance would exceed 3 months, the FBI initiated a five-year Blanket Purchase Agreement (BPA). Five missions were conducted under the three-month contract, which expired on or about 2/2/06, and one 3-day mission in the continental United States (CONUS) and one 5-day mission outside CONUS were conducted for the FBI Director under the BPA.

COUNTERTERRORISM SUBJECT MATTER EXPERTISE

37. A low point in the history of the FBI had to have come when a former FBI Executive Assistant Director for Counterterrorism and Counterintelligence was unable to describe

the differences between Shiite and Sunni Muslims. In that moment, it became clear that some at the highest levels the FBI lack the subject matter expertise necessary to supervise effective counterterrorism investigations against the Muslim extremists who pose a threat to the lives of the American people.

a. What steps, if any, have been taken by the FBI to increase counterterrorism subject matter expertise in the ranks of the agency's supervisory personnel?

Response:

The FBI's Counterterrorism Division (CTD) has increased the subject matter expertise within the ranks of supervisory and executive personnel as well as within the investigative and professional support roles. Supervisors and executives in the field and at FBIHQ have received and will continue to receive training regarding the history, culture, technology, and roots of radical extremism, including training provided by the United States Military Academy's Combating Terrorism Center. These classes have included such topics as Muslim culture, analysis of the ideology behind the terrorist movement, Internet as Emirate, the strategy and logic of suicide bombers, radicalization, understanding terror networks, weapons of mass destruction (WMD), and geospatial mapping. In addition to these seminars are myriad "virtual" classes and Joint Terrorism Task Force (JTTF) training sessions offered throughout the country to all FBI employees. This training teaches us to interact better with Muslim communities and to build the trust critical to effective community policing.

The FBI has also begun implementation of the SA Career Path Program, which is a direct response to the 9/11 Commission recommendation for the FBI to establish a specialized and integrated national security workforce that is recruited, trained, rewarded, and retained to ensure the development of an institutional culture imbued with a deep expertise in intelligence and national security. Included in this initiative are plans to increase specialization within the SA workforce and to develop intelligence expertise in the management ranks.

CTD's current senior leaders have acquired subject matter familiarity through their daily work, their past interactions with Muslim communities during field assignments, and study in this area. These leaders are also knowledgeable regarding terrorists' operational methods and their criminal activities, neither of which depend on Islamic ideology. Because management and leadership qualities are as important as substantive expertise, it is also important that CTD managers come to their jobs with in-depth experience managing high-profile investigative and intelligence efforts.

b. Is counterterrorism subject matter expertise now a requirement for an FBI agent to assume a supervisory role over counterterrorism investigations? If not, why not?

__Response__:

Currently, competition for supervisory positions within the counterterrorism program is open to all qualified persons regardless of their program background. However, many applicants are experienced counterterrorism specialists who have served on multiple JTTFs throughout the FBI. Numerous JTTF supervisors who lead and manage these SAs and task forces have CTD or counterterrorism field experience and mentor the SAs who ultimately seek counterterrorism management positions. An extensive review of each applicant's supervisory and investigative abilities and accomplishments is completed prior to the selection process. If an individual does not have a background in counterterrorism and is selected for such a position, training is readily available to enhance the selectee's understanding of counterterrorism issues and complement their management qualifications.

c. Are there objective tests on FBI rules and procedures required before agents can be promoted to supervisory or senior management positions? If so, please describe the tests in detail. If not, please explain why not?

__Response__:

In the promotion of managers and executives, the FBI specifically chose to focus on those competencies that were determined through a comprehensive, empirical job analysis to be most predictive of successful performance in managerial and executive positions. In this job analysis, the knowledge of rules, policies, and procedures was not determined to be the primary factor in the ability to successfully perform the managerial and SES jobs at the FBI. Rather, those competencies that most strongly contribute to the success of a manager or executive are: leadership, interpersonal ability, liaison, planning and organizing, problem solving, flexibility, initiative and motivation, and communication.

A successful SA, supervisor, manager, or executive is able to apply multiple rules, policies, and procedures in various ways through the course of investigations and operations. Therefore, the FBI explicitly decided not to assess promotion potential based on an applicant's knowledge of rules, policies, and procedures. Rather, the FBI determined it was more practical to assess individuals for promotion based on the manner in which they had addressed certain work challenges, because the creative, innovative, and practical application of policies, rules, and procedures leads to success in all areas, including national security and criminal investigations as well as in leadership roles.

A practical and standardized assessment of the application of rules, policies, and procedures is found in the second phase of the promotion system, in which an applicant provides (in a standardized format) multiple behavioral examples to demonstrate the expertise determined by the hiring official to be germane to a specific position. The quality of an applicant's example is evaluated using a standardized metric to measure complexity, applicability, practicality, and the success of applying a particular technical knowledge, rule, policy, procedure, or technique.

d. Are there objective tests on relevant subject matter expertise before agents can be promoted to supervisory or senior management positions? If so, please describe the tests in detail. If not, please explain why not?

Response:

In its revision of the management promotion system, the FBI explored the possibility of using traditional assessments such as multiple-choice, essay, fill-in-the-blank tests to ascertain an applicant's subject matter expertise. We explicitly decided not to assess promotion potential on this basis for several reasons. First, as discussed above regarding objective tests regarding knowledge of rules and procedures, empirical job analysis indicated that subject matter expertise was not the competency most predictive of successful performance in managerial and executive positions. In addition, it would require substantial resources to track and test the rapidly evolving subject matter knowledge used in national security and criminal investigations under the FBI's purview. Given the high cost and limited benefit of such testing, as revealed by the empirical study discussed above, the FBI decided not to base promotions primarily on subject matter expertise.

As with knowledge of rules and procedures, discussed above, practical and standardized assessment of subject matter knowledge is found in the second phase of the promotion system, in which an applicant provides (in a standardized format) multiple behavioral examples to demonstrate the subject matter expertise determined by the hiring official to be germane to a specific position. The quality of an applicant's example is evaluated using a standardized metric to measure complexity, applicability, practicality, and the success of applying particular subject matter expertise. All those who apply for a particular position are compared with respect to managerial and technical (subject matter) competency, with higher weight ascribed to the managerial competencies.

The job analysis did show that, should the level of managerial/executive competency be equal, experience in a particular subject matter (such as counter-intelligence procedures, WMD, health care fraud, etc.) would predict success over a person who did not possess such subject matter expertise. Consequently, subject matter expertise becomes a significant factor in promotion decisions if management and leadership skills appear to be equal.

e. How does the FBI determine whether an FBI agent has the counterterrorism subject matter expertise necessary for him or her to supervise counterterrorism investigations?

<u>Response</u>:

Please see the response to subpart b, above.

FBI INVOLVEMENT IN THE LIN DeVECCHIO PROSECUTION

38. Former FBI Special Agent Lin Devecchio has been indicted on murder charges in the State of New York and is awaiting trial on those charges. An Internet website has been set up for his benefit at www.lindevecchio.com. The website includes a description of events at Devecchio's bond hearing, including a statement reporting that 47 former and active FBI agents attended the hearing as a sign of support for Devecchio.

a. Has the FBI conducted an investigation to identify the active agents who reportedly attended the Devecchio bond hearing and to determine whether those active agents might be subject to discipline for misusing their status as FBI agents? If so, describe the investigation in detail. If the investigation did not at least include efforts to conduct

interviews of the retired agents identified on the Devecchio website, please state why no effort was made to interview those retired agents.

Response:

No investigation has been initiated. The DOJ OIG received a letter from Angela Clemente and Associates (ACA), dated 5/22/06, alleging potential misconduct by unnamed current or former FBI agents who appeared to support Devecchio. In June 2006, the OIG asked ACA to provide additional information. In August 2006, after receiving no response from ACA, the OIG forwarded ACA's original letter to the FBI. Because the letter contained little detail and appeared to concern misconduct by former FBI SAs, the FBI's Internal Investigations Section (IIS) did not initiate an investigation. If information should be provided regarding misconduct by on-board FBI employees, IIS will reassess the need for investigation.

IIS typically does not initiate investigations relative to the actions of former FBI employees, as they are not subject to the same restrictions placed on on-board personnel. Although current FBI employees are subject to regulations restricting their use of public office for private gain and their use of their Government position, title, or authority to induce others to provide benefits, former FBI employees who are no longer in federal service are not subject to these restrictions. While a federal statute (18 U.S.C. § 709) prohibits the use of the FBI's name to convey the impression that the FBI endorses a publication or production, it does not, by its terms, prohibit former FBI employees from referring to their former FBI positions to "lend credibility" to their own beliefs about a former colleague or from attending events as a show of support.

b. Has the FBI issued any statements or written directives to agents advising them of the impropriety of misusing their status/authority as FBI agents to influence court proceedings against a former agent facing criminal charges? If so, please describe those statements or directives in detail.

Response:

Yes. Current FBI employees, including SAs, are subject to the regulations governing federal employees generally and to internal FBI regulations. Under government-wide regulations, employees are prohibited from using their Government positions, titles, or authorities to induce others to provide any benefit to the employee or to another person, or in a manner that could be construed as implying that the agency or another Government entity sanctions or endorses the employee's personal activities or those of another. (5 C.F.R. § 2635.702.) Internal FBI regulations specifically prohibit employees, except in an official capacity, from becoming involved "in any matter directly or indirectly concerning an employee or non-employee who has been arrested or is otherwise in difficulty with a law enforcement agency" or attempting "to mitigate the action of any arresting officer, agency, or prosecuting officer, or in any way try to minimize publicity concerning such incident." FBI Manual of Administrative Operations and Procedures, Part 1, Section 1-15.2.

In addition, when expressing personal views, employees are cautioned through the FBI's Prepublication Review Manual to make clear that they are stating their personal opinions, not those of the FBI, especially when they have been identified as FBI employees, or when discussing matters related to the functions of the FBI. These standards are discussed in the FBI directives and other materials available to all employees on the FBI's intranet and are also covered in ethics training sessions, which are required for each employee upon entry on duty and for managers on an annual basis. New SAs receive 18 hours of training in ethics, which stresses both the prohibitions on misuse of position and the need to avoid any appearance of impropriety. As noted above, however, former FBI employees who are no longer in federal service are not subject to these restrictions.

DOUBLE STANDARD OF DISCIPLINE

39. The general perception among FBI personnel has long been that there is a double standard of discipline at the agency, with FBI supervisors receiving preferential treatment during disciplinary proceedings. This perception of unfairness in the FBI has had a detrimental effect on the morale of the agency's employees and has diminished the agency's public credibility.

a. What percentage of FBI Agents are currently in supervisory positions?

<u>Response</u>:

Currently, of the 12,559 FBI SAs, 2,827 (or 22.5%) are in supervisory positions.

b. What percentage of the FBI agents who have received suspensions of more than three days since January 1, 2001, have been in supervisory positions at the time the suspensions were ordered?

<u>Response</u>:

From 1/1/01 through 12/31/06, the percentage of SSAs who received suspensions of more than three days was 19%. From 11/1/04 (the effective date of the FBI's Employee Offense Table and Penalty Guidelines, under which disciplinary sanctions are aggravated based on supervisory status) through 12/31/06, the percentage of disciplinary actions imposed on SSAs was 26%. During that same period, the average length of suspension, broken down by grade level, was:

Non-supervisory SAs: 11 days
GS-14 SSAs: 12 days
GS-15 SSAs: 17 days
SES SSAs: 25 days

c. What steps are being taken by the FBI to affirmatively ensure that FBI supervisors are not being given preferential treatment during disciplinary proceedings?

<u>Response</u>:

FBI supervisors are not given preferential treatment during disciplinary proceedings. The Assistant Director (AD) of the FBI's Office of Professional Responsibility (OPR) is a veteran DOJ attorney with more than 10 years of experience investigating employee misconduct cases in her former position as a senior attorney at DOJ/OPR, and more than 2 years of experience adjudicating employee misconduct cases in her current position as the AD of FBI/OPR. The AD reports directly to the Director and Deputy Director, and has complete independence and autonomy in deciding employee misconduct cases. OPR adjudicates its cases using the FBI's Offense Table and Penalty Guidelines, which make an employee's supervisory status an aggravating factor in determining the appropriate penalty. In OPR, a case undergoes multiple levels of review to ensure accuracy, consistency, and impartiality, including peer review and review by an OPR unit chief, the AD's special assistant (a former federal public corruption prosecutor), and the OPR AD.

40. Cecilia Woods is an FBI agent who reported an inappropriate relationship between her supervisor and a paid informant and who was thereafter targeted for a series of disciplinary proceedings that ultimately forced her into retirement. It is my understanding that her supervisor, on the other hand, was allowed to continue his employment with the FBI.

While conducting an inquiry into this matter, I requested a copy of the FBI's table of offenses and penalties for agent misconduct. I received that document on March 8, 2006. In reviewing the FBI's table of offenses and penalties, I discovered that the table does not require the termination of employment of FBI agents who engage in sexual conduct with paid confidential informants. In fact, the penalty provided by Section 1.4 of the table can be as little as a letter of censure.

a. Please explain why FBI guidelines do not require the mandatory termination of employment of all FBI agents who engage in sexual conduct with confidential informants. Shouldn't there be a zero tolerance policy for that sort of behavior?

Response:

The provision of the FBI's Offense Table and Penalty Guidelines to which you refer addresses improper employee-informant personal relationships of all types, not just sexual misconduct. While the FBI does not tolerate agents engaging in sexual misconduct with informants, this provision does not require dismissal in every case because: (1) this provision also addresses non-romantic, non-sexual social relationships that are nevertheless deemed improper; and (2) the varied factual settings of these cases, including sexual misconduct, do not lend themselves to a single penalty. For example, an agent could develop a sexual relationship with someone who is an informant but not know the individual is an informant. Provided the agent reports his or her relationship with the informant when this is discovered, OPR would weigh the circumstances to determine the appropriate response.

b. What is the total amount of money paid by the FBI to the confidential informant who engaged in an intimate relationship with Cecilia Woods' supervisor?

Response:

The FBI's OPR did not find that Cecilia Woods' supervisor had an intimate relationship with a confidential informant. Rather, OPR concluded that the supervisor made payments of nearly $10,000 to the informant for information of little or no value.

c. During the past five years, how many FBI agents have been fired for engaging in sexual conduct with confidential informants?

Response:

Since January 2001, one SA has been dismissed based on a finding of sexual misconduct with an informant and the commission of other disciplinary infractions. In separate cases, two other SAs who were charged with sexual misconduct with informants/witnesses resigned while under inquiry.

ALLEGATIONS OF MISCONDUCT BY FBI SUPERVISOR

41. On January 3, 2005, Agent Jennifer Smith-Love was promoted from the field to a position at FBI Headquarters. According to your answers to previous questions for the record, you approved this promotion while an investigation was still being conducted of her involvement in possible misconduct related to her handling of the investigation of the death of federal prosecutor Jonathan Luna.

a. At the time you approved the promotion of Smith-Love, did you know she would be cleared by FBI/OPR of any misconduct? If so, how did you know that? If not, then why approve the promotion while the investigation is still pending.

Response:

As is typically done before promotion to the SES, an administrative records check was conducted before Mrs. Love was promoted to the position of CTD Section Chief in January 2005. That check revealed that DOJ OIG and FBI OPR inquiries were then pending relating to the Luna investigation. The Director was aware of this and approved Mrs. Love's promotion.

Several months after her promotion to Section Chief, it was alleged that Mrs. Love made inconsistent statements during the administrative reviews of the Luna investigation. Ultimately, FBI OPR determined that the preponderance of evidence did not support a finding of any misconduct, including false statements or lack of candor.

b. The head of FBI/OPR told staff in a briefing earlier this year the mission of the office would not be impaired by providing the Committee access to its final report on this matter. Please provide a copy of the report or a detailed explanation of the basis on which it is being withheld.

Response:

Consistent with longstanding Executive Branch policy, DOJ's goal in all cases is to satisfy legitimate oversight interests while protecting significant Executive Branch confidentiality interests. As a general matter, the disclosure of OPR investigative files implicates significant individual privacy interests because these files discuss allegations against individuals under investigation. DOJ has consistently offered to accommodate Congressional requests for information about OPR investigations through briefings, minimizing the intrusion on the privacy of Executive Branch employees.

On 6/21/06 the FBI responded to the Committee's 5/10/06 request for information and documents relating to the FBI's investigation of the suspected murder of Assistant United States Attorney Jonathan Luna. In its response, the FBI advised the Committee that documents concerning OPR matters raise serious privacy considerations, particularly when, as in that instance, there was no finding of misconduct. Consistent with the policy articulated above, Candice Will, AD of the FBI's OPR, provided a 6/30/06 staff briefing that included an overview of OPR's investigation and addressed both the issues raised in the Committee's 5/10/06 letter and all issues raised by the staff. In response to a question from staff concerning the availability of the OPR report, our records reflect that AD Will did not indicate that she had no objection to producing the report, but rather advised that privacy concerns counseled against providing that document to the Committee.

FBI WHISTLEBLOWERS

42. In May, 2006, I asked the FBI for a description of each instance where an FBI supervisor has been disciplined for retaliating against a whistleblower. Two weeks ago, I

received a response from your agency advising me that since 1999 no FBI supervisors have been disciplined as a result of their having retaliated against whistleblowers.

a. Why haven't any FBI supervisors been disciplined for having retaliated against whistleblowers?

<u>**Response**</u>:

As the FBI has previously indicated in response to Questions for the Record, an Assistant Special Agent in Charge (ASAC) was disciplined for whistleblower retaliation. While that sanction, which was imposed before implementation of the Bell Colwell recommendations, was ultimately vacated on appeal, that case does not indicate that supervisors are not disciplined for retaliation, but instead indicates that the FBI has procedures in place designed to protect the rights of all employees. Since that response, no allegations of whistleblower retaliation have reached final adjudication.

b. The DOJ/IG found that Jorge Martinez retaliated against Michael German for protected whistle blowing activity. Has FBI disciplined Martinez? If not, why not?

<u>**Response**</u>:

The FBI is well aware of this matter and is in the process of taking appropriate action. Consistent with longstanding Executive Branch policy, our goal in all cases is to satisfy legitimate oversight interests while protecting significant Executive Branch confidentiality interests. As a general matter, the disclosure of information from OPR investigative files implicates significant individual privacy interests because these files discuss allegations against individuals under investigation.

c. Since 1999, how many FBI personnel have claimed whistleblower status? How many have claimed retaliation for protected whistleblowing activity?

<u>**Response**</u>:

The FBI is not in a position to provide this information. Pursuant to 5 U.S.C. § 2303 and 28 C.F.R. Part 27, DOJ's OIG and OPR serve as Investigative and/or Conducting Offices in FBI whistleblower cases, while the Director of DOJ's

Office of Attorney Recruitment and Management (OARM) is authorized to adjudicate claims of FBI whistleblower reprisal and to order corrective action subject to appeal to the Deputy Attorney General (DAG). Pursuant to 28 C.F.R.§ 27.4, the identity of employees who make those claims is not disclosed to the FBI unless there is a recommendation for corrective action.

DOJ's OARM advises that, based on numbers collectively reported by OARM, OIG, and OPR for calendar years 1999 through 2006, 96 FBI personnel have made allegations of retaliation for claimed protected whistleblowing activity. It is the FBI's understanding that there is no formalized consolidated record of those who may initially claim whistleblower status because, in the absence of subsequent retaliation based on the whistleblowing, the mere status as a whistleblower does not affect the employees' rights or benefits.

REPORTING OF DRUG SEIZURE STATISTICS

43. The staff of the House Committee on Homeland Security, Subcommittee on Investigations, recently released a staff report entitled, "A Line in the Sand: Confronting the Threat at the Southwest Border." This report describes, among other things, the results of efforts by various federal law enforcement agencies to improve our nation's security. The report indicates that several agencies of the federal government (including the FBI) were asked to provide information on the quantities of drugs that they had seized across the nation. The report states that those several agencies reported to Congress that during FY 2005 they had accomplished the total drug seizures listed in the following table:

FY2005 Federal Drug Seizures

Federal Agency	**Cocaine (in lbs)**	**Marijuana (in lbs)**	**Methamphetamine (in lbs)**
Border Patrol	12,000	1,200,000	728
ICE	345,031	1,036,241	3,501
Coast Guard	338,206	10,026	N/A
DEA	49,172	2,143,260	1,215
FBI	384,866	2,485,962	11,346
TOTAL	1,129,275	6,866,465	16,790

Source: U.S. Customs and Border Protection, U.S. Coast Guard, DEA and FBI

These statistics indicate that the FBI has seized far more drugs than any of the other major federal law enforcement agencies.

a. How did the FBI develop information on the statistical accomplishments set forth in the House report?

Response:

The above chart does not appear to have been taken from the House report referenced in the question. The statistics attributed to the FBI in the above chart were provided to Committee staff in response to an informal inquiry regarding total Federal drug seizures, rather than FBI drug seizures.

It appears that the House report used information obtained from the El Paso Intelligence Center (EPIC), which compiles statistics on drug seizures that meet a specific threshold reporting requirement, and does not represent all of the drug seizures conducted by a federal agency. In the table on page 3 of the House report, EPIC attributed the following drug seizure statistical accomplishments to the FBI for FY 2005:

Cocaine:	1,380 kg
Marijuana:	15,908 kg
Methamphetamine:	107 kg

The methods used by EPIC and the FBI to record drug seizures may differ in significant respects. For example, FBI drug seizure amounts that fall below the EPIC minimum threshold are not captured by EPIC, but they are recorded in the FBI's Automated Case Support (ACS) system using the Integrated Statistical Reporting and Analysis Application (ISRAA), which has no minimum threshold. Also, while both EPIC and the FBI generally record seized drugs by weight, the FBI records "live plants" seized or destroyed, as a special category, while EPIC does not. Other differences in statistical methodologies would create additional distinctions between agency statistics and those of EPIC or others.

For FY 2005, the FBI's drug seizure statistical accomplishments, as recorded in ISRAA, are:

Cocaine:	5,933 kg	13,053 lbs.
Marijuana:	9,200 kg	20,240 lbs. (+ 19,939 live plants)
Methamphetamine:	2,611 kg	5,744 lbs.

These figures indicate that the FBI engaged in a significant number of seizures of cocaine and methamphetamine that were below EPIC's threshold amount, resulting in higher FBI seizure amounts in ISRAA than in EPIC.

b. In the table above, the FBI is listed as being responsible for the seizure of 11,346 pounds of methamphetamine in FY2005. However, according to EPIC, the FBI obtained federal drug identification numbers for only 107 kilos (or 235.4 lbs) of methamphetamine. Please explain this discrepancy.

Response:

For FY 2005, the FBI seized a total of 2,611 kg or 5,744 lbs. of methamphetamine. Because of the nature of methamphetamine distribution, many of the seizures did not exceed the threshold (250 grams) required for reporting to EPIC. Seizures under the threshold, which are common in violent gang investigations, are not reported to EPIC.

c. Does the FBI report the agency's drug seizures to the El Paso Intelligence Center (EPIC) and obtain Federal Drug Identification Numbers (FDINs) for seizures meeting the threshold reporting requirements? If not, why not?

Response:

As discussed above, the FBI reports drug seizures meeting the threshold reporting requirements to EPIC for the assignment of an FDIN.

d. What steps are taken by the FBI to prevent double-counting or double-reporting of seizure statistics by law enforcement agencies?

Response:

The FBI compiles its drug seizure statistics using an "Accomplishment Report" (Form FD-515) to record information for the ACS system's ISRAA. Statistical accomplishments, such as seizures that disrupt or dismantle a drug organization, are reviewed and approved by FBIHQ for accuracy. For drug seizures that meet the threshold requirement, field offices are required to obtain an FDIN from EPIC for entry in Block N of the Accomplishment Form. Additionally, all statistical accomplishments must be associated with an FBI case file. These reporting procedures, which require provision of the name, title, agency, date and time, circumstances, and quantity and type of drug collected, prevent double-counting and double-reporting drug seizures.

e. What steps are taken by the FBI to ensure the veracity of statistical accomplishments provided to Congress?

Response:

The FBI takes its obligation to ensure the accuracy of all information provided to Congress and others, including statistical accomplishments, very seriously. Information requested by an appropriate authority is carefully compiled and analyzed by the FBIHQ substantive unit and thoroughly reviewed before dissemination.

Questions Posed by Senator Sessions

44. Entering Person Files Into the NCIC.

a. What are the minimum standards for entering a person file into the NCIC database?

Response:

The qualification standards for entry in NCIC depend on the NCIC file in which the name will be entered. For example, the criteria for entry into Immigration Violator Files (IVFs) are addressed in response to Question 45a, below. As another example, in order to be entered in the NCIC Wanted Person File related to federal warrants, the individual must be considered a "federal fugitive." Federal fugitives are individuals (including juveniles who will be tried as adults) for whom a federal warrant is outstanding and who:

- Are being sought because they have been charged with one or more federal crimes,
- Have failed to appear for a required court action or for deportation, or
- Have escaped from federal custody.

In addition to particular criteria for entry, minimum standards for entry require that agencies that enter records in the NCIC System be responsible for the accuracy, timeliness, and completeness of these records. To facilitate compliance with hit confirmation requirements, the originating agency must be available 24 hours a day to confirm its record entries. Stringent administrative procedures and controls ensuring the accuracy of data entered in computerized criminal justice information systems are important and can prevent the loss of court cases, false arrests, criminal charges against law enforcement officers, and civil liability suits.

These administrative controls include a requirement that the accuracy of a record be double checked by a second party at the time of initial entry. (For electronic records management systems, electronic cross-checks are acceptable.) Cross-checks must include a check of source documents to ensure accurate, complete, and up-to-date information is maintained.

Records also must be entered and maintained in a timely manner. NCIC records must be entered immediately when the conditions for entry are met. The only exceptions to immediate entry are when otherwise prescribed by federal law or when documentation exists to support delayed entry. After the decision to arrest or authorize arrest has been made, entry of records for Federal warrants must be accomplished within 24 hours of the receipt of information by the inputting agency/office. Appropriate maintenance, modification, and removal of IVFs must also be accomplished in a timely manner.

Complete records include all information available on the person or property at the time of entry. Validation should include a review of whether additional information missing from the original entry has become available for inclusion since that time. Validation also obliges the agency of record to confirm that the record is complete, accurate, and still outstanding or active. Validation is accomplished by reviewing the original entry and current supporting documents and by consultation with any appropriate complainant, victim, prosecutor, court, or other appropriate source or individual. This consultation includes communication with agencies that lack direct terminal access to NCIC (typically called "nonterminal agencies") and, consequently, rely on other agencies, such as dispatch centers, to enter and maintain their records. All NCIC records (except for Article Files, which record stolen property) must be validated 60 to 90 days after entry, and all person file records, including IVFs, are validated annually thereafter.

b. Please explain the process for setting these standards in full.

Response:

The NCIC System standards have been developed over the 40-year history of the system. When new requirements are imposed on the NCIC System (whether through legislation, Executive Orders, Departmental Directives, or user needs), standards are modified or expanded as necessary. These modifications and expansions are deliberated through the Criminal Justice Information Services (CJIS) Advisory Policy Board (APB) as described in response to subpart c, below.

c. Please explain the role, membership, and meeting schedule of the Advisory Policy Board and how this board makes decisions regarding the standards for data entry into NCIC.

Response:

The CJIS APB's role is to recommend general policy to the Director of the FBI with respect to the CJIS Division's philosophy, concept, and operating principles. The APB reviews and considers proposed rules, regulations, and procedures for the operation of CJIS Division systems and programs.

The CJIS APB is composed of 33 members. Twenty of the board members are representatives from law enforcement agencies (12 are from state-level agencies and 8 are from local agencies). Eight members are selected by professional criminal justice associations such as the International Association of Chiefs of Police and the National Sheriffs' Association. One board member represents Federal users of CJIS systems. The remaining four board members are selected by the Director and include representatives of a national security agency and the prosecutorial, correctional, and judicial sectors of the criminal justice community.

The APB meets twice yearly, usually in June and December unless budgetary or other considerations dictate otherwise.

Working Groups usually deliberate first about issues concerning the operation of the NCIC system. Working Groups consist of representatives from local and state law enforcement agencies from each of the 50 states as well as representatives of federal agencies that use the NCIC system. These issues are then discussed by the APB's NCIC Subcommittee, which is composed of APB members and other subject matter specialists who study and review these issues to assist the APB with its deliberations. The Working Groups and the NCIC Subcommittee formulate recommendations concerning the issue and those recommendations are forwarded to the APB for its consideration. The APB then recommends a course of action to the FBI Director. The Board's role is strictly advisory; the FBI Director makes the final decision regarding NCIC data entry standards.

45. Process for Entering Immigration Violator Files Into the NCIC.

a. What are the categories of immigration violators that can be entered into the NCIC?

Response:

The following categories of immigration violators can be entered into NCIC.

Deported Felons: The Deported Felon Category contains records of previously deported felons who have been convicted and deported for drug trafficking, firearms trafficking, or serious violent crimes.

Absconders: The Absconder Category contains records of individuals with outstanding administrative warrants of removal from the United States who have unlawfully remained in the United States.

National Security Entry-Exit Registration System (NSEERS): The NSEERS Category contains records of individuals with outstanding administrative warrants for failure to comply with national security registration requirements.

b. Are you considering adding any new immigration violator categories into the NCIC?

Response:

Not at this time.

c. Because the FBI oversees the NCIC, please explain the process for deciding which immigration violator files are entered into the NCIC and which are not.

Response:

After the events of 9/11/01, there were several initiatives to require DHS's Immigration and Customs Enforcement (ICE) to place into NCIC the names and biographical data of those in violation of their immigration status, including administrative cases. The entry of administrative cases into NCIC caused concern in the law enforcement community, and several jurisdictions debated their authority to detain individuals under state law solely for immigration violations. Based on this concern, and keeping in mind that ICE would continue to enter into the NCIC Wanted Person File records of criminal aliens with federal warrants, the FBI's CJIS Division presented options for consideration through the APB process.

During the fall of 2002, the APB recommended that records of criminal aliens with federal warrants continue to be entered into NCIC but that the Deported Felon File be restructured and included in the IVF. Based on this recommendation, the IVF was implemented in August 2003. Administrative immigration information is entered into NCIC pursuant to 28 U.S.C. § 534, 28 C.F.R. Part 20, Subpart C, and policy recommended by the CJIS APB. ICE's Law Enforcement Support Center (LESC) is the only agency authorized to enter, modify, validate, or delete records in the IVF, and LESC is responsible for the institution of procedures for entering and maintaining these records.

The NCIC operates under a shared-management concept in which the FBI and Federal, state, local, and tribal criminal justice agencies participate. The FBI maintains the host computer and provides a telecommunication network accessed by the CJIS Systems Agencies (CSAs) in each of the 50 states, the District of Columbia, Puerto Rico, the U.S. Virgin Islands, Guam, and Canada, as well as by other Federal criminal justice agencies. The CSAs provide the networks by which local and regional agencies access NCIC. When an agency enters a record in NCIC, that agency must comply with NCIC policies and is responsible maintenance of the record.

d. What keeps each and every immigration violator file from being entered into the NCIC?

Response:

The only records that may be entered in an NCIC file are those that satisfy the criteria for inclusion in that file. The criteria for the IVF are set out in the response to subpart a, above. Beyond that, for the reasons indicated in subpart c, above, we defer to DHS with respect to how they determine which records satisfy these criteria and how they prioritize their entry.

e. Please explain the phrase "lack of identifying information."

<u>**Response**</u>:

"Lack of identifying information" indicates that some of the mandatory data elements are not available. The following data elements are required for entry of a person's record in the IVF: name, sex, race, height, weight, hair color, IVF category, case number, and at least one of the following numeric identifiers: date of birth (including year, month, and day); FBI number; social security number; military serial number; alien registration number; Canadian social insurance number; mariner's document or identification number; passport number; state-issued personal identification number; port security card number; Selective Service number; Veterans Administration claim number; driver's license number (with state and year of expiration); license plate number (with state, year of expiration, and type); vehicle identification number (with model year, make, and style).

f. Is this "lack of identifying information" an issue in entering immigration files into the NCIC?

<u>**Response**</u>:

We defer to DHS for response to this question for the reasons indicated in subpart c, above.

g. How many employees at the DHS Law Enforcement Support Center in Vermont are assigned to NCIC activities?

<u>**Response**</u>:

We defer to DHS for response to this question.

46. Immigration Violator File Subfiles. The "Immigration Violators" file is divided into subfiles for the three types of immigration violators: deported felons, alien absconders, aliens with outstanding ICE criminal warrants, and NSEERS violators.

a. How many total entries are currently in the "Immigration Violators File" in the NCIC? ***(In your testimony before the Senate Judiciary Committee on December 6, 2006, you stated that approximately 107,000 alien absconders had been entered into NCIC).***

Response:

As of 1/9/07, there were 240,836 records in the IVF. Please note that records for aliens with outstanding ICE criminal warrants are included in the NCIC Wanted Person File.

b. How many of the IVF entries are deported felons?

Response:

123,612 of the IVF entries represent deported felon records.

c. How many deported felon entries are pending (waiting to be entered into the NCIC)?

Response:

We defer to DHS for response to this question for the reasons indicated in Question 45c, above.

d. What is the current total number of deported felons?

Response:

We defer to DHS for response to this question.

e. How many of the IVF entries are alien absconders?

Response:

117,224 of the IVF entries represent alien absconder records.

f. How many alien absconder entries are pending (waiting to be entered into the NCIC)?

Response:

We defer to DHS for response to this question for the reasons indicated in Question 45c, above.

g. What is the current total number of alien absconders in the United States?

Response:

We defer to DHS for response to this question.

h. How many alien absconder files exist that are not pending (waiting to be entered into the NCIC)?

Response:

We defer to DHS for response to this question for the reasons indicated in Question 45c, above.

i. What is the current rate per day of entering alien absconders into NCIC?

Response:

During December 2006, ICE averaged 205 alien absconder record entries per day.

j. Please outline each step in the process of entering the name of an alien absconder into NCIC.

Response:

We defer to DHS for response to this question for the reasons indicated in Question 45c, above.

k. How many of the IVF entries are aliens with outstanding ICE criminal warrants?

Response:

As of 1/9/07, there were 1,875 records for outstanding ICE criminal warrants in the NCIC Wanted Person File.

l. How many aliens with outstanding ICE criminal warrants entries are pending?

Response:

We defer to DHS for response to this question for the reasons indicated in Question 45c, above.

m. What is the current total number of aliens with outstanding ICE criminal warrants in the United States?

Response:

We defer to DHS for response to this question.

47. Process for Entering Alien Absconder Files into NCIC.

a. Because the FBI oversees the NCIC, please explain the process for deciding which alien absconder files are entered into the NCIC and which are not.

Response:

We defer to DHS for response to this question for the reasons indicated in Question 45c, above.

b. What keeps each and every alien absconder file from being entered into the NCIC?

Response:

We defer to DHS for response to this question for the reasons indicated in Question 45c, above.

48. Process for Entering Aliens with Outstanding Criminal Warrants into NCIC.

a. Because the FBI oversees the NCIC, please explain the process for deciding which aliens with outstanding criminal warrants files are entered into the NCIC and which are not.

Response:

We defer to DHS for response to this question for the reasons indicated in Question 45c, above.

b. What keeps each and every alien with outstanding criminal warrant file from being entered into the NCIC?

Response:

We defer to DHS for response to this question for the reasons indicated in Question 45c, above.

49. Process for Entering Deported Felon Files into NCIC.

a. Because the FBI oversees the NCIC, please explain the process for deciding which deported felon files are entered into NCIC and which are not.

Response:

We defer to DHS for response to this question for the reasons indicated in Question 45c, above.

b. What keeps each and every deported felon file from being entered into NCIC?

Response:

We defer to DHS for response to this question for the reasons indicated in Question 45c, above.

c. Is this "lack of identifying information" an issue in entering alien with outstanding criminal warrant into the NCIC?

Response:

We defer to DHS for response to this question for the reasons indicated in Question 45c, above.

<u>Questions Posed by Senator Leahy</u>

IRAQ STUDY GROUP RECOMMENDATIONS

50. In its recent report about the situation in Iraq, the bipartisan Iraq Study Group found that the Iraqi Police Service ("IPS") is in dire straits. In particular, the report states (on pages 9-10):

> **The state of the Iraqi police is substantially worse than that of the Iraqi Army. The Iraqi Police Service currently numbers roughly 135,000 and is responsible for local policing. It has neither the training nor legal authority to conduct criminal investigations, nor the firepower to take on organized crime, insurgents, or militias.... Iraqi police cannot control crime, and they routinely engage in sectarian violence, including the unnecessary detention, torture, and targeted execution of Sunni Arab civilians. ... There are ample reports of Iraqi police officers participating in training in order to obtain a weapon, uniform, and ammunition for use in sectarian violence. Some are on the payroll but don't show up for work. In the words of a senior American general, "2006 was supposed to be 'the year of the police'" but it hasn't materialized that way.**
>
> **In recommendation #54 of the report, the Iraq Study Group advocates having the Justice Department direct the training mission of the IPS forces that remain within the Iraq Ministry of the Interior.**

a. Please state whether you agree with this recommendation and explain your response.

b. What role has the FBI had in the training of the Iraqi police, thus far?

c. What additional steps will the FBI take to train the IPS in light of the Iraq Study Group's report and in particular, this recommendation?

Response to subparts a-c:

In January 2004, FBI Executive Assistant Director (EAD) Charles Prouty and Training Division (TD) Unit Chief Judson Ray traveled to Iraq as part of a Department of State (DOS) led training needs assessment team. Pursuant to the findings and recommendations of this team, the FBI agreed to provide training in the areas of organized crime, counterterrorism, kidnapping, intelligence analysis, establishment of a fingerprinting system in Iraq, and training on recruitment, selection, evaluation, and assessment of potential Iraqi Police Service (IPS) personnel. The FBI entered into an interagency agreement with DOJ and the DOS Bureau for International Narcotics and Law Enforcement Affairs. This interagency agreement was the basis for the Iraqi Training Initiative (ITI), which was established in coordination with Iraq's Ministry of Interior (MOI) and the Civilian Police Assistance Training Team (CPATT) to provide training assistance to the IPS. (The current CPATT was not established until May 2004 under the Multinational Force-Iraq. Prior to that, all police training was provided in support of the Coalition Provisional Authority.)

Following the needs assessment, the TD's International Training and Assistance Unit attended weekly meetings chaired by the National Security Council. Representatives from the DoD, DOS, and the FBI's Baghdad Legal Attaché (Legat) participated in these meetings. Training began in June 2004 and, to date, 653 students have graduated.

From 2004 to 2006, the following courses were conducted:

- Intelligence (one-week course)
- Kidnaping/Hostage Negotiation (one-week course)
- Counterterrorism (six week course)
- Iraqi -U.S. Major Crimes Task Force (six-week course)

51. In recommendation #57, the Iraq Study Group recommends that the practice of embedding U.S. police trainers with Iraqi police units be expanded and that the number of civilian officers training Iraqi police be increased.

a. Please state whether you agree with this recommendation and explain your response.

Response:

By letter of January 16, 2007, the Department of Justice advised that its International Criminal Investigative Training and Assistance Program ("ICITAP") has deployed senior law enforcement advisors to oversee teams of approximately 250 police trainers and 80 trainers for the Iraqi Correctional System, and that the Department's law enforcement components have provided support to the Department of Defense-led police training program in Iraq. The size and functional scope of such police training efforts are determined in full coordination with the Department of State and the Department of Defense, in furtherance of Presidential guidance.

b. Are there currently any FBI agents embedded with the Iraqi Police Service? If so, how many?

Response:

The FBI does not have, and has not had, SAs embedded with the IPS.

c. Will the FBI provide additional police trainers to participate in the training of the Iraqi Police Service and, if so, how many?

Response:

The FBI's TD is currently developing and conducting training for FY 2007, as discussed further in response to Question 52d, below. These courses of instruction will require the deployment of approximately 6 FBI SAs.

52. In recommendation # 58, the Iraq Study Group further recommends that the FBI expand its investigative and forensic training and facilities in Iraq, to address both terrorism and criminal activity.

a. Please state whether you agree with this recommendation and explain your response.

<u>Response</u>:

The FBI agrees that investigative and forensic training and facilities in Iraq would be beneficial. While the FBI's Laboratory Division (LD) does not anticipate the provision of forensic training in the near future due to concerns regarding the resources required (in terms of both people and equipment) and the safety and security of the non-agents who would provide on-site training, the LD does currently provide forensic training in the U.S. that can be made available to Iraqi forensic scientists. Training by the FBI's TD was suspended due to security concerns but is expected to resume by the late spring of 2007. This training will be provided in support of CPATT and coordinated through the U.S. Mission. The TD conducted a Major Crimes Task Force Course in Iraq during December 2005 - January 2006, and will deliver training in 2007 in: Intelligence, Kidnapping/Hostage Negotiations, Money Laundering/Terrorist Financing Investigations, Law Enforcement Training for Safety and Survival, and Basic Crime Scene/Post Blast Investigations.

b. How many FBI agents and personnel are currently providing investigative and forensic training in Iraq?

<u>Response</u>:

The FBI is not currently providing investigative or forensic training in Iraq because training was suspended to address security concerns. As indicated in the response to subpart a, above, the FBI's TD intends to resume training in the late spring of 2007. While the FBI's Major Case Task Force provides ongoing mentoring and informal situational training, it is not currently providing any classroom instruction or other formal training.

c. How many FBI agents and personnel are currently assisting with counterterrorism activities in Iraq?

<u>Response</u>:

On average, there are typically 55 to 60 FBI employees, including both SAs and support personnel, working on counterterrorism matters in Iraq. In addition, an average of 10 other U.S. Federal law enforcement officers typically join in this effort, including representatives from Immigration and Customs Enforcement, the

U.S. Marshals Service, the DEA, and the Bureau of Alcohol, Tobacco, Firearms, and Explosives.

d. Will the FBI expand its role in these programs as the Iraq Study Group recommends and, if so, what additional resources, including staff, equipment and funding, will be dedicated to that effort?

Response:

The FBI and CPATT have proposed the following training agenda for FY 2007.

- Iraqi-U.S. Major Crimes Task Force Directorate - Delivers investigative methodologies and techniques on post-blast crime scene investigations, kidnapping/hostage negotiations, law enforcement training for safety and survival, and organized crime and counterterrorism.

- Kidnaping/Hostage Negotiations Directorate - Course focuses on sophisticated investigative techniques, hostage negotiation practices, evidence collection, case management, intelligence fusion, and case studies of subject behavior patterns. This course also provides basic negotiating skills and explores the various psychological factors involved with the hostage taker, the hostage, and police authorities.

- Money Laundering/Terrorist Financing Investigation Directorate - This course provides a fundamentally sound base of knowledge, skill sets, tactics, techniques and investigative modalities necessary to confront and neutralize criminal operations funding terrorism. Practical problems are used throughout the course.

- MOI National Command Center (NCC) Assessment and Training Course Design - A Critical Incident Response Group command post expert assesses Iraqi NCC structure and functions, to include command center systems, communications networks, staffing, and crisis management methodologies and will formulate recommendations. In addition, the Iraq Provisional Joint Command Center Directors and Operations Chiefs will be trained in conventional command center operations, protocols, and practices.

- <u>Intelligence Directorate</u> - Provides instruction in the collection, collation, analysis, and dissemination of strategic and tactical intelligence used to investigate terrorist and criminal activities. Collection topics include open source, private, government, and human sources as specifically related to criminal activities. Emphasis also on the use of analytical tools to enhance strategic analysis and planning.

53. Public corruption is a significant problem in Iraq. According to the Iraq Study Group's report, one senior Iraqi official estimated that official corruption cost the Iraqi Government between $5 and $7 billion per year. To address the rampant corruption in Iraq, the Iraq Study Group concludes that Justice Department programs to create institutions and practices to fight public corruption in Iraq "must be strongly supported and funded."

a. What resources, including staff, equipment and funding, does the FBI currently have dedicated to helping to fight public corruption in Iraq?

<u>Response</u>:

There are no FBI resources specifically designated to help the Iraqi government fight corruption among Iraqi officials. The FBI's Legat office in Baghdad provides law enforcement cooperation assistance similar to the support provided by other FBI Legats in their host countries. The FBI is seeking to expand its foreign corruption training program to include countries in greatest need of this kind of assistance. If resources permit, the FBI anticipates that both Iraq and Afghanistan will be among the first countries to receive this training. In Iraq, this training will be coordinated with the programs already under way, with the support of such programs as the International Criminal Investigative Training Assistance Program.

b. Will the FBI increase the resources that it currently has in Iraq to further assist the Iraqi government in fighting public corruption?

<u>Response</u>:

Our recognition of the sovereignty of the Iraqi government prevents the FBI from directly combating corruption among Iraqi government officials. The FBI does, however, take an aggressive approach to fighting corruption tied to United States Government funding initiatives in Iraq, which may offer the Iraqi government a strong model to follow and aid in identifying criminal elements that may also be involved in internal government corruption. In addition to the aforementioned foreign corruption training initiative, the FBI has partnered with U.S. Army Criminal Investigation Command, the Special Inspector General for Iraq Reconstruction, the Defense Criminal Investigative Service, and DOS, among others, to participate in the International Contract Corruption Task Force (ICCTF) and the DOJ National Procurement Fraud Task Force to actively investigating U.S. officials, private citizens, and business entities involved in public corruption and governmental fraud in Iraq. Temporary Duty (TDY) rotational assignments of FBI SAs to Baghdad will begin early in 2007, an Assistant Legal Attaché (ALAT) wholly dedicated to public corruption and governmental fraud matters will be posted in Iraq later in 2007, and FBIHQ has assigned two FBI SA ICCTF program managers and several IAs to these matters. A number of FBI field offices are conducting Iraq-related public corruption investigations supported by the ICCTF, and all 56 field offices are available to support these and related investigations. As the FBI continues to increase its resources within and outside the U.S. in support of the ICCTF, liaison with our Iraqi counterparts in mutual support of these investigations will also increase. Any FBI programs to assist the Iraqis in combating public corruption will be undertaken in full coordination with existing programs and with the programs described in the President's 2007 Supplemental Appropriations Request.

DATAMINING/ATS AND IDW

54. At the hearing, I asked you about the Department of Homeland Security's Automated Targeting System ("ATS") and recent revelations that, since 9/11, the Bush Administration has been using this program to secretly assign terror scores to millions of law-abiding Americans who travel across our borders. You were not prepared to answer my questions about ATS at the hearing; however, you stated that you would look into this matter. Please respond to the following questions:

a. During an unclassified briefing for Judiciary Committee staff, the Department of Homeland Security said that it shares the sensitive personal information in the ATS database with the FBI and checks the information in this database against the Terrorist Watchlist. Does the FBI receive the terror scores or assessments and the other information contained in the ATS database? Please describe the information that the FBI receives from ATS and explain how the Bureau uses this information.

Response:

The FBI's TSC maintains the consolidated terrorist watchlist, but it does not receive Automated Targeting System (ATS) passenger risk assessments from DHS. TSC also does not place individuals on the terrorist watchlist based on ATS risk assessments. Instead, ATS checks air passenger data against the terrorist watchlist data provided to DHS by TSC, and DHS then contacts TSC if there appears to be a match between a passenger on an inbound flight and an identity on the watchlist, passing that passenger's identifying information and flight information to TSC so a final identity match determination can be made by TSC. ATS risk assessments do not result in calls to the TSC unless the individual is a possible match to the terrorist watchlist. If TSC determines the passenger is, in fact, the person on the watchlist, TSC will notify the FBI's Terrorist Screening Operations Unit, a unit within the FBI's CTD, which will determine what operational response is appropriate.

In a TSC database called the Encounter Management Application (EMA), TSC retains records of all such contacts from DHS and from other agencies that perform terrorist watchlist screening. The EMA record includes the identifying information regarding the individual being screened (the airline passenger) and TSC's determination of whether the person is a positive match to the watchlist. EMA records of positive matches are used to produce TSC's daily report, which is distributed to the Federal law enforcement and intelligence communities. EMA records of "negative matches," which usually concern individuals whose names are the same as or similar to watchlist identities, are used by TSC to help ensure that future encounters with those same individuals are quickly and properly resolved as negative matches in order to minimize the adverse impact on those innocent persons in the future.

b. Does the FBI use the information that it receives from ATS to assist it in investigating traditional criminal cases as well as counterterrorism matters?

Response:

No. Within the FBI, ATS information is available only to the TSC and only for counterterrorism purposes. While individuals assigned to the TSC may have access to ATS and may include this information during the identification or post-encounter process, ATS does not directly feed information into the TSDB, TSC's EMA, Investigative Data Warehouse (IDW), or any other FBI system. The risk assessment scores generated by ATS are not reviewed by the TSC or used in any TSC processes.

c. What safeguards are in place at the FBI to ensure the accuracy of this information and to protect the privacy interests of the millions of law-abiding Americans whose sensitive personal data is contained in ATS?

Response:

As discussed above, TSC does not receive all passenger data in ATS, but only data regarding passengers who are determined by DHS to be possible matches to identities on the terrorist watchlist.

TSC relies upon existing DHS privacy and data security/integrity processes to ensure the accuracy of the passenger data DHS sends to TSC. TSC does not have contact with the airlines or with individual passengers to permit us to verify the passenger manifest data supplied by the carriers to DHS's Customs and Border Protection (CBP). Once the passenger arrives at the border, he or she will present a passport and/or other identity documents to DHS's CBP officers, who will verify identity data at that time using the Treasury Enforcement Communications System. Any errors in identity data that were passed by the airline should have been detected by DHS and corrected at that time or, if discovered by CBP during inspection, passed by CBP to TSC for an update of all appropriate records.

TSC has in place a robust privacy compliance program, led by a full-time privacy officer, to ensure that the personal information TSC maintains is protected by strong privacy and security policies and practices. TSC would be pleased to brief the Committee in order to provide more detailed information about its privacy compliance program upon request.

55. You also testified that you would check into whether the FBI's own Investigative Data Warehouse database ("IDW") – which now contains more than 560 million FBI and other agency documents – shares information or data with ATS. Does the IDW database share information or otherwise interface with the ATS data-mining program?

Response:

The IDW system does not have interface with DHS's ATS. The IDW project does not have a listing of the ATS data sources and we cannot determine what, if any, information the two systems have in common.

56. You further testified that the FBI has issued a privacy impact statement for IDW.

a. Has the Bureau publicly released this privacy impact statement for IDW and, if not when will the FBI do so?

Response:

As a national security system, the IDW is exempt from the privacy impact assessment (PIA) requirement of section 208 of the E-Government Act. Even though the IDW was not required to be assessed under Section 208 of the E-Government Act, the FBI nevertheless examined the privacy issues presented by the development of this system and is satisfied that the system adequately protects privacy. The FBI has, however, determined that, consistent with the balance struck by Congress when it enacted the E-Government Act, the harm to the Bureau's national security mission outweighs the need to provide public awareness of the precise details of the technological tools the FBI employs in fighting terrorism. Therefore, we have decided not to make the PIA available to the public. The PIA was, however, provided to DOJ's Privacy and Civil Liberties Officer.

b. Has the FBI filed a notice in the Federal Register regarding the IDW program? If not, why not, and when will the Bureau do so?

Response:

As noted above, the PIAs for IDW have not been made publicly available.

The IDW system is covered by the FBI's Central Records System (CRS) Privacy Act system notice. The CRS notice was last published in full in the Federal Register at 63 Federal Register 8659, 8671 (2/20/98).

57. What policies are in place to ensure the accuracy and security of the sensitive personal data contained in the IDW database?

Response:

The IDW system contains copies of data from source systems maintained by the FBI and other government agencies. The accuracy of the data is ensured by the source system data governance processes and procedures. IDW services and functions are used to perform code-based or tool-based verification that data sent to or received by IDW are in compliance with established and documented form requirements (e.g., file structure, file type, number of fields, field formats, and value ranges). Daily tests are conducted to determine if data ingestion and data extraction/transformation/loading processes have been successfully completed. Users are provided with contact numbers on IDW web pages for use in the event that anomalous data or results are encountered. Anomalies are tracked either as problems or as security events.

IDW has an approved PIA, has completed the FBI Certification and Accreditation process, and has obtained an Authorization to Operate. IDW has dedicated system security administrators and an Information System Security Officer whose responsibilities are to monitor system security; verify that secure system operations and operating practices are maintained; document, respond to, and record security incidents; and document remedial actions.

DETAINEE TREATMENT

58. Last year's Detainee Treatment Act and this year's Military Commissions Act both set standards for what types of interrogation techniques are and are not permissible. In each case, though, the standards are general and open to interpretation.

a. Did the Office of Legal Counsel or any other legal office at the Justice Department or the FBI provide guidance to the FBI regarding how to interpret the provisions of the Detainee Treatment Act governing what interrogation practices are permissible?

b. What form did this guidance take? Did it dictate what specific interrogation techniques can and cannot be used?

c. What was the substance of this legal guidance? Will you share this document with the Committee?

Response to subparts a-c:

The FBI's policy relative to interrogation of detainees at Guantanamo has always been that the only techniques that are permissible are those that would be permitted in the United States with criminal suspects. That policy was documented in a 5/19/04 communication signed by the FBI's General Counsel and Deputy Director. In order to ensure that all FBI interrogators are aware of FBI policy, FBI interviewers at Guantanamo are provided a block of legal instruction (two to three hours) upon their arrival reminding them of the rules that govern the interrogation of detained individuals. In addition, an Assistant General Counsel from the FBI's Office of the General Counsel (OGC) has maintained a full-time presence at Guantanamo since April 2004.

Because FBI policy relative to the treatment of detainees is more limited than that permitted by the Detainee Treatment Act and the Military Commissions Act, the provisions of those Acts have not been a significant training issue for the FBI. We have, however, included limited information concerning those Acts in the legal instruction provided to FBI personnel upon their arrival at Guantanamo. Specifically, the instruction now includes information on the Military Commission Act of 2006 and on the Detainee Treatment Act of 2005.

The instruction on the Military Commission Act addresses the establishment of military commissions under that legislation and the rules of evidence applicable to military commission proceedings. The instruction on the Detainee Treatment Act addresses the prohibition on cruel, inhuman, or degrading treatment of persons under the custody or control of the U.S. Government; the procedures for Combatant Status Review Tribunals and Administrative Review Boards; and the fact that no court has jurisdiction to hear or consider writs of habeas corpus filed by or on behalf of aliens detained at Guantanamo.

The document in which policy and advice was conveyed to agents deployed to Guantanamo is attached as Enclosure B.

59. Has the Office of Legal Counsel or any other legal office at the Justice Department or the FBI provided guidance to the FBI regarding how to interpret the provisions of the newly passed Military Commissions Act governing what interrogation practices are permissible?

a. If so, what is that guidance? Please provide a copy of any legal guidance provided to the FBI regarding the Military Commissions Act.

b. If not, please explain how your agents know what is permitted or prohibited by the broad language of the Military Commissions Act without legal guidance. Do you expect to receive legal guidance in the future?

<u>Response to subparts a and b</u>:

Please see the response to question 58, above.

60. An FBI Supervisory Special Agent at Guantanamo Bay wrote a memo in November 2002 entitled "Legal Analysis of Interrogation Techniques," in which he or she concluded that rendering terrorism suspects to "Jordan, Egypt, or another third country to allow those countries to employ interrogation techniques that will enable them to obtain the requisite information" would violate 18 U.S.C. §2340 (the torture statute). Specifically, the memo states:

> **In as much as the intent of this category is to utilize, outside the U.S., interrogation techniques which would violate 18 U.S.C. §2340 if committed in the U.S., it is a per se violation of the U.S. Torture Statute. Discussing any plan which includes this category, could be seen as a conspiracy to violate 18 U.S.C. §2340. Any person who takes any action in furtherance of implementing such a plan, would inculpate all persons who were involved in creating this plan. This technique can not be utilized without violating U.S. Federal law.**
>
> **Legal Analysis of Interrogation Techniques (available online at http://www.humanrightsfirst.org/us_law/etn/pdf/fbi-brief-inter-analysis-112702.pdf).**

a. Do you agree that the "technique" of rendering suspects to third countries in order to allow those countries to use coercive interrogation techniques that violate U.S. law "cannot be utilized without violating U.S. Federal law"?

b. Does the legal analysis contained in the November 2002 memo reflect the FBI's current thinking with respect to rendition and other interrogation techniques? If not, how does the FBI's current analysis differ from the analysis in the memo?

__Response to subparts a and b__:

It is our understanding that the referenced 2002 memorandum was drafted by a military officer and was cut and pasted into a document transmitted by an FBI Supervisory Special Agent at Guantanamo. It was not a product of the FBI's Office of General Counsel. FBI policy on the treatment of detainees limits our agents to techniques that would be permissible to use with criminal suspects in the United States. It would not be permissible under FBI policy for an FBI agent to threaten to remove a criminal suspect to a third country to be mistreated.

61. You testified that the FBI is not investigating any of the allegations that have been made by German national Khalid El-Masri and others regarding possible violations of U.S. law in connection with the rendering of individuals to foreign countries. Why isn't the FBI investigating these allegations?

__Response__:

In circumstances such as this, where there has been no direct report to the FBI of allegations of violation of U.S. law, but where such information is made known to the U.S. government through a public forum such as a news report, those allegations are typically examined in the first instance by the OIG of the agency that employs the officer or employee about whom the allegation was made. If the employing agency determines that there is a reasonable basis to believe that El-Masri's allegations constitute a possible violation of federal criminal law, then the employing agency is required to refer those allegations to the FBI and the AG pursuant to a Memorandum of Understanding (MOU) for Reporting of Information Concerning Federal Crimes between several members of the IC that has been in effect since August 1995. If the FBI receives a referral in this case, it will conduct whatever investigation is appropriate.

BRANDON MAYFIELD

62. In December, the government agreed to pay $2 million to settle a case that had been brought by Oregon lawyer Brandon Mayfield. Mr. Mayfield was jailed for two weeks in 2004 as a material witness, in connection with the Madrid train bombing. As part of the settlement, the government made a formal apology to Mr. Mayfield and his family for the suffering caused by his mistaken arrest. Mr. Mayfield was arrested and held for two weeks on a material witness warrant. Under the material witness law, the government is authorized to arrest a witness to secure his testimony in a criminal proceeding. After the

9/11 attacks, the Justice Department began using the material witness law <u>not</u> to secure testimony from possible witnesses, but rather to lock up possible suspects in counter-terrorism investigations without charge until there is enough evidence to indict. Is it accurate to say that this is what happened in the Mayfield case?

<u>Response</u>:

The decision to arrest Mr. Mayfield on a material witness warrant on 5/6/04 was made to secure his testimony and was based upon probable cause to believe that Mr. Mayfield had testimony material to the investigation of the 3/11/04 Madrid train bombings (primarily because his fingerprint was matched, albeit erroneously, to evidence found in Madrid and connected to the bombing) and that it may become impracticable to secure his testimony by subpoena. In the days leading up to the decision to seek the material witness warrant, media reporting on the investigation was believed to be imminent, and there was significant concern about the risk of flight by Mr. Mayfield once the story broke. On Friday, 5/7/04, the day after his arrest, U.S. District Court Judge Robert E. Jones advised Mr. Mayfield that his deposition could begin at 1:30 p.m. that day, Mr. Mayfield could be released for the weekend with electronic monitoring, and the deposition could resume on the morning of 5/10/04. Mr. Mayfield declined to be deposed on that date and, as a result, he remained incarcerated.

It is important to clarify DOJ's use of material witness warrants after the 9/11 attacks. Every person detained as a material witness as part of the 9/11 investigation was found by a federal judge to have information material to the grand jury's investigation. An individual is detained under the material witness statute, 18 U.S.C. § 3144, <u>only</u> when a federal judge concludes that (1) the witness' testimony is "material in a criminal proceeding"; (2) it may become impracticable to secure the witness' presence by subpoena; and (3) the witness meets criteria for detention under the Bail Reform Act, 18 U.S.C. § 3142. Each and every material witness is entitled to counsel by statute, and counsel will be appointed if the witness cannot afford to pay for an attorney. (18 U.S.C. § 3006A(a)(1)(G).) Once the warrant is issued and the witness is arrested, a <u>court</u> applies the Bail Reform Act (18 U.S.C. § 3142) to decide whether to detain the witness pending his or her testimony. An individual detained under the statute is entitled to a speedy detention hearing before the court, where the witness is afforded representation by counsel and is entitled to present evidence and cross-examine government witnesses. (18 U.S.C. § 3142(f).) At such a hearing, the government must establish that "no condition or combination of conditions will reasonably assure the appearance of the person as required." (18 U.S.C. 3142(e).)

Moreover, under Federal Rule of Criminal Procedure 46(h), a court must supervise the detention of material witnesses to eliminate unnecessary detention and an attorney for the government must report biweekly to the court, listing each material witness held in custody for more than 10 days and explaining why the witness should not be released. In short, there are numerous judicial safeguards built into the long-established practice of detaining material witnesses pursuant to a warrant. (See, for example, the case of United States v. Awadallah, 349 F.3d 42, 62 (2d Cir. 2003), in which the court noted that the material witness statute and related rules "require close institutional attention to the propriety and duration of detentions.")

63. The Second Circuit Court of Appeals wrote in 2003 [in the *Awadallah* case] that the purpose of the material witness law is to secure testimony where it may become impracticable to secure the presence of the witness by subpoena. The Court added: "It would be improper for the government to use [the material witness law] for other ends, such as the detention of persons suspected of criminal activity for which probable cause has not yet been established." Do you agree that it is improper for the government to use the material witness law for purposes other than securing testimony?

Response:

18 U.S.C. § 3144 permits DOJ to seek an arrest warrant for a material witness if a judge can be persuaded that it appears that the witness possesses information material to a criminal proceeding and that it is impracticable to secure the presence of that person by subpoena. Pursuant to the same statute, a judge may order such a witness to be detained as necessary to secure the witness's testimony after careful application of the factors identified in 18 U.S.C. § 3142. As in the Awadallah case, wherein the Second Circuit Court of Appeals ruled that the detention was a scrupulous and constitutional use of the statute, DOJ only seeks such warrants when authorized by the statute to secure the presence and testimony of a material witness. See U.S. v. Awadallah, 349 F.3d 42, 64 (2d Cir. 2003).

64. The government noted as part of the settlement with Mr. Mayfield that the FBI had taken steps "to ensure that what happened to Mr. Mayfield and the Mayfield family does not happen again." What steps has the FBI taken? Do they include any new guidance respecting the use of the material witness statute?

Response:

In the aftermath of the 3/11/04 Madrid train bombing, the FBI's Latent Print Unit performed a fingerprint analysis and reported a match with a candidate print from an Integrated Automated Fingerprint Identification System (IAFIS) search. It was subsequently determined that the match was in error, and the latent print was ultimately identified to a different subject.

Upon recognizing the error, the FBI's Laboratory implemented its established corrective action process regarding the three FBI examiners who made the error, which included a review of all cases that involved identifications by these examiners, re-training, and a review of cases involving individuals awaiting execution.

In June of 2004, the FBI Laboratory convened an international committee of distinguished latent print examiners and forensic experts to review the fingerprint analysis performed by the FBI Laboratory in the Madrid Train Bombing Case. The Panel recommended improvements to procedures and guidelines to help minimize the possibility of this type of error occurring in the future.

Following the International Committee's review, the FBI Laboratory assembled eight teams of experienced forensic scientists from within and outside the FBI Laboratory to methodically inspect every aspect of the latent fingerprint process in a scientific manner and address each recommendation made by the International Panel. Each team was headed by non-latent print unit personnel from the FBI Laboratory and most teams included external members from the forensic community. These teams were tasked with a number of missions, including: 1) review of the policy regarding cases with "less than original evidence" (in the Madrid Bombing case the FBI Laboratory was provided, via e-mail, digital images of the processed latent fingerprints; the team recommended the establishment of minimum requirements for accepting digital images in lieu of actual evidence), 2) review of the training provided to all Latent Print Unit employees (all aspects of the training program were reviewed, with resulting changes to training programs for both new and experienced examiners), and 3) a complete review of the latent print standard operating procedure (the team provided detailed recommendations for revisions to the procedures).

The FBI's Laboratory approved the implementation of all internal review team recommendations, which were published as a special report in the Journal of

Forensic Identification ("Review of FBI Latent Print Unit Processes and Recommendations to Improve Practices and Quality," Journal of Forensic Identification, 56(3): 402-434, May/June 2006), and continues to conduct research relating to latent print identification and to work with the FBI's CJIS Division to complete the implementation process pertaining to IAFIS system improvements.

A review of the FBI's investigation by DOJ's OIG concluded that the investigation and arrest were driven by the misidentification of the fingerprint, rather than by misuse of any authority or statute. Therefore, the corrective steps taken by the FBI have focused on the Laboratory procedures used in this case.

DOJ believes the existing framework for the use of material witness warrants, as detailed in the responses to Questions 62 and 63, above, is sufficient and no new guidance is necessary.

SENTINEL

65. You testified that there will be no cost overruns or budget shortfalls for the Sentinel program. However, in December 2006, the Department of Justice Office of Inspector General ("OIG") released a report that found that the FBI will need an additional $56.7 million over what the President requested in his budget for next year to continue the Sentinel project, and that these additional costs could have an adverse impact on the FBI's counterterrorism and other programs. The OIG's report also calls the FBI's cost estimate for the Sentinel program into serious question.

a. Does the FBI need additional funds to pay for Phase II of Sentinel and if so, how much additional funding is needed?

b. You testified that the FBI has set aside $57 million to make up the difference between the President's $100 million budget request for Sentinel and the anticipated program costs for Phase II. What FBI programs will be cut back or eliminated in order to use these funds to pay for Sentinel?

Response to subparts a-b:

The funding requested in the President's FY 2007 budget will fund O&M for Phase 1 and most of the system development, training, and program management costs for Phase 2. The full FY 2007 requirement for Sentinel, $156.7 million, was estimated during formulation of the FY 2007 budget and has not changed. In consultation with DOJ, OMB, ODNI, and Congress, the FBI has identified $56.7 million remaining from Phase 1 funding and prior-year unobligated balances available to support the FY 2007 requirements of the Sentinel program. All identified funds are either expired or were previously approved for use on Sentinel; no programs will be reduced or eliminated due to the reprogramming. Funding for Phases 3 and 4 and for the remainder of O&M for all Phases will be included in future budget submissions.

c. Will you promptly inform Congress of Sentinel's operational impact on other FBI programs if reprogramming of funds is necessary to pay for Sentinel?

Response:

The FBI has offered quarterly updates to each of its oversight Committees since the Sentinel contract was awarded to Lockheed Martin on 3/16/06. These briefings cover all aspects of Sentinel, including progress of each phase of development, independent verification and validation, and budget issues.

66. Earlier this year, the Government Accountability Office ("GAO") found that the FBI paid about $10.1 million in unallowable costs to contractors during the Trilogy program. You have said that the FBI would pursue these funds upon completion of a closeout audit of the Trilogy program by the Defense Contract Audit Agency. When will the FBI start to recover these taxpayer funds?

Response:

The FBI is doing everything possible, consistent with the laws governing federal acquisition, to recover any improper payments made during the Trilogy program. The FBI has engaged the services of the Defense Contract Audit Agency (DCAA) to thoroughly audit the Trilogy program in order to identify any improper costs that could be recovered. In a December 2006 letter to the GSA, the FBI requested that the DCAA audit address the concerns identified in GAO's review of Trilogy, including double billing for labor, payments for first class travel, subcontractor invoice validation, timecard validation, extended work week policies, and other direct costs (ODCs). The audit effort will include a 100 percent review of incurred costs for labor, travel, and ODCs. Completion of the full audit is anticipated a minimum of nine months after the Trilogy contractors and their subcontractors provide all supporting documentation. The FBI will conduct interim progress meetings with GSA's Federal Systems Integration and

Management Center (FEDSIM) and DCAA during the audit period, and GSA-FEDSIM will use the audit recommendations in the efforts to recover monies owed to the FBI.

67. Another concern raised by the GAO is the FBI's over-reliance on government contractors to complete Sentinel. According to the GAO, 77 percent of the positions for Sentinel will be filled by contractors rather than by government personnel. Given the FBI's past experiences with contractors on the Trilogy program, is the Bureau overly relying on contractors for Sentinel?

Response:

We do not believe the FBI is over-relying on contractors to staff the Sentinel Program Management Office (PMO). In the Bureau's response to the draft GAO report, we did not agree with the GAO's observation regarding contractor versus government staffing levels. In our discussions with one of the GAO auditors, we learned that this was intended to be an "observation" rather than a "recommendation," that it was based on two other programs the GAO had reviewed, and that this observation has no basis in industry or government "best practices."

As currently configured, contractors, including personnel from the Federally Funded Research and Development Centers (FFRDC), will comprise 72 percent of the Sentinel PMO staff. The Bureau believes this allows flexibility in bringing on board qualified individuals with the appropriate clearances and special skill sets relatively quickly. We believe many successful information technology (IT) programs have had higher ratios of contract to government personnel, using personnel from FFRDCs, nonprofit centers, and similar organizations to augment government personnel in successfully managing program offices.

The PMO staffing plan is the product of a great deal of thought and research.

- The Office of the Chief Information Officer (OCIO) invested three months to assess the correct mix of engineering, business and administrative management, contract, legal, transition, operations and maintenance, organizational change management, and communications and staff support necessary to manage the Sentinel program, interface with major stakeholders, and keep the FBI user population informed and engaged.

- The staffing plan was based on an analysis of program needs, consideration of the lessons learned from other IT projects, and full coordination with FBI leadership. The PMO Staffing Plan, which was aligned with the personnel needs identified in Program Management Plan, defined the staff's skill requirements, associated government and contractor PMO staffing levels, and proposed plan for filling the PMO positions. The Staffing Plan included the use of FFRDC personnel to manage units (under the supervision of the unit chief) until qualified government replacements were found to provide continuity.

- The Program Manager (PM) and Deputy PM personally reviewed the résumés of all potential staff members, including both government employees and contractors, to ensure that we reached the proper mix and balance of skills. The PM formed an integrated team of subject matter experts from government, FFRDCs, and Systems Engineering and Technical Assistance contractors in order to maximize program expertise, ease the staffing burden for any one contractor, and afford the greatest possible flexibility in addressing known and unforeseen staffing requirements. The PM also ensured that the organizations providing contract support to the PMO have a well- established and positive reputation and history of work with the FBI.

ARABIC-SPEAKING AGENTS AND TRANSLATORS

68. Despite progress on hiring Arabic translators, the FBI lags far behind when it comes to the number of agents who are proficient in Arabic. Recently, *The Washington Post* reported that only <u>33</u> FBI agents have at least a limited proficiency in Arabic and only <u>1 percent</u> of FBI agents have any familiarity with the language.

a. How can the FBI effectively fight the war on terror when most of its agents lack even a basic proficiency in the Arabic language?

<u>**Response**</u>:

Please see our response to Question 14b, above.

b. How has the lack of Arabic speaking agents impacted the Bureau's ability to develop relationships with Arabic-speaking and Muslim communities within the United States?

Response:

The number of Arabic speaking agents has not impacted the FBI's ability to develop relationships with the Arab-American/Muslim communities within the United States. The FBI's Community Relations Unit has established a close working relationship with Arab-American, Muslim, Sikh, and South Asian leaders at the national level. All 56 FBI field offices have also established and/or strengthened relationships within those communities in their jurisdictions.

c. How has the lack of Arabic speaking agents impacted the Bureau's ability to gather critical counterterrorism intelligence?

Response:

It is important to understand that no national security threats have gone unaddressed due to an insufficiency of Arabic-speaking FBI SAs. Despite the limited number of Arabic-speaking SAs, the FBI has been able to address the national security threats by maximizing our use of our on-board Arabic-speaking SAs, using our non-SA Arabic-speaking employees in direct support of operations, and turning to our partners in the intelligence, law enforcement, and military communities to provide language resources to address the national security threats as they arise. Nonetheless, our efforts to address national security threats have been made more challenging by our limited number of Arabic-speaking SAs. For example, this limitation impedes our ability to interact with, recruit sources in, and interview subjects and witnesses in Arabic speaking communities.

The FBI is very aware of our need for more investigators with Arabic language abilities and we have adjusted our hiring practices with a view toward the recruitment and retention of SAs with relevant language skills. While clearly the objective of maintaining a cadre of employees with language abilities sufficient to address national security matters in a timely fashion is made more challenging by the fact that the individuals who threaten us speak a wide variety of languages, in a plethora of dialects, and come from a wide range of social, cultural, geographic, and religious backgrounds, we are actively recruiting and training those who can best serve in this complex and challenging mission. The FBI is implementing expedited testing and security background processing of SA applicants who possess fluency in critical foreign languages. As a result of these procedures, a large number of SAs who possess fluency in foreign languages critical to the FBI are expected to attend new Agents training classes in July, August, and September, 2007.

69. You previously testified that the FBI can translate high-priority counterintelligence material within 24 hours. Is this still the case, and what are the realistic prospects for this type of material to be translated in something approximating real time?

Response:

The FBI continues to translate foreign language collection from its highest priority investigations within 24 hours, except in rare circumstances where an unusual or rare dialect is used. Translation of foreign language materials in "real time" is the least efficient method for translating because those operations require dedicating linguists to single projects. Most of the FBI's linguists are simultaneously tasked with myriad projects, providing support to each based on current priorities. However, during periods of heightened activities, the FBI does assign linguists to "live monitoring" of these priority targets.

AFGHANISTAN OPIUM TRADE

70. Earlier this year, the United Nations Office on Drugs and Crime ("UNODC") reported that there has been a surge in opium cultivation in Afghanistan that is fueling the insurgency in that country. According to the report, opium production in Afghanistan has increased 59 % over last year and in the southern region where Taliban insurgents have intensified their attacks on Afghan government and U.S. forces, opium cultivation has increased by 162 %. Given that the Bush Administration routinely describes the international narcotics trade as a national security issue, and that the production of opium has skyrocketed since the invasion of Afghanistan and removal of the Taliban, what does this mean for our national security at home and for the safety of our troops in Afghanistan?

Response:

The large scale production of opium in Afghanistan is not only a significant threat to Afghanistan's future and the region's stability, it also has worldwide implications. In the past, terrorist groups derived much of their funding and support from state sponsors of terrorism. With increased international pressure, many of these funding sources have become less reliable and, in some instances, have disappeared altogether. As a result, terrorist groups have turned to alternative sources of financing, including fund raising from sympathizers and nongovernmental organizations and criminal activities such as arms trafficking, money laundering, kidnapping for ransom, extortion, racketeering, and drug trafficking. This trend is true not only in Afghanistan but around the world, and increasingly blurs the distinction between terrorist and drug trafficking organizations.

Both criminal organizations and terrorist groups continue to develop international networks and to establish alliances of convenience. In the new era of globalization, both terror and crime organizations have expanded and diversified their activities, taking advantage of the globalization of communications and banking systems and the opening of borders. There are many facets of combating narcotics production and trafficking in Afghanistan. In addition to eradication, interdiction, and seizing heroin labs, it is critical to attack the trafficking networks, their infrastructures, and their illicit assets.

Much of this important work has been accomplished by the DEA, which fully reopened its Kabul Country Office in January 2004, making significant progress under difficult conditions. To date, DEA has increased staffing levels in the Kabul Country Office, deployed "Foreign-Deployed Advisory and Support Teams in Afghanistan, mentored and trained the Afghan Narcotics Interdiction Unit, targeted high-value trafficking organizations and their leaders, achieved the first extradition from Afghanistan, and coordinated Afghan-based investigations with its law enforcement partners, including the FBI. DEA's investigative approach focuses on the use of credible, corroborated, confidential sources whose activities are closely directed and monitored by SAs to identify, penetrate, disrupt, and dismantle these organizations. In Pakistan and Afghanistan, DEA has developed a cadre of reliable sources of information and developed many valuable relationships. Because DEA is concerned with the nexus between terrorist activity and its association with narcotics trafficking, DEA personnel are directed to solicit information of assistance in the global war on terror at all informant debriefings. These relationships have yielded actionable intelligence regarding ongoing anti-coalition activities, and information gathered through DEA human intelligence (HUMINT) sources has assisted in thwarting hostile acts against U.S. personnel and interests inside of Afghanistan.

TERRORIST WATCHLIST

71. You recently disclosed that the Terrorism Screening Database ("TSDB") contains <u>491,000</u> records and that the FBI's review of the database to ensure the accuracy of these

records will take years. The glaring errors in the FBI's Terrorist Watchlist – including the names of Members of Congress, infants and even nuns – clearly make the case for why this review is needed. These errors also suggest that any review of the TSDB must also include finding out how the bad information that is in this database got there in the first place.

a. What is the FBI doing to find out how bad data got into the TSDB and onto the terrorist watchlist?

b. Is there any procedure in place that requires the FBI to conduct an internal investigation whenever errors are detected in the TSDB? Should there be?

Response to subparts a and b:

It is important to understand that records in the TSDB meet only the threshold for suspicion of terrorism for inclusion in the database. Once the suspicion has been established, it is appropriate to include that identity on watch list. As more information becomes available, the record may be updated or removed from TSDB. This is not an indication that the record was initially included in error, but rather a reflection of the additional information obtained regarding the individual and its impact on the record's status. It has been widely reported in the media that persons who are wholly inappropriate for watchlisting, such as members of Congress and young children, are included on the terrorist watchlist and, as a result, have had difficulty boarding planes. These reports are highly misleading in that they suggest that every individual who has been delayed or had difficulty during a screening process is on the terrorist watchlist. Unnecessary alarm is often caused by airline ticket agents who erroneously inform travelers that they are "on a watchlist" if the individual encounters any difficulty during the security screening process. Unfortunately, individuals who share an identical or similar name with watchlisted individuals may experience delays at various points of screening (e.g., U.S. ports of entry, airports, etc.) until screeners can verify they are not, in fact, those watchlisted. These individuals are commonly referred to as "misidentified persons" because their inconvenience is due to a temporary misidentification with a watchlist record. GAO recently issued a detailed report (GAO 06-1031) regarding this problem and the Executive Branch's efforts to minimize the inconvenience caused to these persons. TSC's efforts to assist misidentified persons include an operational procedure to maintain records of encounters with misidentified persons and check those records when a new encounter occurs so TSC can rapidly identify and clear known misidentified persons during screening. TSC has also established an inter-agency redress process for persons having watchlist-related screening difficulties.

As discussed in response to Question 11a, above, the TSDB contains data on known and appropriately suspected terrorists, which is provided to the TSC by either the NCTC (for international terrorists) or the FBI (for purely domestic terrorists). The TSDB was initially created by consolidating all data in U.S. government data systems into a single database. Because of the urgency of establishing a consolidated watchlist, terrorism data from other systems was added to the TSDB with limited review or quality controls. As a result, much of the quality assurance efforts that ideally would have been performed prior to compiling TSDB were, by necessity, pushed to the back end of the process. Since the TSDB was created, significant efforts have been underway at the TSC to establish strong gate-keeping controls to prevent inappropriate records from being added to the TSDB and to review existing TSDB records to ensure they are appropriate for watchlisting.

The TSC has developed numerous internal quality controls for the various stages of the watchlist process to increase the quality of the TSDB. These quality control efforts are discussed at length in response to Question 11, above. While there is no policy requiring a formal investigation when watchlist errors are identified, TSC takes appropriate steps to determine if the error was an isolated one or part of a larger problem involving multiple records that now must be reviewed and corrected. TSC also provides feedback to the nominating agencies when errors are made in the nomination process that would degrade the quality of the watchlist.

The TSC's ability to improve the quality of the watchlist is limited, however, as TSC is not in a position to validate information provided by nominating agencies. For example, TSC has no ability to investigate, verify, or judge whether information in an intelligence cable is accurate as reported or from a reliable source. TSC must rely upon the agencies that investigate terrorism and gather and analyze intelligence to provide accurate, complete, and current information to support terrorist watchlist nominations, and to critically review that information before nominating someone for inclusion on the watchlist. Through the TSC Governance Board, inter-agency working groups, and other means, TSC works closely with nominating agencies to clarify watchlist standards and to streamline operational protocols to improve the quality of the watchlist data that is sent to TSC daily. Clearly, though, the agencies that nominate individuals to the watchlist are in the best position to improve the accuracy and reliability of the watchlist by ensuring the validity of the underlying intelligence and investigatory data that support these nominations.

CYBER SECURITY

72. During the hearing, you testified that cyber crime is one of the FBI's top three priorities on the national security side. In late November, there were unconfirmed reports of a threatened attack on U.S. stock market and the Banking industry websites by a radical Muslim group. According to press reports, the attack would be in retaliation for the detention of Muslim prisoners at Guantanamo Bay.

a. What steps did the FBI take to respond to this threat?

__Response__:

The FBI's Cyber Division was informed on 11/13/06 that DHS's U.S. Cyber Emergency Response Team (US CERT) had released a threat report concerning a cyber attack on the U.S. Stock Exchange in New York. The Cyber Division, which has a full-time senior manager detailed to the US CERT for liaison purposes, immediately requested additional information from US CERT and its member agencies and briefed the FBI's CTD and National Press Office.

The web site referenced in the threat report is generally known to law enforcement, the IC, and the media, having posted a threat against the Vatican in October 2006. The FBI continued its coordination with the US CERT to determine the necessity for additional public announcements and investigative activity. US CERT decided to retract the threat release and inform the public that the threat was not credible, and ultimately no additional public alerts were necessary.

b. What resources does the FBI currently have dedicated to U.S. cyber security?

__Response__:

The FBI's Cyber Division includes 59 Supervisory Special Agents at FBIHQ to ensure coordination of cyber matters with other agencies and among FBI programs (including counterterrorism and counterintelligence programs) and to provide program oversight on a national and international basis. In addition, 527

SAs in the field are dedicated to U.S. cyber security matters; in each of the FBI's 56 field offices there is at least one SA dedicated full time to cyber security. The FBI has also created Cyber Action Teams (CAT), which are computer emergency response teams that can deploy worldwide and can draw on both FBIHQ and field assets. The CATS are comprised of highly trained cyber SAs, Computer Analysis Response Team examiners, IAs, and other FBI assets, and can address incidents that require advanced cyber expertise. In addition, the FBI's InfraGard program is dedicated to promoting ongoing dialogue and timely communication between the FBI and the private sector (including the banking industry) concerning critical infrastructure protection issues.

In addition to these FBI-wide programs, individual field offices have developed cyber security programs tailored to their individual circumstances and threats. For example, the FBI's New York Division includes a cyber intrusion squad that has developed a very productive working relationship with the financial services industry and the brokerage industry in New York. Among many other liaison efforts, representatives from the New York Division annually address the Chief Information Officer (CIO) forum, which includes numerous Fortune 500 companies.

PUBLIC CORRUPTION

73. In your testimony at the hearing, you called public corruption the FBI's top criminal investigative priority and you asserted that there has been an increase in the number of agents investigating public corruption cases and the number of cases investigated. However, a September 2005 report by the Department of Justice Office of the Inspector General found that, from 2000 to 2004, there was an overall *reduction* in public corruption matters handled by the FBI. The report also found declines in resources dedicated to investigating public corruption, in corruption cases initiated, and in cases forwarded to U.S. Attorney's Offices. It further found that some field offices were not giving public corruption sufficient emphasis and had scaled back their anti-corruption efforts.

a. What have you done since the Inspector General's report came out to ensure that combating corruption gets the resources and attention it needs?

Response:

In May 2002, Director Mueller designated public corruption as the top criminal priority, and overall as the fourth investigative priority of the FBI. Since then, SA resources expended to address the public corruption program have increased markedly, with a 40% increase occurring from FY 2004 to FY 2006. In FY 2004, 434 SAs addressed public corruption; in FY 2005, the number of SAs who worked public corruption increased to 528; and in FY 2006, 606 SAs addressed public corruption. Considering that the total number of SAs allocated to address criminal matters decreased by almost 1,000 after 9/11, the increase of 172 SAs in the public corruption program clearly demonstrates the FBI's commitment to addressing public corruption. The 40% increase in SAs resulted in an increase in statistical accomplishments in the public corruption program, as follows:

Category	**FY 2004**	**FY 2005**	**FY 2006**	**% increase from 2004 to 2006**
# of Agents	434	528	606	40%
Pending Cases	1854	2118	2233	20%
Informations/Indictments	785	890	954	22%
Convictions	595	759	800	34%

In addition, over $300 million in restitution was obtained as a result of public corruption cases adjudicated in FY 2006.

This significant increase in statistical accomplishments is attributable to the dedication of more public corruption resources in the field to address myriad public corruption crime problems, including judicial, executive, legislative, law enforcement, municipal, regulatory, and prison corruption, that affect every FBI jurisdiction in the United States. They are also attributable to the FBI's focus on specific crime problems, such as the Hurricane Fraud Initiative, International Contract Corruption Initiative (with current emphasis on the Middle East), Southwest Border Corruption Initiative, Campaign Finance and Ballot Fraud Initiative, Capital Cities Initiative (with emphasis on state-level legislative corruption), and the Foreign Corrupt Practice Act Subprogram. To support these investigations, the public corruption program provides regular domestic and international public corruption training and also conducts regular field office visits throughout the United States pursuant to the Program Enhancement Initiative (PEI).

The FBI recognizes that public corruption poses an enormous threat to the credibility of federal, state, and local government in the areas of legislative, executive, law enforcement, judicial, municipal, regulatory, contract, and prison corruption. Public corruption can not only place physical security at risk, it also undermines the community's faith and confidence in government and erodes trust in the institutions upon which the American democratic system is based. The strategic focus of FBI public corruption investigations is on the most corrosive criminal acts by public officials. Most investigations are long-term and complex in nature. Because of this focus, the public corruption program cannot be evaluated solely based on the number of cases initiated. Instead, the quality and significance of the impact exerted by these corruption investigations is a better indicator of the success of the FBI's efforts to combat corruption.

b. Would the FBI benefit from additional resources to combat public corruption? If so, what types of resources would be the most helpful?

Response:

The FBI will continue to address program needs through the budget formulation process in coordination with DOJ and OMB.

74. In your written testimony, you cited the Phoenix Division's Lively Green investigation as an example of the FBI's commitment to, and success in, investigating public corruption. The *Arizona Republic* reported earlier this year that FBI agents working on the Lively Green investigation paid for a room for informants to stay in a presidential suite at the MGM Grand Hotel in Las Vegas. According to a disclosure made by prosecutors, the informants and suspects staying in the room hired prostitutes and sexually abused an unconscious prostitute. Soon after, FBI personnel recorded conversations which included detailed descriptions of the incident, and agents reviewed lewd photographs from the incident. FBI personnel failed to report the incident to prosecutors, who learned of it only many months later from an informant, and one agent was found to have made statements apparently suggesting that the informants get rid of the incriminating photographs. Although the Lively Green prosecutions went forward successfully, these cases were placed in jeopardy by this conduct.

a. What is the FBI doing to ensure that the problems that plagued the Lively Green investigation and other past investigations – agents covering for their informants' misconduct – do not happen again?

Response:

Several months ago the FBI's DI initiated a comprehensive review and revision of our HUMINT program in conjunction with DOJ. As one part of the re-engineering project, the FBI is working with DOJ to draft revised AG Guidelines governing source operations and to develop new internal manuals. The Validation Standards Manual details the implementation of a comprehensive, Bureau-wide validation process that has been reviewed by DOJ and complies with the standards developed by the ODNI. In addition to requiring the validation of every source and every relationship between an SA and a source on a regular and consistent basis, the revised validation process will be streamlined and automated through a new technology application. By automating the administrative aspects of human source operations, the FBI will improve compliance with AG Guidelines and reduce human error.

b. Are you satisfied with the steps that the FBI took to investigate and respond to the misconduct in the course of this operation?

Response:

Yes. Based on allegations of misconduct, a timely, thorough, and comprehensive internal investigation was conducted by the FBI Inspection Division into the course of events surrounding the Lively Green case. Numerous signed, sworn statements were provided by FBI employees. Interviews were also conducted with the Assistant United States Attorneys familiar with the Lively Green case. Several interviews were conducted with cooperating witnesses who actively participated in the Lively Green case. At the conclusion of the internal inquiry, the results were forwarded to the FBI's OPR for adjudication. The two subject employees specifically denied any awareness of criminal misconduct by the cooperating witnesses. Based on these denials and the lack of preponderant evidence to the contrary, no findings were made against the two employees. To prevent a recurrence of the problems encountered in the Lively Green investigation, the FBI has taken the steps outlined in response to question 42a, above, and increased its training in this area.

FBI COMPUTER SYSTEM FAILURE

75. According to several press reports, the FBI's National Instant Criminal Background Check System, which is used to screen gun buyers, crashed several times in November 2006

– potentially allowing gun buyers to purchase firearms without being properly screened. According to the FBI, this background check system receives between 30,000 and 50,000 background check request each day, so this is not an insignificant matter. I have three questions:

a. Has the FBI determined what caused the system to crash, and has this problem been fixed?

Response:

The FBI's CJIS Division has been reviewing and analyzing logs that were generated during the National Instant Criminal Background Check System (NICS) outage on 11/26 and 11/27/06 in order to determine the cause of the outage. As of 1/7/07, no clear cause of the outage had been determined.

System and database administrators continue to monitor the NICS system in case of recurrence. Since the NICS outage on 11/26-27, the NICS system has only received a few of the "Two Task" Oracle 3106 errors (the errors seen during the November outage) and the system has recovered on its own with no intervention needed. Developers have reviewed the computer code and have not identified any changes to code that would cause this type of error.

NICS developers are receiving daily system logs for further analysis. In addition, the FBI is working in the non-operational environment in an attempt to recreate the outage, but to date these efforts have been unsuccessful.

Absent a clear indication of the cause of the outage, the only changes made to NICS as a result of it have been an increase in the shared memory pool and Oracle database cache, which appear to have resolved the issue. The FBI's CJIS Division will continue to monitor and analyze the NICS in order to prevent or minimize future outages.

b. Does the FBI know how many gun sales were completed without background checks while the system was down?

Response:

The outage on Sunday, 11/26/06, lasted 45 minutes, and the three outages on Monday, 11/27/06, lasted 34 minutes, 1 hour 24 minutes, and 35 minutes. Even with these outages, NICS processed 17,983 firearms transactions on Sunday (11/26) and 29,867 on Monday (11/27). For comparison purposes, on the Sunday and Monday after Thanksgiving in 2005, NICS processed 14,574 and 28,200 firearms transactions, respectively. The FBI has no reason to believe gun sales were executed during the outage in violation of the legal requirements of the Brady Handgun Violence Prevention Act of 1993.

c. What is the FBI doing to make sure that this problem never happens again?

Response:

The FBI's CJIS Division has made all of the changes recommended by the vendors. As indicated in response to subpart a, above, the problem has not recurred, but the CJIS Division will continue to monitor the system and make any corrections we identify.

MIKE GERMAN / WHISTLEBLOWERS

76. According to the Office of the Special Counsel ("OSC"), the average number of whistleblowers who have filed complaints with the government has increased by 43% since September 11, 2001. Yet, sadly, the number of whistleblowers who have filed reprisal complaints with the OSC because their employers have retaliated against them for coming forward has also increased by 21% during the same time period. For example, former FBI special agent Michael German has said that his reputation and career were ruined after he reported concerns about misconduct on the Bureau's terrorism investigations to his superiors. What is the Bureau doing to protect the rights of whistleblowers within the FBI to come forward and disclose government fraud, waste and abuse?

Response:

Although the FBI can never completely eliminate an employee's fear of whistle blower retaliation, factors likely to induce such fear can be reduced or eliminated. The anonymous nature of inspection leadership surveys (which are conducted prior to internal FBI inspections to assess management effectiveness), private interviews with the inspection staff during these inspections, and executive managers who promote the proper environment all help to reduce the fear of whistleblower retaliation. If an employee nonetheless believes retaliation has occurred, this may be reported to the Inspection Division's IIS or to DOJ's OIG or

OPR. FBI employees are also frequently reminded through FBI-wide emails and other mechanisms that there is a procedure established under law (5 U.S.C. § 2303) and implemented by regulation (28 C.F.R. Part 27) that provides a formal avenue for an employee to seek corrective action based on a personnel action taken in reprisal for whistle blowing.

77. Many whistleblowers in the intelligence community are discouraged from coming forward because intelligence agencies are exempted from the Whistleblower Protection Act. Would you support legislation to extend whistleblower protections to national security employees?

Response:

Congress specifically excluded the FBI and other IC agencies from the application of 5 U.S.C. § 2302 (the government-wide Whistleblower Protection Act) because of the classified and sensitive nature of their work and the fact that any employee may have access to such information. The legislative history indicates that the exceptions for the FBI and the other specified agencies is tied to the intelligence aspect of their missions. See H.R. Rep. 328, 101st Cong., 1989 WL 225002 (Leg. Hist.). We support the Congressional reasoning that underpins these exceptions.

Congress has provided separate whistleblower protections for national security employees through the IC Whistleblower Protection Act of 1998 (ICWPA). The ICWPA provides that an employee may communicate "a complaint or information with respect to an urgent concern" regarding intelligence activities to the appropriate Inspector General (or designee) and thereafter, under specified circumstances, "to Congress by contacting either or both of the intelligence committees directly." Inspector General Act of 1978, 5 U.S.C. Appendix 3, §§ 8H(a)(1) and (d).

ANTHRAX INVESTIGATION

78. The Bureau's investigation into the 2001 anthrax attacks that killed 5, infected 17 others and terrified millions of Americans is now well into its fifth year. Many believe that the investigation has gone very cold and no arrests have been made in the case.

a. What is the current status of the anthrax investigation?

b. Do you expect that criminal charges will be brought in the case and if so, when?

c. You testified at the hearing that the FBI currently has 17 agents and 10 postal inspectors assigned to the anthrax investigation. Has the number of personnel dedicated to the investigation changed? Will you consider increasing the number of agents and investigators dedicated to this investigation?

d. How much money has the FBI spent on the anthrax investigation to date?

Response to subparts a through d:

Pursuant to the longstanding DOJ policy against disclosing non-public information concerning pending law enforcement and litigation matters, we are unable to provide a response at this time.

79. A frequent criticism of the anthrax investigation is that the FBI has made a number of incorrect assumptions about the source of the anthrax and refused to heed outside expert advice in the case. Will the Bureau be open to new theories about the case and more receptive to outside expertise and criticism going forward?

Response:

Pursuant to the longstanding DOJ policy against disclosing non-public information concerning pending law enforcement and litigation matters, we are unable to provide a response at this time.

80. You testified that the FBI has "periodically" provided briefings for the family members of the anthrax attacks. When was the Bureau's last briefing to victims and their family members? How often does the FBI provide these briefings?

Response:

During the months of May, June, and July, 2003, the FBI and United States Postal Inspectors provided investigative briefings to various victims and/or their family members. Some victims or family members declined briefings. Subsequent investigative updates were provided through letters to the victims or their family members dated 12/11/03, 3/3/04, and 10/25/04. The FBI provided additional oral briefings in person or through conference calls to the victims and/or their family members on 11/10/05 and again on 10/27/06. These briefing provide as much information as can be provided without compromising the criminal investigation.

COMBINED DNA INDEX SYSTEM (CODIS)

81. A recent investigation by *USA Today* uncovered nearly three dozen cases during the past five years in which investigators failed to pursue potential suspects whose DNA matched evidence found at crime scenes. ("Many DNA Matches Aren't Acted On, Nov. 21, 2006). According to *USA Today*:

The unpursued matches had this in common: All were recorded as 'hits' by the CODIS system and added to the list of CODIS-aided investigations that the FBI makes public. Through September, the FBI counted 39,291 such matches since 1990. No one is certain how many of those matches resulted in arrests or convictions, however. In part that's because no law or regulation requires crime labs, the FBI or local law enforcement to follow through and determine what becomes of DNA matches after the CODIS system reports them to the police. Crime lab officials believe hundreds more matches have not been pursued by authorities. They say those matches might become evident only after a perpetrator is caught for a second time.

a. Does the FBI keep any data on how many CODIS matches are pursued by investigators?

b. Does the FBI keep any data on how many CODIS matches have helped solve crimes?

Response to subparts a and b:

Not currently. The Combined DNA Index System (CODIS) database, by statute, does not include any personal identifiers, as the system was established to link DNA laboratories together in order to share DNA information. We welcome a dialogue with our state partners to discuss a reporting mechanism for tracking matches that lead to arrests and convictions.

While there is no reporting mechanism that links prosecutors, law enforcement, and crime labs, the success of CODIS can be measured by tracking the number of crimes it helps to solve. CODIS's primary metric, "Investigation Aided," is defined as a case that CODIS assisted by producing a lead that would not otherwise have been developed. Through October 2006, CODIS had assisted in more than 40,000 investigations covering 49 states and two federal laboratories. CODIS has also produced nearly 9,000 forensic hits, 4,000 national offender hits, and 26,000 state offender hits.

82. The leader of the FBI's CODIS unit told *USA Today* that tracking the results of DNA matches would present a "significant task" that the FBI is not geared to undertake, and that accounting for CODIS matches should be the responsibility of local police and prosecutors who are given match information. Do you agree?

__Response__:

Yes. The FBI Laboratory is responsible for the maintenance and enhancement of the CODIS software used by Federal, state and local law enforcement laboratories. The FBI also supports the communication infrastructure for forensic DNA laboratories participating in the National DNA Index System (NDIS). The FBI Laboratory's points of contact for CODIS and NDIS are the forensic DNA laboratories, of which there are 178. These forensic DNA laboratories interact with each other when a potential CODIS match is identified in order to confirm that match.

Once a CODIS match is confirmed, the information is transmitted to the appropriate Federal, state, or local law enforcement agency. The reporting of the CODIS match to law enforcement has long been considered to be part of the analysis of the evidence and part of the investigative process. Once the forensic DNA laboratory has provided this information to law enforcement, is often no further interaction between the forensic DNA laboratory and the law enforcement agency unless or until the case goes to trial, since the forensic DNA laboratories may not be involved in the resolution of a case unless they are called upon to testify to the evidence. There are over 18,000 law enforcement agencies in the United States, and laboratories can work cases for multiple law enforcement agencies. This makes the tracking of the results of DNA matches throughout the country very difficult.

83. Do you have any recommendations for improving accountability in this area? How can the federal government get an accurate measure of CODIS's real world value in solving crimes?

Response:

The FBI Laboratory has mechanisms to measure the effectiveness of CODIS and, therefore, to provide some measure of accountability. Participating forensic DNA laboratories are required to report to the FBI, on a monthly basis, on investigations aided, offender hits, and forensic hits. These statistics are reported on the FBI's web site.

The selection of these particular performance measures was determined because CODIS was designed as a tool to assist in criminal investigations, especially cases in which law enforcement has not identified a suspect. When CODIS provides information, either the identity of a potential suspect or a link between two or more cases, we consider that to be investigative information - information we would not have were it not for CODIS and the DNA database.

During the implementation of the NDIS in the 1990s, the FBI Laboratory sponsored a limited study to determine whether it was possible and effective to track confirmed CODIS matches through resolution of the case. At the conclusion of the study, very little meaningful information was obtained regarding the resolutions of the related cases because many of the cases were still pending and because of the difficulties inherent in obtaining information across multiple agencies.

A couple of jurisdictions (New York and Virginia) are currently trying to track CODIS match information through case resolution. These jurisdictions are working to coordinate communication between the agencies involved in the processing of a case through resolution (laboratories, law enforcement, prosecutors, and courts). Preliminary information reported by these jurisdictions indicates that there is still a significant percentage of the CODIS match cases that falls in the "pending" category. Additionally, one jurisdiction has encountered inconsistent reporting practices by the multiple agencies involved. Additional follow-up by the agency conducting the study is necessary in order to obtain the case status.

CORPORATE FRAUD

84. You testified during the hearing that white-collar criminal cases were one of the FBI's top three priorities on the criminal side. Recently, Deputy Attorney General McNulty issued new guidelines for corporate fraud investigations to address growing concern about

the Department of Justice's investigation and prosecution of corporate fraud cases and, in particular, criticisms of the Department's policy – embodied until recently in the so called "Thompson Memorandum" – to request that corporate defendants produce attorney-client privileged and/or work product information in these investigations.

a. Does the FBI request or demand that corporate defendants turn over attorney-client privileged or work product information in its corporate fraud investigations? If so, would you describe such requests as routine in white collar fraud cases?

Response:

According to DOJ guidelines, the FBI may request attorney-client privileged or work product information only at the direction of a federal prosecutor who has obtained a waiver of attorney-client or work product protections from a corporate defendant. These requests are not routine, but waiver of privilege may be sought in an appropriate case after a federal prosecutor obtains the necessary supervisory approvals to make the request. The approval process is set forth in the McNulty Memorandum.

b. What will the FBI do to ensure that agents investigating corporate fraud cases conform their conduct to fit the standards set out in the new McNulty Memorandum?

Response:

The FBI conducts all corporate fraud investigations in close collaboration with DOJ attorneys. The FBI strictly abides by applicable laws, regulations, and guidelines, including the McNulty Memorandum. Agents will consult with prosecutors when necessary to ensure that any production of documents by a corporate defendant is consistent with the McNulty Memorandum's requirements.

GARDNER-QUINN MURDER INVESTIGATION

85. During the hearing, you testified that the FBI agent who published details of the Gardner-Quinn murder investigation in a Vermont newspaper is under investigation. What is the status of this investigation and has the agent involved been disciplined by the FBI?

Response:

In December 2006, the DOJ OIG reviewed an allegation regarding this disclosure and subsequently referred the matter to the FBI for review. The FBI's IIS initiated an administrative inquiry into the allegation, and that inquiry is currently pending.

Questions Posed by Senator Kennedy

I. HATE CRIME STATISTICS

In your written responses to my questions, you confirmed the number of federal hate crimes prosecutions in 2004.

86. Can you please provide the same data for 2005 and 2006?

Response:

FBI investigations resulted in 31 indictments/informations and 19 convictions in hate crime matters during FY 2005. During FY 2006, 21 indictments/informations and 23 convictions were obtained.

87. Can you include details relating to each case that you are including in the statistics for 2004 and 2005, including the state in which each case was opened or an indictment was issued?

Response:

Because the question acknowledges that the statistical data for 2004 was previously provided in response to a Question for the Record following the 5/2/06 hearing (Question 78), and the preceding question (Question 86) requests Hate Crime information for 2005 and 2006, we interpret this question as requesting details and statistics for the years 2005 and 2006.

2005

During FY 2005, the following Federal hate crime convictions and informations/ indictments were obtained (information is provided by category and location).

Racial Discrimination with Force and/or Violence

Location	Convictions	Informations/Indictments
California	3	1
Kentucky	-	1
Missouri	-	2
New York	1	-
North Carolina	3	-
Texas	2	4
Total	**9**	**8**

Racial Discrimination with No Force or Violence

Location	Convictions	Informations/Indictments
California	2	3
Nebraska	1	-
District of Columbia	1	1
Total	**4**	**4**

Religious Discrimination Involving Force and/or Violence

Location	Convictions	Informations/Indictments
Illinois	-	1
Kentucky	-	1
Oregon	-	4
Tennessee	-	1
Texas	1	1
Washington	1	3
Wisconsin	1	1
Total	**3**	**12**

Religious Discrimination with No Force or Violence

Location	Convictions	Informations/Indictments
Illinois	-	1
Nevada	1	-
Total	**1**	**1**

Housing Discrimination Involving Force and/or Violence

Location	Convictions	Informations/Indictments
Indiana	1	-
Maryland	-	6
Michigan	1	-

Total	**2**	**6**

Housing Discrimination with No Force or Violence

There were no convictions or informations/indictments in this category in FY 2005.

2006

During FY 2006, the following Federal hate crime convictions and informations/indictments were obtained (information is provided by category and location).

Racial Discrimination with Force and/or Violence

Location	Convictions	Informations/Indictments
Arkansas	2	2
California	4	1
Florida	1	1
Maryland	1	1
Missouri	1	2
North Carolina	1	-
Total	**10**	**7**

Racial Discrimination with No Force or Violence

There were no convictions or informations/indictments in this category in FY 2006.

Religious Discrimination Involving Force and/or Violence

Location	Convictions	Informations/Indictments
Alabama	-	3
Illinois	2	-
Oregon	4	1
Washington	2	-
Total	**8**	**4**

Religious Discrimination with No Force or Violence

There were no convictions or informations/indictments in this category in FY 2006.

Housing Discrimination Involving Force and/or Violence

Location	Convictions	Informations/Indictments

Arkansas	3	4
Michigan	1	3
Ohio	-	2
Total	**4**	**9**

Housing Discrimination with no Force or Violence

Location	Convictions	Informations/Indictments
Michigan	-	1
Total	**-**	**1**

II. USE OF CONFIDENTIAL INFORMANTS

88. In response to written questions submitted by Senator Grassley, the FBI responded that the Department of Justice is working on new Attorney General Guidelines on source operations. As you know, many members of the Senate Judiciary Committee have an interest in this topic. Please provide a copy of the revised Guidelines to the Committee as soon as the revised Guidelines are complete. Can you please confirm when these new Guidelines will be issued? Can you also provide further detail on the process that FBI personnel will follow under the new Validation Standard Manual for every source and relationship?

Response:

The AG Guidelines Regarding the Use of FBI Confidential Human Sources were approved on December 13, 2006 and are provided as Enclosure C.

Every human source will be subjected to the validation process as outlined in these AG Guidelines and the Validation Standards Manual, which is still in draft form. For further details on the validation process, please see the section titled "Validation of a Confidential Human Source" in the attached copy of the AG Guidelines.

89. Specifically, how will the guidelines be revised, in particular Section IV Special Notification Requirements pertaining to notifications to federal, state and local prosecutors of crimes committed by confidential informants?

Response:

Under the new AG Guidelines Regarding the Use of FBI Confidential Human Sources, notification to state and local officials is required when, with the concurrence of the Chief Federal Prosecutor and the FBI SAC, an FBI SA has reasonable grounds to believe that the alleged felonious activity of a current or former confidential human source is being prosecuted by, is the subject of an investigation by, or is expected to become the basis of a prosecution or investigation by a Federal, state, or local prosecutor's office.

In addition, if an FBI SA has reasonable grounds to believe that a confidential human source has engaged in unauthorized criminal activity (other than minor traffic offenses), the Chief Federal Prosecutor and the FBI SAC, with mutual concurrence, shall notify any state or local prosecutor's office that has jurisdiction over the confidential human source's criminal activity and that has not already filed charges against the confidential human source for that criminal activity. For specific language on these requirements, please see the "Special Notification Requirements" of the attached AG Guidelines.

90. Under the existing guidelines, the Chief Federal Prosecutor and Special Agent in Charge must concur prior to notifications to federal, state and local prosecutors. Will the revised Guidelines require prompt notification of information pertaining to crimes committed by confidential informants, to federal, state and local prosecutors having jurisdiction with or without this concurrence?

Response:

Please see the response to Question 89, above. According to the AG Guidelines section titled, "Exceptions and Dispute Resolution," whenever there is a dispute between or among entities, the dispute shall be resolved by the Assistant Attorney General for the Criminal Division or the National Security Division, whichever is appropriate, or his/her designee.

91. Will the guidelines be revised to expressly prohibit FBI contact or utilization of confidential informants who are fugitives or the subject of warrants issued by federal, state and local jurisdictions without notice to those jurisdictions? A grand jury in New York has found that Special Agent Lindley DeVecchio did have contact with an FBI confidential informant (Gregory Scarpa, Sr.) who was at the time the subject of a state warrant for gun

possession charges. How will the revised guidelines address situations like those arising in the case of Special Agent Lindley DeVecchio?

Response:

The revised AG Guidelines Regarding the Use of FBI Confidential Human Sources expressly prohibit FBI contact or utilization of sources who are fugitives or who are the subjects of warrants issued by Federal, state, or local jurisdictions without notice to those jurisdictions. For specific language regarding fugitives, please see the subheading titled, "Fugitives" in the section titled, "Special Approval Requirements" in the attached copy of the AG Guidelines.

92. Please provide the Committee with more information on the changes being implemented in the Confidential Informant Review Committee (CIRC) process. Specifically, identify under what circumstances (if any) a source could have a designated classification that would not be reviewed by such a committee.

Response:

According to the approval process detailed in the section titled, "Special Approval Requirements" in the attached copy of the AG Guidelines Regarding the Use of FBI Confidential Human Sources, those sources providing information for use in international terrorism investigations, national security investigations, or other activity under the AG Guidelines for FBI National Security Investigations and Foreign Intelligence Collection would not be reviewed by the Human Source Review Committee (HSRC). The HSRC, previously called the Confidential Informant Review Committee, is a committee composed of DOJ and FBI representatives that will review certain human sources who report on criminal matters. Pursuant to the new AG Guidelines, the following categories of human sources will require special approvals: Senior Leadership Sources, Privileged or Media Sources, High-Level Government or Union Sources, and Long-Term Sources. All sources will be subject to the validation process as detailed in the FBI's Confidential Human Source Validation Standards Manual (pending approval).

93. Will the FBI make changes to existing policy in order to allow an investigation to be conducted when an FBI agent retires or resigns? What is your view on whether the FBI has an institutional interest in reviewing whether there were violations of its internal disciplinary system, even when the agent subsequently retires or resigns?

Response:

Prior to November 2004, internal investigations were discontinued when an employee resigned or retired during the pendency of an investigation/adjudication. On 11/1/04, that policy was changed so that, notwithstanding the resignation or retirement of an employee, a disciplinary matter is completed when necessary to protect the institutional interests of the FBI (such as when a retiree seeks FBI re-employment as a contractor), while also considering the finite resources available to the FBI in investigating/adjudicating employee misconduct cases, the need for speedy resolution of matters impacting current employees, and the limited impact the FBI's administrative process can have on a former employee. This determination to complete a case notwithstanding the subject's retirement or resignation will be made on a case-by-case basis.

94. The GAO has reported that no government-wide policies or process are in place to improve the sharing of critical counter-terrorism information. Please provide more information on what steps the FBI is taking to improve information-sharing with its state and local partners. Specifically, how will bureaucratic measures such as the creation of an "FBI Information-Sharing Policy Board" ensure that "real time" information-sharing of terrorist information with state and local law enforcement authorities will take place?

Response:

Since the attacks of 9/11/01, the FBI has enhanced our partnerships with state, local, and tribal law enforcement to ensure that we share information as fully and appropriately as possible with our law enforcement and IC partners. The guiding principle is that FBI information and IT systems must be designed to ensure that those protecting the public have the information they need to take action. Three primary initiatives are: Law Enforcement National Data Exchange (N-DEx); Law Enforcement Regional Data Exchange (R-DEx); and the Law Enforcement Online (LEO) network. N-DEx will provide a nationwide capability to exchange data derived from incident and event reports. The national scale of N-DEx will enable rapid coordination among all strata of law enforcement. R-DEx enables the FBI to join participating Federal, state, tribal, and local law enforcement agencies in regional full-text information-sharing systems under standard technical procedures and policy agreements. The FBI makes national intelligence more readily available to state, tribal, and local law enforcement agencies through LEO. This system provides web-based communications to the law enforcement community to exchange information, conduct online education programs, and participate in professional special interest groups and topically focused dialog.

FBI efforts to ensure the "real time" sharing of terrorist information with state and local law enforcement authorities include the FBI's JTTFs and FIGs, the TSC, the NCIC Violent Gang and Terrorist Organization File (VGTOF), LEO, and other activities discussed further below.

From an information sharing perspective, the FIGs are the FBI's primary component for receiving and disseminating information. They complement the JTTFs and other squads and task forces. The FIGs play a major role in ensuring that we share what we know with our IC and law enforcement partners. The FIGs share information with law enforcement partners through Fusion Centers. State Fusion Centers and other Multi-Agency Intelligence Centers have become a focal point of information exchange and relationship building, and the FBI is committed to participating in these centers as resources permit. We have identified 43 states with designated State Fusion Centers in varying stages of development. FBI personnel are assigned to 24 of these centers and we are assessing the remaining 19 centers for assignment of FBI personnel. Some of the existing Fusion Centers are co-located with the FBI's FIG and local JTTF. In addition to supporting the State Fusion Centers, we are also participating in 8 select Multi-Agency Intelligence Centers throughout the country; a total of 188 FBI personnel are assigned to 32 state and regional Fusion Centers.

In addition to these efforts, the FBI shares classified intelligence and other sensitive FBI data with Federal, state, and local law enforcement officials who participate in the JTTFs, which are important force multipliers in the fight against terrorism. Since 9/11/01, the FBI has increased the number of JTTFs from 35 to 101 nationwide. We have also established the National Joint Terrorism Task Force (NJTTF) at FBIHQ, staffed by representatives from 38 Federal, state, and local agencies. The mission of the NJTTF is to enhance communication, coordination, and cooperation by acting as the hub of support for the JTTFs throughout the United States, providing a point of fusion for intelligence acquired in support of counterterrorism operations.

The FBI has also established the TSC to consolidate terrorist watchlists and provide around-the-clock operations support for Federal, state, local, and tribal law enforcement personnel across the country. Police on the streets access the TSC through the FBI's NCIC and its VGTOF. The FBI will continue to create new avenues of communication between law enforcement agencies to better fight the terrorist threat.

To provide a single source of coordinated Federal assessments to state and local officials, the FBI is also joining with DHS, the ODNI, and other agencies to establish an Interagency Threat Assessment Coordination Group located at the NCTC.

The FBI's Information Sharing Policy Board (ISPB), which is chaired by the EAD of the NSB, further enhances our information-sharing efforts with our law enforcement partners. The ISPB brings together the FBI entities that generate and disseminate law enforcement information and intelligence to implement the FBI's goal of sharing by rule and withholding by exception. The ISPB initiates, develops, enacts, monitors, and maintains the primary policies, decisions, and procedures concerning substantive criminal and intelligence information sharing internally and externally. The FBI ISPB oversees the FBI's participation in the Information Sharing Environment (ISE) and addresses any ISE-related FBI information-sharing policy issues. For example, upon the recommendation of the ISE PM in 2006, the ISPB reviewed the policies associated with FBI pilot projects funded by the ODNI.

On 11/14/06, the ODNI submitted to Congress the Implementation Plan for the terrorism ISE, which serves five communities: intelligence, law enforcement, defense, homeland security, and foreign affairs. For information sharing at the Federal level, the ISE Implementation Plan calls for greater coordination so that strategic and time sensitive threat information gets to those who need it. Key elements are a national management structure, architecture, and standards. FBI roles include:

- The AD for the DI is a full member of the ISE Information Sharing Council, which is chaired by the ISE PM, who comes from the ODNI. A senior FBI executive is a deputy to the ISE PM.

- The FBI's CIO develops and implements plans for the ISE Enterprise Architecture Framework and Common Terrorism Information Sharing Standards, consistent with the DOJ and IC architectures and standards.

- The FBI has established the NSB to combine intelligence, counter-terrorism, counterintelligence, and WMD functions, making the FBI a preeminent domestic intelligence agency. The NSB shares information with the other U.S. intelligence agencies through secure communications and the Intelink network.

- The FBI has assigned SAs and analysts to the NCTC, which analyzes all intelligence pertaining to terrorism. A senior FBI executive is the principal deputy director of the NCTC. The FBI CTD is co-located with the NCTC and the CIA's Counterterrorism Center.

For information sharing with state, local, and tribal governments, the ISE Implementation Plan provides for a network of state and regional Fusion Centers that communicate, cooperate, and coordinate with each other and with the Federal government. In 2006, the FBI provided to the ISE PM an Enterprise Architecture report on 39 FBI programs related to the ISE (29 Unclassified, 10 Secret). The FBI followed up with briefings by senior representatives of the NSB, the Science and Technology Branch, the OCIO, and PMs of the following 13 unclassified programs related primarily to the ISE Implementation Plan.

Dedicated National Counterterrorism Programs:

1. Foreign Terrorist Tracking Task Force (FTTTF) (including E-Guardian)
2. TSC

Counterterrorism-Related Web-based Networks

3. LEO (including InfraGard support)
4. SCI Operational Network

Information Sharing Infrastructure

5. Sentinel
6. N-DEx

Analysis and Dissemination Capabilities

7. FBI Automated Messaging System

Collection and Exploitation Capabilities

8. ELSUR Data Management System

Federal Multi-source Information Resources

9. IDW

Primary Law Enforcement Community Resources

---

10. NCIC (including VGTOF)
11. Next Generation Integrated IAFIS
12. Biometric Interoperability
13. CODIS

Additional FBI projects are supported by the ISE PM as pilot projects.

95. Please clarify your response to my written question regarding Inspector General Fine's report of a 42% rate of noncompliance with confidential informant files with respect to the Section 1V, Special Notification Requirements of the current Attorney General Guidelines. Contrary to the written response provided by the FBI to the Committee on November 30, 2006, there is a requirement that the FBI notify state and local prosecutors of criminal activity by confidential informants. Specifically, subsection B.2 of the Special Notification requirements states "whenever such Notifications are provided the Chief Federal Prosecutor.....and the Special Agent in Charge with the concurrence of each other shall notify any state or local prosecutor's office that has jurisdiction over the confidential informant's criminal activity".

a. Please explain how compliance can be achieved when it is not known whether compliance is required under the existing Guidelines.

Response:

Please see the responses to Questions 89 and 90, above.

b. Please explain how the new and revised Guidelines will deter future non-compliance with the Guidelines when the Guidelines have failed to act as a sufficient deterrent in the past.

Response:

The new human source policy will mandate compliance. Appropriate communications will be sent to the field to ensure familiarization with the new AG Guidelines and SSAs' Quarterly Reviews will address compliance with these Guidelines. One of the critical elements of the performance work plans for both SAs and their supervisors specifically identifies compliance with the AG Guidelines as a performance measurement, making it clear that non-compliance with the new Guidelines will be addressed as a performance matter. If merited by the violation, a report may be issued to the appropriate entity within DOJ or to the FBI's OPR, resulting in formal review and potential disciplinary action.

96. In light of the FBI's failure to comply with the existing Guidelines and the ineffectual sanctions to deter violations of the Guidelines, please state the FBI's position on H.R. 4132, the Law Enforcement Cooperation Bill introduced by Congressmen Lundgren and Delahunt. The bill would require mandatory prompt Notification to federal, state and local prosecutors having jurisdiction, whenever the FBI obtains knowledge a confidential informant or any other individual has committed a violent crime. If the FBI has concerns about this proposed legislation, please provide the Committee with a detailed explanation of those concerns.

Response:

The FBI's concerns regarding H.R. 4132 are articulated in the 8/25/06 letter provided as Enclosure D.

III. NEW REPORTING REQUIREMENTS UNDER THE REAUTHORIZATION OF THE PATRIOT ACT

The USA Patriot Improvement and Reauthorization Act enacted last March contains new reporting requirements relating to National Security Letters as well as an audit of the use of these letters.

97. Under the Act, a report on the number of National Security Letters is due to the Senate Judiciary Committee by April 2007. Please provide the Committee with an update and detailed information on the FBI's progress to comply with implementation of these new reporting requirements.

Response:

Pursuant to the USA PATRIOT Improvement and Reauthorization Act of 2005, the AG submitted the first annual report on 4/28/06. The FBI is currently compiling the information required for the calendar year 2006 report. We expect that report to include a caveat regarding the reported number of different U.S. persons on whom we have collected data through NSLs because, toward the end of the year, we discovered that we had not adequately explained the change in the reporting requirement to our field personnel. That lack of clarity, together with the fact that the U.S. person status of the subject of an NSL (as opposed to the

U.S. person status of the target of the investigation) is not always clear, leads us to believe that the statistics we have this year on the number of different U.S. persons whose data is gathered through NSLs will not be as precise as we would like. Further, we have learned from the review conducted by the DOJ OIG that there are other errors in our compilation of these numbers. We continue to work to ensure the accuracy and reliability of these statistics.

98. Please provide the Committee with information relating to any changes in FBI policy or procedures following the enactment of the USA Patriot Improvement And Reauthorization Act last March.

Response:

The USA Patriot Improvement and Reauthorization Act ("Patriot IRA") amended several statues that are regularly used by the FBI in the conduct of its national security investigations. In limited respects, some of these statutory changes required changes to FBI processes; other notable changes largely codified procedures the FBI already followed.

NSLs. The Patriot IRA modified the various authorities pursuant to which the FBI issues NSLs in several respects, it increased the number of committees to which certain semi-annual reports are made, and it altered the content slightly of those reports.

Those changes required three changes to FBI process and procedure. First, the FBI is now required to report the number of different persons (including status as a U.S. Person or Non-U.S. Person) about whom information is sought. As discussed further above, before enactment of the Patriot IRA the FBI reported only the U.S. Person status and the number of different targets about whom information was gathered. This change in external reporting has required changes in internal reporting. Agents are now required to include with every request for an NSL the U.S. Person status of the person to whom the requested NSL relates.

The second change to FBI process and procedure required by the Patriot IRA relates to the internal evaluation that must accompany every request for an NSL. Prior law automatically imposed an obligation of confidentiality on the recipient of an NSL. The Patriot IRA requires a case-by-case evaluation of the need *vel non* for the recipient to be obligated not to disclose the existence of the NSL. In response, FBI process now requires its employee initiating the NSL request to explain in the request whether, and if so why, the recipient should be obligated not to disclose the NSL. That justification is reviewed along with the request for the NSL and must be approved by the official who executes the NSL.

Finally, the Patriot IRA mandated that the recipient of an NSL be affirmatively notified of: the process by which he or she can challenge the NSL or the nondisclosure provision and his or her right to disclose the NSL to persons necessary to comply with the NSL request, including an attorney to obtain legal advice or legal assistance regarding the NSL. The FBI made conforming changes to the standard forms of all NSLs.

Roving Foreign Intelligence Surveillance Act (FISA) Surveillance. The Patriot IRA modified FISA regarding the amount of detail the FBI must provide in connection with a FISA roving surveillance order. The application must now include a description of the "specific" target when the target is identified by description rather than by name. The Court, in turn, must find the possibility of the target thwarting surveillance based upon specific facts. The FBI has always provided a description of the target of surveillance, to the extent known. (The FBI's describing the target with as much specificity as possible has always been necessary to accomplish collection on the correct person or persons authorized by the Court.) Thus, this change, in effect, codified existing practice and did not require changes to FBI procedures.

The Patriot IRA also added a statutory return requirement, pursuant to which the FBI is generally required to notify the Court within ten days of instituting surveillance of a new facility under the roving authority. In the notice, the FBI must inform the Court of the nature and location of the new facility, the facts and circumstances upon which the applicant relies, any new minimization procedures, and the total number of electronic surveillances that have been or are being conducted under the roving authority. As a practical matter, that change simply codified the practice that was generally followed with roving surveillance. Even before the Patriot IRA, the FISA Court typically mandated notice to the Court when the surveilled facility changed. The new statute has imposed some more reporting requirements, and FBI has adjusted its process to generate the required information in a timely fashion.

Business Records under FISA. The Patriot IRA made significant changes to Section 215 of the Patriot Act (FISA Business Records Order). Among other things, the law now requires that a FISA Business Records Order describe the tangible things that must be produced with sufficient particularity to permit them to be fairly identified. The Order must also contain a date on which the tangible things must be provided, and that date must afford thc recipient a reasonable period of time in which to produce them. The Patriot IRA also imposes high-level supervisory approval of FISA Business Records Orders when they are seeking certain special categories of things such as library circulation records, library patron lists, book sales records, book customer lists, firearm sales records, tax return records, educational records, and medical records containing information that would identify a person.

The new statutory obligation to specifically describe the documents sought and to provide a date on which they must be produced did not required changes to FBI policy and procedures. Rather, it simply codified existing policy and procedure.

The obligation to obtain high-level supervisory approval for sensitive FISA Business Records Requests has resulted in an alteration in practice. Previously, virtually all FISA Business Records Requests were signed by either the FBI General Counsel or the FBI Deputy General Counsel for the National Security Law Branch. As a result of the Patriot IRA, that process has been altered to the limited extent that, in those very limited situations in which sensitive records are sought, the General Counsel obtains the signature of either the FBI Director or Deputy Director.

FISA Duration Changes. The Patriot IRA extended the duration of initiations and renewals of electronic surveillance, physical searches, and pen register/trap-and-trace surveillance for agents of foreign powers who are not U.S. persons. Initiations and renewals for U.S. persons remained the same.

The duration of FISA surveillance and physical search for non-U.S. persons was increased from the standard of 90-day initiations and 90-day renewals. Electronic surveillance and physical search coverage increased to a 120-day initiation and one-year renewal, and the pen register/trap-and-trace increased to a one-year initiation.

While there was little, if any, effect on FBI policies or procedures, both DOJ and the FBI have benefitted from the substantial savings in resources that resulted from the new durations.

IV. FBI'S ANTI-GANG STRATEGY

The FBI has undertaken various initiatives to combat gang violence.

99. Please provide the Committee with information on the current status and activities of the MS-13 National Gang Task Force.

<u>Response</u>:

The MS-13 National Gang Task Force (NGTF), which is staffed by six SSAs, six IAs, and one program analyst, is currently coordinating 105 cases in 44 FBI Field Offices, having recently initiated new investigations in Omaha and Seattle. The MS-13 NGTF has also assisted Field Divisions by drafting four wire-tap affidavits and its analysts have provided "hands-on" analytical assistance in investigations being conducted by the following Field Offices: Los Angeles, Washington Field Office, Seattle, Houston, Sacramento, Baltimore, and Charlotte. In addition, pursuant to a recent expansion in authority, FBI SAs assigned to Resolution 6 in Mexico City are conducting drug investigations and gathering information in support of transnational criminal gang investigations.

The MS-13 NGTF continues to direct a criminal file/fingerprint retrieval initiative known as the Central American Fingerprint Exploitation (CAFÉ). CAFÉ was developed in conjunction with the FBI's CJIS Division to retrieve and store in the FBI's IAFIS the criminal fingerprints of gang members from Chiapas, Mexico, and the Central American countries of El Salvador, Guatemala, Belize, and Honduras. CJIS has acquired approximately 180,000 sets of criminal fingerprints from Mexico, El Salvador, and Belize, and approximately 20% of these subjects have had some contact with American law enforcement officers. This project is supported by DOS and DHS, both of which have strong interests in being able to identify individuals who have criminal records and/or use aliases at the time they seek entry into the United States. In addition to contributing to border security and assisting in the coordination of gang investigations in the U.S., the CAFÉ initiative is serving as a catalyst for our Central American partner countries to develop their own versions of IAFIS, which will significantly enhance their ability to conduct effective criminal investigations in their own countries.

The NGTF is coordinating the collection and analysis of MS-13 communication activity in areas with significant MS-13 criminal activity or key communication activity among MS-13 cliques. Among other things, the NGTF coordinates the identification of additional gang cells and members, assists Field Offices in formulating investigative strategies that target MS-13's leadership structure, and ensures state and local law enforcement agencies are notified when MS-13 activity is detected in their jurisdictions. The NGTF also ensures that close coordination is maintained with the National Gang Intelligence Center and DOJ's Gang Targeting, Enforcement, and Coordination Center, and is developing a means of using Interpol's "blue notice" system to detect when MS-13 subjects travel or are arrested.

100. Please provide additional information on efforts to coordinate anti-gang activities with government leaders in Central America. Specifically, please provide the Committee with more information regarding the FBI's agent working in El Salvador.

<u>**Response**</u>:

The FBI's San Salvador Legat office was opened as a regional office in June 2006 and provides coverage for El Salvador, Guatemala, Honduras, and Belize, specifically addressing the gang crime problem attributed to the MS-13 and 18th Street gangs. The San Salvador Legat office, which is staffed with a Legal Attaché and an ALAT, has assessed the needs of the judicial systems of the covered and has identified three areas that would benefit from coordinated FBI/U.S. Mission assistance: development of an effective fingerprint system, providing training in conducting investigations, and assisting in controlling the activities of gang members in the inmate population. The effective coordination of anti-gang activities will require improvement in all three areas, and the Legat is facilitating the necessary improvement.

The Legat's assessment revealed that none of the countries in the region have the capability to collect and compare fingerprints through automated means such as IAFIS. Without the ability to compare latent fingerprints from crime scenes or weapons with a subject's fingerprints, law enforcement efforts to solve crimes such as homicides, 70% of which are attributed to gang members, are significantly impeded. To address Ambassador Barclay's concerns regarding the recent increase in violent crime in El Salvador, the Legat coordinated a visit to El Salvador by the Los Angeles Police Department, Los Angeles Sheriff's Office, and Fairfax County Police Department. At the end of the visit, the U.S. law enforcement officers provided an out brief to the Director of the El Salvador police (the Policia National Civil) and to the U.S. Mission, sharing "best practices" and recommendations for combating the MS-13 and 18th Street gangs and making clear the need to fund an El Salvador IAFIS.

Learning from meetings with prison officials in El Salvador, Guatemala, and Honduras that they attribute the gang-controlled prisons to overcrowding, a lack of resources, and poorly paid guards, the San Salvador Legat began to facilitate the provision of technical assistance and the donation of surplus equipment by U.S. Bureau of Prisons (BOP). The Legat is also coordinating the provision of specialized gang investigation training for Salvadoran police officers and prosecutors and is continuing to assist in bringing technology and training to the law enforcement agencies in the region, with the ultimate goal of enabling these organizations to conduct joint investigations of transnational gangs with U.S. law enforcement agencies and to more effectively investigate and prosecute crime within their own borders. To bolster our relations with Central American law enforcement, the MS-13 NGTF recently co-sponsored the Los Angeles International Chiefs of Police Summit on Gangs. The Summit successfully brought together Chiefs of Police from El Salvador, Honduras, Guatemala, Belize, and Chiapas, Mexico, to discuss with American and Canadian law enforcement and other government officials the impact transnational gangs have on Central America, the United States, Mexico, and Canada. This meeting resulted in the identification and development of four initiatives that will be further developed at the April 2007 International Anti-Gang Conference in El Salvador: Top 20 Gang Fugitives, Officer Exchange Program, Prevention/Intervention, and Intelligence/Information Sharing.

101. Please identify the criteria used by the FBI to identify gang members. Specifically, please explain in detail the criteria used to identify gang members arrested in the 650 arrests announced in September 2005.

<u>Response</u>:

The FBI considers an individual to be a gang member if he or she admits to gang membership when arrested or while incarcerated. Absent such an admission, the FBI considers an individual to be a gang member if any two of the following occur: 1) the individual has been identified as a gang member by someone of proven reliability; 2) the individual has been identified as a gang member by an individual of unknown reliability and the information provided by that individual has been corroborated in significant respects; 3) the individual has been observed by law enforcement to frequent a known group's area, to associate with known group members, and/or to affect that group's style of dress, tattoos, and symbols or hand signals; 4) the individual has been arrested on more than one occasion with known gang members for offenses consistent with gang activity; 5) the individual has admitted membership in an identified group at any time other than arrest or incarceration.

The 659 subjects arrested during the 9/7/05 international take-down were selected based upon outstanding warrants or their illegal status within the United States. Seventy-seven of the 659 subjects were MS-13 gang members arrested in the United States on outstanding warrants or immigration violations. Of those 77 MS-13 gang members, 4 were arrested on federal charges other than immigration, 34 were arrested on state and local charges, and 39 were arrested for immigration violations. The 77 subjects were identified as MS-13 gang members through law enforcement resources in the states where they were arrested, including: Rhode Island, New York, New Jersey, Virginia, Georgia, North Carolina, Tennessee, Ohio, Wisconsin, Nebraska, California, and Texas. In addition, the following foreign countries identified and located gang members who were wanted for outstanding warrants, El Salvador (232), Honduras (162), Guatemala (98), and the state of Chiapas, Mexico (90).

102. What additional resources are needed to continue operations of the National Gang Intelligence Center established in 2005? What steps are being taken to coordinate efforts of the Center with state and local law enforcement?

__Response__:

Working in concert with other Federal, state, and local criminal justice agencies, the FBI established the National Gang Intelligence Center (NGIC) to further the collection and analysis of gang intelligence for appropriate use by all criminal justice agencies. The mission of the NGIC is to support criminal justice agencies through information sharing; to perform strategic and tactical analysis of available data focusing on the growth, migration, criminal activity, and associations of gangs; to provide one-stop shopping for gang information; to conduct research and analysis to identify nationwide gang trends; to develop intelligence for the deconfliction and coordination of gang investigations and prosecutions; and to identify any associations or credible links to terrorist activities. A continuation of funding at its current level is required to maintain on-going efforts in support of this mission.

State and local law enforcement remain the primary consumers of NGIC intelligence, which is shared using a three-pronged approach.

The first aspect of this approach is the provision of information access using existing and emerging technologies, including the use of Special Interest Groups (SIGs) on LEO. The NGIC site stores intelligence collected from law enforcement entities across the country on LEO, which is available to users 24 hours a day. LEO also provides a vehicle through which law enforcement can to request tactical or strategic support, or specific intelligence or information, from NGIC analysts. Another NGIC partner, the Regional Information Sharing System, will provide a site that mirrors that found on LEO. In February 2006, the NGIC began using a standardized Request for Information (RFI) form through LEO's NGIC SIG, allowing users to request gang-related information from the NGIC. The RFI enables users to request analytical or tactical support or information on specific gangs, individuals, or tattoos/graffiti.

As part of NGIC's mission, an information technology team comprised of engineers, project management specialists, and financial specialists has been working to develop a single access point for state and local law enforcement entities to receive, request, and access intelligence products and tools. NGIC is acquiring access to several databases used by law enforcement across the country, including GangNET, CalGang, I-CLEAR, and R-DEx.

Secondly, the FBI ensure that the perspectives and needs of our state and local law enforcement partners are recognized and accommodated by participating in the NGIC's Law Enforcement Executive Fellow Program, a six-month program that provides a forum in which state, municipal, and tribal law enforcement executives can share expertise and intelligence.

Lastly, NGIC analysts routinely attend gang conferences to keep current on evolving issues and provide training and briefings to state and local law enforcement personnel. This training includes techniques to assist law enforcement authorities recognize gang activity and gang migration, which is especially valuable to venues that have no historic gang problem but have been newly identified as having a developing gang presence. The NGIC partners with the National Alliance of Gang Investigators Association and sponsors their bi-annual executive board meetings.

Questions Posed By Senator Biden

LOCAL CRIME – COMMUNITY ORIENTED POLICING SERVICES

103. Director Mueller. As you know, I spent my career working to ensure that law enforcement has the tools to do the job to combat crime, and I must say that I am very troubled by the recent Uniform Crime Reports that show what many local chiefs and

sheriffs have been telling me for years – crime is on the rise in the United States. I have often said that fighting crime is like cutting grass. You mow the lawn and it looks great. You let it grow for a week and it looks a little ragged. You let it grow for a month or two, and it looks like a jungle. Well – we are starting to see a jungle. And, listen – I think that we know what we need to do. I believe that we need to reinstate the COPS hiring program and we need to add 1,000 new agents to fill the gaps left by transitioning from local crime to counter-terrorism. Unfortunately, we have decimated the COPS hiring program despite evidence that it works. Study after study showing us what we all know – more cops equals less crime. And despite this evidence we have killed the program. Do you believe that more local COPS on the streets helps combat local crime and can help with counter-terrorism efforts?

Response:

The FBI has a long history of working with our state and local partners, and we believe there are mutual benefits to maintaining robust law enforcement capabilities at all levels.

Local Crime – Federal responsibility to help combat crime

104. Mr. Mueller, many of my Republican colleagues make the ideological argument that local crime is a local problem, and therefore, the Federal government should not play a role in helping local agencies address the local problems. I strongly disagree! How can a local police Chief in Wilmington control the drug trafficking running up and down the I-95 corridor? How can a local sheriff prevent the farming of opium in Afghanistan? How can a local cop address the MS-13 gang that got it roots in El Salvador? It is my view that crime is a national problem and it requires a federal solution. This is why I strongly support federal funding for the COPS program and the Justice Assistance Grant and why I want to add 1,000 new FBI agents to work on local crime with local agencies. What is your view on local crime? Is it a purely local problem in your view and do you agree that international and national problems can have a local impact?

Response:

There is often an international component of crimes that are ultimately executed in, or that directly impact, U.S. localities, and it appears that the trend is toward an increase in multi-jurisdictional crimes. In addition to the circumstances you note, cyber crime is another example of crime crossing jurisdictional and international boundaries. While the FBI must prioritize its resources to protect the nation from terrorism while balancing other responsibilities, we continue to work with and support our state and local law enforcement partners in many ways to address these crimes, including the provision of intelligence analysis and specific expertise.

LOCAL CRIME – LEGISLATION TO AUTHORIZE 1,000 ADDITIONAL FBI AGENTS

105. 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-9/11 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 additional SAs will not be able to function at their full potential.

DOMESTIC SECURITY – CREATING A HOMELAND SECURITY AND PUBLIC SAFETY TRUST FUND

106. Many of the things that we need to do to secure our nation will cost more money, but we can afford it if we change our priorities. This year, the tax cut for individuals making over $1,000,000 dollars is $60 billion. At the same time, the budget for the Department of Homeland Security is $35 billion and the budget for the Department of Justice, which includes the FBI, is $21 billion. So, the two major agencies charged with our nation's domestic security are funded at a lower level than the tax cut for our most fortunate. This is the wrong priority in my view, and I have proposed that we take less than one year of the

tax cut for millionaires and put it in a trust fund to invest in our homeland security over the next five years. With this funding, I would implement the 9/11 Commission Recommendations, fully fund the COPS program, invest in 1,000 new FBI agents, invest in critical infrastructure protection. I know that you will argue that these budgeting decisions are above your pay grade, and that tax policy is not your area of expertise, but I'd like for you to get back to me on the priorities that you would invest in if you had access to additional resources in the coming years.

Response:

The FBI appreciates the efforts of this Committee and the Appropriations Committees to ensure we have the necessary resources. As always, the FBI will work with DOJ and OMB to identify the programs and budgeting needed for the FBI to continue to fulfill its responsibilities.

BACKGROUND CHECKS FOR VOLUNTEERS WORKING WITH CHILDREN

Over the last several years, the FBI has been working with the National Center for Missing and Exploited Children and other organizations on the Child Safety Pilot Program. This pilot program aimed to test the usefulness of background checks being run for volunteers who will be working with children. 25,000 background checks have now been run and a significant number (seven percent) were returned raising concerns about that particular volunteer applicant. In other words, this program led directly to hundreds of volunteers rightfully being kept from securing positions in which they could harm and prey on kids. These results show the usefulness of background checks in this context, and I want to explore ways to expand the program.

107. Will you commit your staff's time and resources to help us expand this program?

108. Does the FBI have any recommendations for how to most effectively and efficiently expand this model?

Response to Questions 107 and 108:

On 12/17/05, Congress enacted the "Violence Against Women and Department of Justice Reauthorization Act of 2005." Section 1197 of this Act extended the child safety pilot program for an additional 60 months and expanded the pilot program to include nonprofit organizations that care for children. The Act also increased the number of fingerprint submissions allotted for the pilot program from 100,000 to 200,000. Eligibility for participation in the pilot program is determined by the National Center for Missing and Exploited Children (NCMEC), with the AG's concurrence. To date, the following nonprofit organizations have been approved to participate in the pilot program: American Camp Association, National Alliance for Youth Sports, National Crime Prevention Council, and the Palouse-Clearwater Environmental Institute.

To support the expansion of the program, the FBI installed a circuit for the CJIS Wide Area Network at NCMEC so that they could submit fingerprints to, and receive criminal history records from, the FBI electronically. The FBI also modified its billing policy to permit any agency that participates in the pilot program to establish a billing account with the FBI. (Previously, only agencies that submitted 500 fingerprints or more a year could establish a billing account. All other agencies had to submit a personal or business check with their fingerprint cards.) As a result of these program improvements, almost every volunteer organization participating in the pilot program is submitting their fingerprints through NCMEC. The FBI believes the current infrastructure is sufficient to process the 200,000 fingerprints allotted for the pilot program.

Recommendations for ways to expand access to FBI background checks for employees and volunteers working with children have been offered in the "Attorney General's Report on Criminal History Background Checks," which was submitted to Congress in June 2006. This report was prepared pursuant to section 6304 of the Intelligence Reform and Terrorism Prevention Act of 2004, which required the AG to make recommendations for improving, standardizing, and consolidating the existing statutory authorization, programs, and procedures for the conduct of criminal history record checks for non-criminal justice purposes. Further expansion of the program would likely require additional fee-funded or other resources to manage enrollments and process fingerprint cards.

109. One finding from the pilot program is that volunteer organizations can only undertake the background checks if it is low cost and administratively feasible. For example, we've found that if organizations face a $20 fee per background check they will be much less able to participate than if the cost were $5 per background check. What can the FBI do to work with volunteer organizations to lower the costs as much as possible?

Response:

The FBI fee for processing volunteer fingerprints is calculated to cover the actual cost of processing the check, including the costs for collecting, maintaining, and disseminating criminal history record information up to the statutory maximum of $18. This fee, which applies to all volunteer checks (not limited to the pilot program), is currently $16 or $18 per submission, depending on the method of payment. The FBI is currently reviewing its fee structure and will propose any necessary revisions by the end of Calendar Year (CY) 2007 (fees will remain within statutory constraints).

110. How can we bring live scan fingerprint technology to bear in the expansion of this program?

Response:

On 11/8/06, the FBI announced the selection of 19 contractors to serve as pre-approved "channelers" who can contract with authorized recipients to capture and submit fingerprints to the FBI for criminal history records checks for noncriminal justice purposes, receive the results of the criminal history checks from the FBI, and promptly forward those results to the authorized recipient. NCMEC has been designated as the authorized recipient of criminal history record information under the PROTECT Act pilot program; the volunteer organizations are not authorized to receive criminal history record information. Therefore, NCMEC could contract with one or more of the approved channelers to provide live-scan fingerprint identification services, though the cost of the service provided by a channeler would add to the total cost of the background check.

Questions Posed by Senator Feinstein

Background: In the November 28, 2006 *Washington Post*, it was reported that the FBI computer system that screens gun buyers' backgrounds for criminal activity – the National Criminal Background Check System – had crashed several times over the past two days, with the outages potentially allowing people to buy firearms without being screened if sellers gave up on making the required check. An FBI spokesman that there was a technical glitch, but said it was still unclear when the problem would be fixed.

111. Can you provide a fuller explanation of what happened, and explain what steps have been taken to fix this problem?

<u>Response</u>:

Please see the response to Question 75c, above.

112. Is there a back-up system in place to perform background checks should the system face any breakdowns in the future?

<u>Response</u>:

There is not currently a back-up system to perform background checks if the primary system is nonoperational.

Background: A DOJ audit released on December 4 says the FBI faces a $56.7 million funding gap in its Sentinel computer project, and "uncertainty" over how to meet its funding needs to continue building it. The FBI responded that this money has been identified from existing FBI balances but will not impact operational programs.

113. Is this still the case? If not, what is needed to keep the Sentinel computer project on track, and why is it needed?

<u>Response</u>:

Please see the response to Question 65b, above.

114. Can you provide us with your candid assessment of how the implementation of the Sentinel project is going, especially as Sentinel enters its higher-risk second phase in 2007?

<u>Response</u>:

We believe the Sentinel Program is on track based on all of the completed program reviews and control gate checks required by the FBI's Life-Cycle Management Directive with respect to capabilities to be delivered in Phase I. In late October 2006, the Sentinel PMO received approval to move from the final design stage to the development of the Phase 1 product. Hardware for the system was delivered and installed at the data centers in both Clarksburg, West Virginia, and FBIHQ. In parallel with development, we are also completing the training curriculum and materials required for deployment of this phase. Completion of Phase I is still anticipated by the late spring of 2007.

We have also started planning for how to develop the capabilities currently allocated for Phase II, and we intend to have all requirements understood, the development approach refined, and a realistic schedule defined (including all lessons learned from Phase I) before beginning the implementation of Phase 2.

As currently planned, the same stringent checks and balances currently practiced for Phase 1 will be employed in Phase 2 - weekly briefings to the Director and Deputy Director; regularly scheduled updates to the DOJ CIO, OMB, several Congressional committees, and other oversight and advisory bodies; a thorough Earned Value Management (EVM) process for both Lockheed Martin and the PMO; and financial reviews by the FBI's Finance Division.

The PMO anticipates continued success in holding program changes and additional costs in check, while realizing that there may be occasions where the right decision will be to modify or adapt the program to meet new critical requirements. Again, there is a detailed process in place for managing change.

Background: As you know, during the 1980s and 1990s, Ms. Leung was being used an informant by the China Squad of the FBI's Los Angeles Field Office. Shortly after our last FBI Oversight Hearing, Inspector General Fine issued a public version of his report on the FBI's handling of Ms. Katrina Leung, along with a list of 11 recommendations beyond the FBI's own corrective steps that were implemented after the Leung investigation began.

Following the last Oversight hearing, Senator Grassley asked you about a separate matter, involving Cecilia Woods' allegations that her supervisor engaged in a sexual relationship with a paid informant. Senator Grassley noted that the standard FBI penalty for an improper personal relationship with an informant is a mere 7-day suspension, and that Ms. Woods' supervisor received a 14-day suspension even though the FBI's administrative review substantiated allegations that he had engaged in misconduct, and he has now apparently admitted in a deposition to sexual activity with an informant.

115. What is the status of the FBI's efforts to implement the Inspector General's 11 recommendations? If some of those recommendations are not being implemented, please explain why.

Response:

Recommendations 1, 6, 7, 8, 9, 10, and 11 have been implemented. Recommendation 7 provides as follows: "The FBI should require alternate case agents meet with asset a specified number of times a year. The frequency of alternate case agent meetings with an asset should depend on the importance of the asset." The FBI believes the current policy sufficiently addresses the OIG's concern. Under current policy, for every source opened, the FBI requires an alternate SA be assigned to the case. Moreover, two SAs must be present when paying a source. The frequency with which an alternate case agent meets with an asset is based on numerous factors and will be left to the discretion of each field office.

Recommendations 2 and 5 have been partially implemented, with full implementation scheduled by the summer of 2007.

Implementation of Recommendation 4 is in progress; the FBI intends to complete implementation by the winter of 2007.

Implementation of Recommendation 3 is also in progress. This recommendation suggests as follows: "The FBI should require the field SSA, the ASAC [Assistant Special Agent in Charge], and the FBIHQ SSA responsible for each asset to signify that they have reviewed the entries in this subsection as part of the routine file review or of the semi-annual or annual asset re-evaluations. If anomalies exist, the SSA should note what action has been taken with respect to them, or explain why no action is necessary, and the ASACs agreement should be noted." The FBI believes the creation of new asset review mechanisms satisfactorily addresses the OIG's concern. During the past two years, the FBI has been developing new policies regarding the utilization of confidential human sources through our Confidential Human Source Re-engineering Project. The FBI's DI and DOJ are collaborating to simplify and standardize administrative procedures, clarify compliance requirements, and improve compliance with the AG's Guidelines. This re-engineering project will include the upcoming Confidential Human Source Validation Standards Manual and the subsequent implementation of a revamped validation process that will apply to all confidential human sources. FBI SAs, the FIGs, FBIHQ, and DOJ will all have roles in measuring the value of a source's operation as well as managing the risks associated with using a human source. Redundancy of review will be an intentional part of the validation process, serving as a check and balance on human source activities, including authorized and any possible unauthorized criminal activities. The EAD of the FBI's NSB has approved a draft of the Validation Manual, and the FBI is moving toward implementation throughout the FBI.

116. Some critics argue that the FBI often allows agents involved in wrongdoing to quietly retire. What are you doing to ensure future accountability, since most of the FBI personnel responsible for the Leung security breach avoided negative consequences by retiring? Do you believe that the penalties described in your colloquy with Senator Grassley about the Woods allegations are consistent with the recommendations of the Inspector General in the Leung affair? If so, why?

Response:

As stated above in response to question 93, in order to ensure the accountability of agents who engage in wrongdoing and then attempt to quietly retire, the Director amended FBI policy governing the administrative inquiry process so that, notwithstanding the resignation or retirement of an employee, a disciplinary matter is completed where necessary to protect the institutional interests of the FBI. Obviously, any matters involving criminal allegations are pursued irrespective of an employee's retirement or resignation.

117. In response to a written question from Senator Grassley after our last Oversight hearing, you appear to acknowledge that no one has ever been disciplined for whistleblower retaliation under the FBI's guidelines. Is that accurate? Can you explain? What is being done to ensure that FBI whistleblowers are being protected from retaliation?

Response:

That is not accurate. As stated above in response to question 42a, the FBI has disciplined a number of employees for engaging in retaliatory behavior, including whistleblower retaliation. OPR recently suspended one supervisor for 30 days for engaging in retaliation against a whistleblower. Although not final, in another disciplinary matter, OPR has proposed the dismissal of a supervisor for retaliating against a whistleblower. In another, OPR imposed a 3-day suspension on a supervisor who threatened to retaliate against a whistleblower.

118. You also noted that, in the one FBI case where a 3-day suspension was initially imposed for whistleblower retaliation, that decision was later reversed, through an

appellate process that the FBI's General Counsel declared to be "flawed." What has been done to fix the appellate process?

<u>Response</u>:

Upon the completion of the Bell/Colwell Commission's study of the FBI's disciplinary process, the FBI adopted changes recommended by the Commission to improve the FBI's disciplinary process. With respect to the FBI's appellate process specifically, the Commission recommended key changes designed to improve the transparency and fundamental fairness of the appellate process for all FBI employees. These changes were adopted and made effective by the FBI Director on 8/19/05.

One such improvement offers non-SES employees the option to choose a mid-level manager, rather than an SES employee, to participate on the three-member Disciplinary Review Board (DRB), which convenes to hear appeals in those cases in which an adverse disciplinary sanction has been imposed by the FBI's OPR. (Previously, the voting members of the DRB's were composed strictly of SES employees.) The advantage of this change is that non-SES employees are now being judged with input from "one of their own." This concept is especially important in light of past OIG investigations into allegations of disparate treatment in the FBI's disciplinary process.

Another important change, recommended by the Commission and adopted by the FBI Director, was elimination of the ability to increase a disciplinary penalty on appeal. This change was made to ensure all employees could take full advantage of the FBI's appellate process without fear of facing additional sanctions. In addition, the Commission recommended that the "de novo" appellate standard be replaced with a "substantial evidence" standard, which is now being used to review matters on appeal. This change allows the FBI's appellate authority to continue to serve as an important check and balance on the entire OPR process.

In addition to the improvements mentioned above, the FBI's appellate authority will continue to seek the advice of the FBI's OGC when guidance is needed on legal matters. The FBI is dedicated to ensuring the FBI's appellate process continues to operate in a fair, effective, and efficient manner for all employees.

Background: In response to questions following the last FBI Oversight hearing about press reports relating to the New York Field Office, you seem to acknowledge that there

may be some FBI agents who do not even have access to e-mail accounts and the internet. You also noted that the FBI has "not dedicated funding for Blackberry purchase or use," with such devices used by FBI divisions only on a limited fee-for-service basis.

119. Do you think these levels of e-mail, Internet and Blackberry access are sufficient? Please explain.

Response:

The FBI is becoming a more strategic, threat-based, and intelligence driven organization, with its IT infrastructure becoming a key enabler of increased flexibility in operations and sharing of information with external organizations. Several ongoing initiatives, including increased access to and use of the Internet and unclassified email accounts by SAs and professional staff, are making this possible.

Increased emphasis has been put on providing every SA with mobile wireless capability (currently using BlackBerry devices) to ensure ubiquitous capability to support the FBI mission. In the FBI, BlackBerry accounts are centrally managed but funded by a combination of sources, including allocations from centralized FBI funding, Field Office budgets, and a fee-for-service plan that is funded and managed in accordance with an office's priorities and needs.

At our current levels of email use, Internet and BlackBerry access are adequate to execute the FBI mission. However, changes in the scope and complexity of the mission will necessitate the use of technology to maintain our capabilities. These changes include improvements to our communications to increase the levels of unclassified and wireless mobile capability.

Recent efforts to upgrade our communications capabilities have included providing every SAC and senior executive with a BlackBerry account and device; connecting FBIHQ, all 56 field offices, and a few off-sites to the FBI's unclassified network (UNET); and conducting a requirements survey to determine how many individual circuits and personal computers are required to install an Internet-access, unclassified personal computer in every employee's workspace. To date, there are 10,623 terminals available; a total of 26,161 UNET accounts have been assigned to 9,387 FBI SAs, 1,783 IAs, and 14,991 other FBI employees, task force members, and contractors. The UNET email server environment is capable of expanding to 30,000 accounts, affording adequate UNET accessibility once other requirements are met.

Additionally, we are conducting a mobility pilot project that will make wireless mobile devices more SA-friendly and provide instant access to critical databases anywhere at any time. Our fee-for-service policy allows those field offices with mobile communication requirements to provide additional BlackBerry functionality for their users until more widespread use in the Bureau.

Background: With[in] the past two weeks, the FBI issued an unusual apology to Brandon Mayfield. Mayfield, a lawyer and Muslim from Oregon, was arrested and held for weeks by the FBI, after FBI examiners erroneously linked him to a fingerprint found after the Madrid train bombing in 2004.

120. [O]ur written testimony describes a variety of internal reviews by teams of forensics examiners and scientists, and new policies adopted since the Mayfield error, all designed to prevent future latent print mistakes. Please explain why fingerprint examiners need to know a suspect's faith or underlying personal characteristics. What procedures have been put in place to ensure that the FBI Laboratory personnel are segregated from a suspect's faith, for example, or his race?

Response:

The latent print examiners were not aware of Brandon Mayfield's religious faith when they erroneously matched his fingerprint to the latent print found near the scene of the Madrid train bombings. When latent print examinations are performed, examiners are not informed of, and have no need to know, the religious faith of the person whose fingerprint they are examining.

Under certain circumstances, an examiner may be aware of physical characteristics such as sex, race, height, weight, eye color, and hair color, which are recorded on the standard fingerprint card. The fingerprint card does not record the individual's religion, so this information is not included in the fingerprint repository and is not addressed in an IAFIS search. If, for example, an unidentified subject commits a bank robbery, a latent print is lifted from something he touched, and the teller identifies him as being male, Caucasian, and over 6 feet tall, the latent print examiner may use those known physical characteristics to search for fingerprints in the database of individuals meeting that description. Since only about 30% of the IAFIS repository may be searched at any one time due to technological constraints, those known factors may assist the examiner in conducting a more efficient search. Each individual in IAFIS is assigned an FBI number. Once an identification is made, strictly on the basis of the fingerprint comparison, the examiner will use the FBI number to obtain the fingerprint record, which contains identifying information such as name, arrest record, and the physical characteristics identified above.

121. Was the Mayfield error an isolated mistake, or did the FBI's internal reviews uncover other problems with accuracy in the analysis of evidence performed by the FBI's three Latent Print Units in other cases?

Response:

The Mayfield error was an isolated mistake. Previous similar case work of the latent print examiners and supervisor who made the error (i.e., cases in which identifications and/or IAFIS searches/comparisons were conducted), dating from 1997 to the time of the Mayfield error, was reviewed and no erroneous identifications were detected. The internal reviews of the three FBI Latent Print Units did not uncover other problems that called into question the accuracy of latent print analysis performed by these units. Nonetheless, recommendations for improvement in the latent print operations have been implemented in order to further minimize the possibility of future errors.

Background: In your recent written responses, you noted that the so-called terrorist watchlist – the FBI's Terrorist Screening Data Base, or TSDB – now contains almost half a million records. You agreed that erroneous inclusion in the TSDB "exerts a negative impact on the individual," and said that "the FBI takes errors seriously and is working to eliminate them."

122. [W]hat is the current backlog for such reviews, and has it increased or decreased in the past year? By how much? What is your definition of "backlog" in this context, and has it changed over the years?

Response:

As stated in the preamble to the question, the TSC and FBI do take errors seriously and work hard to eliminate them with a variety of approaches. There is no "backlog" in the review of incoming records because each records is subject to quality assurance reviews before it is added to the TSDB. The following approaches have been implemented to ensure that the data in the TSDB is current, accurate, and thorough.

- Analysts in the TSC's Nominations and Data Integrity Unit (NDIU) review terrorist records submitted by the NCTC and the FBI daily to ensure the accuracy of biographical and derogatory information through SRQ software. This application enables the TSC to review every nomination of Known or Suspected Terrorists before it is added to the TSDB. As a result of this review, the analysts ensure that the records are exported to the appropriate support systems for screening opportunities based upon the requirements of the respective screening agencies (i.e., Customs, DOS, FBI, and state and local police). For example, individuals nominated to the TSA No Fly List must meet TSA's established criteria and also present a complete name and date of birth (a carrier requirement).

- In addition to the daily quality assurance provided by the SRQ, NDIU analysts work on various proactive quality assurance projects. For example, these analysts are currently "scrubbing" TSA's No Fly List. The "scrub", which has also been supported by 10 TDY Federal Air Marshals, involves a thorough review of every TSDB record currently exported to TSA's No Fly List. The "scrub" of TSA's No Fly List should be completed during the spring of 2007. These analysts will next "scrub" TSA's Selectee List. The Selectee scrub is scheduled to begin in approximately February of 2007.

- The NDIU analysts also conduct encounter-driven quality assurance. When a known or appropriately suspected terrorist is encountered by a law enforcement officer, border official, etc., the records associated with that individual are immediately reviewed for completeness and accuracy. If the records are determined to be accurate and complete, they are maintained as they are. If the records require modifications or removal, the analyst coordinates with the appropriate entity (the NCTC or the FBI) and ensures that record is adjusted or removed accordingly.

123. What is the timeline for resolving the backlog of challenges from those who claim they have been placed on this watchlist improperly?

Response:

Complaints from individuals who are having watchlist-related screening problems are handled through the watchlist redress process, by which individual complaints of adverse screening experiences (e.g., denied boarding on a plane, repeated secondary screening) are referred to the TSC when it appears the complainant is a watchlisted person. TSC established its formal redress process in January 2005 and now has a redress office dedicated to researching and resolving these matters. Because of the in-depth research and analysis the TSC performs on each redress matter, and the fact that most redress matters require that TSC consult with and/or seek additional information from other agencies, TSC does not consider any redress matter to be overdue (and therefore part of a backlog) unless it has not been concluded within 60 days TSC's receipt of the referral.

Following are the statistics for redress matters as of 1/3/07.

	CY2005	CY2006
Total Redress Matters Received	134	253
Total Closed	134	197
Total Pending	0	56
Average Completion Time (Calendar Days)	86	49
Backlog (Number of Pending Matters Open More Than 60 Calendar Days)	0	20

124. If there is a problem processing this backlog, what resources would be necessary to fix it?

Response:

The TSC redress office requires sufficient staffing to handle the volume of redress matters in a timely manner. As noted above, in 2006 TSC experienced an 89% increase in the number of redress matters it received over the previous year. TSC increased its redress staffing in FY 2006 by adding a dedicated redress supervisor, an additional full-time analyst, and several temporary-duty personnel, but has identified the need for additional permanent staff in FY 2007 to address the increased workload. Therefore, TSC is in the process of adding four new redress analysts during FY 2007, which would increase the compliment of full-time, permanent redress analysts from two to six. Under a recently signed agreement between TSC and DHS, DHS has agreed to provide staff to fill the four redress analyst positions during this FY.

It is important to note that redress backlogs can also develop when other agencies do not respond in a timely manner to TSC's request for consultation or additional information. For the past year, TSC has been leading an effort to establish a multi-agency MOU to be signed by all agencies that participate in the watchlist redress process. Among other things, the MOU would secure a commitment from these agencies to provide adequate resources to support the redress process. The MOU also seeks to document the existing inter-agency redress process to reduce confusion and to establish procedures to resolve conflicts among agencies, which TSC believes will streamline the process and thereby speed the resolution of most redress matters. The MOU would require each signatory agency to designate a senior official for redress to ensure that the obligations under the MOU are properly carried out. Currently, the MOU is in the interagency clearance process.

Background: On August 17, 2006, the *Washington Post* published an article describing the FBI Academy at Quantico. It noted that, while 37 hours of counterterrorism training are now given to new agents, this still represents just 5% of the curriculum.

125. The Washington Post article contrasts the FBI Academy with "the Farm" run by the CIA, in which CIA agents-in-the-making train for a year, focusing on how to identify, recruit and manage foreign informants. The article notes that CIA officers assigned to penetrate terrorist organizations are provided with additional, specific training that is heavy on language and cultural indoctrination. Is the CIA's "Farm" and additional formal training approach a model the FBI could use, at least for FBI recruits who plan to serve as intelligence analysts instead of criminal investigators? Why or why not?

<u>Response</u>:

The FBI's TD has entered into a partnership with the CIA to develop an FBI training program that models the CIA's Core Collector training. While the FBI's overall approach to HUMINT collection is similar to the CIA's, as are some techniques and tactics used, there are legal restrictions placed on the FBI that are not applicable to CIA Core Collectors. For example, FBI SAs must identify themselves as FBI when asked or within the early stages of the recruitment cycle, whereas the CIA is not held to those same requirements.

The content of the CIA course will be used as the foundation to build FBI-specific content and practical exercises. The new FBI course (the National Security Domestic Collectors Course) is expected to be six weeks for journeyman-level SAs.

For both agencies, IAs have separate and distinct responsibilities from FBI SAs/CIA Core Collectors, and therefore have different training requirements. FBI SAs have the sole operational responsibility of initiating and managing sources and assets, a function not shared by IAs. FBI new SA trainees receive course work in basic skills development relating to confidential sources, cooperating witnesses, and asset development during the 21-week course at the FBI Academy.

126. An NBC news report on December 4, 2006 also reported that, until recently, new agents received only two hours of Arabic culture training at the FBI Academy. Has this situation been changed, and if so, how many hours are now spent in each category?

<u>Response</u>:

The 21-week new SA training curriculum has, in fact, changed, consisting now of the following international terrorism topics taught by FBI instructors.

- Introduction to International Terrorism (2 hours)
- International Terrorism Case Management (2 hours)
- International Terrorism Investigative Techniques (2 hours)
- International Terrorism HUMINT Practical (4 hours)

This new curriculum also integrates 20 hours of instruction focusing on Arabic, Muslim, and Islamic topics taught by instructors from the United States Military Academy's Combating Terrorism Center in the following areas.

- Islam and the Evolution of Militant Islamic Ideologies (4 hours) (this block of instruction includes: origin of Islam, different schools of Islamic Thought, ideological tenets of Hezbollah, and the Five Pillars of Islam, among other topics).
- Shia Extremism (4 hours) (this block of instruction covers the origins and ideological tenets of Shia Extremists and Hezbollah).
- Beginnings of Sunni Extremism (4 hours) (this block of instruction covers the origins and ideological tenets of Sunni Extremists and Al-Qaeda).

- Virtual Caliphate: Web Use by Terror Networks (4 hours) (this block of instruction looks at breeding grounds for extremism and informal education methods used to radicalize youth).

- European Muslim Diaspora (4 hours) (this block of instruction addresses immigration patterns from threat countries and discusses the origins and operations of terror groups and their threat to the United States).

In addition to the training received during the new SAs' course, the FBI's TD sponsors Bureau-wide training in the areas of Arabic culture and Radical Islam culture as it relates to Sharia Law. The revised training curriculum for new SAs will include "Enrichment" nights that address these areas, and this training will also be offered to those serving in JTTFs and in various executive forums. In addition, beginning in 2005 the FBI's TD has sponsored one-year sabbaticals to Jerusalem for six SAs per year for full-emersion training in Arabic language and culture.

127. The NBC news report also noted that only 33 of the FBI's 12,000 agents have even a limited proficiency in Arabic, and that the FBI currently has a pool of only six fluent, Arab-speaking agents. What is being done to change this situation and accelerate the recruitment of agents proficient or fluent in Arabic?

Response:

The FBI has a variety of training programs designed to improve the language abilities of onboard SAs. For example, in October 2005, the FBI established a year-long overseas Arabic language training program for SAs, with instruction concentrating on practical Arabic for professional use and including familiarization with Arab customs and traditions and with the culture of Islam. Six SAs completed the first program in November 2006.

In addition to this program, the FBI provides shorter-term Arabic language training to SAs on a regular basis. In FY 2006, 34 SAs at various levels of proficiency were provided with survival, full-time, and immersion Arabic language training. For FY 2007, 72 SAs at varying levels of proficiency have submitted applications for Arabic language training programs at DOS's Foreign Service Institute, Middlebury College, and commercial schools with which the FBI has contracts. Approval of these training requests will depend on available funding.

The FBI has developed a self-study computer-based "survival" Arabic language training program that will be ready for distribution in January 2007. This interactive program is targeted to the specific language needs of SAs, and will provide them with a strong foundation in language skills on which to build higher-level proficiency. The FBI has also originated a self-study computer-based program both to teach agents to Romanize Arabic names according to IC standards and to predict nonstandard Romanizations that may be encountered. This program will also be available in January 2007. In addition, the FBI has created new listening and speaking exams that can test for dialect-specific Arabic ability, including Egyptian, Palestinian (Levintine), Algerian, and Iraqi, and we are considering adding other dialects. In the past, all SAs studying Arabic and those applying for SA positions were tested only with exams that measured ability in the Modern Standard Arabic. These exams were not always indicative of true useful speaking or comprehension ability.

The FBI's recruitment and marketing strategies targeting Arab Americans for FBI recruitment have greatly expanded to include the following initiatives.

- A strategy to expedite the testing of SA candidates possessing fluency in Middle Eastern languages has been implemented and will continue throughout FY 2007 and 2008. This strategy immediately identifies new applicants possessing language fluency and expedites all FBI testing and processing of these critically skilled language candidates.

- The FBI has dedicated staff who are solely responsible for the development and implementation of targeted Middle Eastern recruitment strategies. These strategies include building relationships (national and regional outreach to both the public and private sector and to the academic community); education (dispelling myths and misconceptions); direct recruitment; candidate referrals, special career invitational events; collegiate recruitment; high school information sessions and career days; enhanced advertising and marketing; and the promotion of cultural awareness.

- The National Recruitment Program has been restructured to ensure greater accountability and targeted recruitment programs have been implemented nationwide.

- A Middle Eastern Recruitment Task Force has been developed, comprising respected member of Middle Eastern Professional

Organizations, a Middle Eastern Advertising Agency, and current Middle Eastern FBI SAs. The Task Force held its first meeting on 11/13/06 and will meet monthly throughout FY 2007 to develop targeted recruitment strategies and to ensure these strategies are implemented with measurable results. The Task Force will also develop plans to build relationships with Middle Eastern communities and to provide appropriate training to FBI personnel and recruiters in all 56 field offices.

- The FBI is using the services of both Allied Media (a Middle Eastern Marketing Agency) and Bernard Hodes Advertising Agency to develop and implement a robust marketing strategy targeting Middle Eastern linguists for the SA position. This marketing campaign includes special career invitational events and Internet and direct marketing strategies.

- In 2006, the FBI developed the Middle Eastern Foreign Language Honors Internship Program, a targeted internship program designed specifically for students fluent in critical Middle Eastern languages. This program creates an immediate pipeline of SA candidates fluent in Middle Eastern languages.

- Advertisements have been placed in various mediums, including Al Manassah Weekly, Al Arab Weekly, Arab American Business, Copts.net, Arab American News, Aramica, The Arab Voice, Al Hureya, Al Akhbar, Al Nahar, Al Offok, Al Arabi, Detroit Chaldean Times, Arab World, Al Nashra, The Beirut, The Foreign Affairs Journal, Language Magazine, Arab American Business Journal, The Arab American Chaldean Council, Al Sahafa newspaper, Dandana Arabic Television.

- In partnership with numerous Middle Eastern organizations, the FBI hosted "An Evening with the FBI - Career Invitational" on 10/25/06 at FBIHQ. The participating organizations invited selected members of their communities who qualified and were interested in SA positions to attend the event, and 80% of the attendees spoke a critical foreign language.

- The FBI continues to identify and participate in career and job fairs throughout the country in an effort to reach Middle Easterners interested in SA positions.

Questions Posed by Senator Feingold

128. Last year the Government Accountability Office reviewed the Foreign Terrorist Tracking Task Force. GAO recommended that the FBI conduct a Privacy Impact Assessment of this program, which is required by FBI regulations, and has since occurred. GAO also recommended that the FBI make that Privacy Impact Assessment available to the public as appropriate, a recommendation that the FBI has stated is under consideration.

a. Has the FBI decided whether to issue publicly all or part of the Privacy Impact Assessment for the Foreign Terrorist Tracking Task Force?

Response:

As a national security system, the FTTTF system is exempt from the PIA requirement of section 208 of the E-Government Act. Even though the FTTTF system was not required to be assessed under Section 208 of the E-Government Act, the FBI nevertheless examined the privacy issues presented by the development of this system and is satisfied that the system adequately protects privacy. The FBI has determined that, consistent with the balance struck by Congress when it enacted the E-Government Act, the harm to the Bureau's national security mission outweighs the need to provide public awareness of the precise details of the technological tools the FTTTF employs in fighting terrorism. Therefore, we have decided not to make the PIA available to the public. The PIA was, however, provided to DOJ's Privacy and Civil Liberties Officer.

b. If not, will the FBI share the full document with the Judiciary Committee, in classified form if necessary?

Response:

This information is provided separately.

129. According to your recent response to a written question from Senator Leahy after the last oversight hearing, as of May 2006 there were 491,000 records in the Terrorist Screening Database. You also stated that the Terrorist Screening Center began its own record-by-record review in March to make sure that each entry actually belongs on the list. This is obviously a massive task with respect to a database with nearly half a million entries, but it is also important – to make sure that mistakes do not keep people off

airplanes or otherwise adversely affect them. How long do you believe it will take to complete the review of the Terrorist Screening Database?

Response:

The TSC's NDIU is aggressively working to ensure an expeditious and thorough review of all records contained in the TSDB and it is hoped that this process can be completed by the fall of 2007.

As discussed in response to Question 122, above, the NDIU has adopted a multifaceted approach to this review, including the following.

As noted above, the SRQ is a daily and on-going process through which all additions, modifications, and deletions to TSDB records are reviewed by an NDIU analyst. From the deployment of the SRQ in late March 2006 to 1/10/07, NDIU analysts processed a total of 670,444 records. (This does not represent individuals, but the number of records received from NCTC for inclusion, update, or removal from the TSDB.) This new process directly supports the goal of the NDIU eventually reviewing every record contained within TSDB.

In addition, during each positive TSC encounter, TSC analysts review the related TSDB record(s) for accuracy and completeness. If a change to a record is required, the Terrorist Screening Tactical Operations Center forwards the record(s) to NDIU analysts for review and resolution, and NDIU analysts coordinate any required changes with the NCTC or the FBI to ensure situational awareness and data consistency. These full derogatory reviews have resulted in the review of 39,978 TSDB records (as of 11/30/06).

As discussed above, the TSC is also in the process of conducting a "No Fly" review, pursuant to which all records in the TSDB that are currently exported to the TSA No Fly List are being reviewed. This project will result in the review of over 77,000 TSDB records (60,117 of these records had been reviewed as of 1/10/07). At the completion of the No Fly review, NDIU analysts will begin a review of all records in TSDB that are exported to the TSA Selectee List. This project, which would consist of a review of nearly 118,000 records if it were started today, is expected to be complete by the end of 2007. In addition to these projects, the NDIU will continue to identify smaller groups of data that require quality assurance scrubbing and will conduct these reviews as appropriate.

At the conclusion of these reviews, we will identify all records in the TSDB that have not been reviewed and begin that final scrub, resulting in a 100% review of the TSDB and its supporting information.

130. A professor at Seton Hall recently released a report on the designation of terrorist organizations by the U.S. government, and found that different government agencies had different lists of organizations that each agency designated as terrorist groups. Although there seems to be agreement that we need a consolidated terrorist watch list, the U.S. government does not have a consolidated terrorist organization list, at least according to the Seton Hall report. Is that accurate? If so, do we need one?

__Response__:

While the FBI generally looks to the Foreign Terrorist Organization (FTO) list as the consolidated list of designated terrorist groups, Congress has authorized the use of other criteria to identify terrorist organizations, as well. There are three key mechanisms for designating terrorist groups, each with different statutory authority. They reflect different criteria and consequences tied to the designations.

First, the Anti-Terrorism and Effective Death Penalty Act, codified at 8 U.S.C. § 1189, authorizes the Secretary of State, in consultation with the AG and the Secretary of the Treasury, to designate an organization as an FTO if the Secretary of State finds that the organization in question is foreign, is engaged in terrorist activity, and that such activity threatens the national security of the United States or the security of U.S. nationals. Currently, 41 organizations are so designated. Once an organization is listed by the Secretary of State as an FTO, it is a crime for persons in the United States to knowingly provide material support or resources to the organization. In addition, alien representatives and members of designated FTOs may be denied admission to the United States and may be removed if they are already in the United States. Financial institutions that become aware that they possess or control funds belonging to a designated FTO, or that its agent has an interest in such funds, must freeze the relevant assets and alert the Department of the Treasury.

Second, Section 411 of the USA PATRIOT Act, codified at 8 U.S.C. § 1182, authorizes the Secretary of State, in consultation with the AG, to designate terrorist organizations for immigration purposes, prescribing different criteria for designation than for FTOs. This immigration-oriented list is known as the Terrorist Exclusion List.

Third, the Specially Designated Global Terrorist list provides for the designation of organizations and individuals and is based on Executive Order 13224 and various statutes. This list enables the United States to impede terrorist funding in connection with national emergencies to deal with the unusual and extraordinary threats to our national security relating to foreign terrorism, such as the 9/11 attacks. It is a crime to engage in financial transactions with the more than 500 organizations and individuals currently on this list. Financial institutions in possession of assets of such organizations or individuals must freeze those assets and notify the Treasury Department.

The NCTC's Interagency Intelligence Committee on Terrorism includes the various lists in the National Intelligence Priorities Framework Counterterrorism Priorities rankings, which rank these organizations according to the level of threat they impose. Because FBI investigators and analysts can run a single search that would check all relevant lists, and because each list is developed according to different criteria to meet different needs, we do not believe it is necessary or productive to develop an additional list that would either consolidate these lists or establish yet another list according to a new set of criteria.

131. The 2005 FBI Uniform Crime Report shows a startling increase in violent crime, reporting the largest single-year percent increase in violent crime in fourteen years. The figures from the Midwest—and Wisconsin in particular—are especially troubling. While violent crime increased 2.3% overall at the national level, in the Midwest crime increased 5.6% and in Wisconsin it increased 15.8%. According to the Police Executive Research Forum, in many cities crime rates have continued to rise in the first six months of 2006. For example, according to its figures, in Milwaukee robberies are up 36% and aggravated assaults are up 31.6% in the first half of 2006.

a. Do you believe that these statistics accurately reflect what is happening in our communities, or is there another explanation for these statistics?

<u>Response</u>:

While the 2005 Uniform Crime Reports (UCR) indicate that violent crime has increased in some cities, it has decreased in others. Nevertheless, the FBI is concerned about any increases in violent crime and is actively working with its Federal, state, and local counterparts to address those increases.

b. Some argue that overall crime is still relatively low and that these statistics may not be the start of an overall trend. From your vantage point, do these numbers appear to be indicative of a longer term problem?

Response:

Overall crime is, by recent historical standards, still low, and it is very possible that recent UCR statistics are not indicative of a longer-term problem. It is simply too early to determine with any certainty whether this is the case. That said, the FBI is not waiting for the long-term picture to develop, but is instead aggressively responding to the recent crime statistics.

c. How is the FBI planning to respond to the rise in violent crime? Is the FBI going to expand or modify existing initiatives or launch any new initiatives?

Response:

Through partnerships with state, local, tribal, and other Federal law enforcement agencies, the FBI has achieved significant results in combating violent crime over the past several years. Since 1996, the collaborative efforts of the FBI's Violent Gang Safe Streets Task Forces (SSTFs) have resulted in 24,883 indictments and informations and 23,170 convictions. These results were achieved using the full range of investigative tools available to the FBI, including 122 undercover operations, 1,137 Title III wiretaps, and the use of racketeering laws in 1,872 indictments obtained in order to dismantle gangs by removing their leadership structure.

Part of the FBI's response to the rise in violent crime is to ensure there are no reductions in its current resource commitment to the highly productive partnerships that have led to these results. Task forces increase the effectiveness and productivity of limited personnel and logistical resources, avoid duplication of investigations, and expand the cooperation and communication among Federal and state law enforcement agencies. Currently, the FBI operates 33 violent crime SSTFs, 131 violent gang SSTFs, 16 "Safe Trails" task forces, and 23 child prostitution task forces.

Central to the FBI's response to the increase in violent crime is the expanded use of technology and of unique violent crime initiatives; FBI SAs and their law enforcement partners have collaborated to create tools to more efficiently use their limited resources. Significant successes have been achieved through the following initiatives.

1. Project Pin Point (PPP)

PPP is an analytical/intelligence tool created by the FBI's Philadelphia Division in conjunction with its partners in the Philadelphia Police Department, Judicial Warrant Squad, and others, to assist in violent crime investigations. PPP uses numerous layers of data sets, including arrest warrants from various law enforcement organizations, the addresses of registered sex offenders, and the locations of shootings and other violent crimes. The combined information identifies high crime areas, crime trends, intelligence gaps, and response capabilities that the FBI and local law enforcement can use in tailoring their tactics and resource allocation to most efficiently address an ever-changing crime threat. The FBI is now implementing this successful tool in additional FBI Field Offices.

2. Shot Spotter

Shot Spotter is an audio sensor system that uses portable sensors to detect and transmit sounds to software that determines their source and location. After detecting a gunshot, sensors send wireless signals through a Global Positioning System satellite to a home base computer that is set up in a strategic location, such as a command post or 911 center. The computer triangulates sensor input to locate the source of the shot, which it displays as a street address. Law enforcement officers are then able to respond quickly to the exact location of the gunshot and take immediate action. Thirteen American cities have deployed Shot Spotter and the FBI's Washington Field Office has deployed a system in cooperation with the Washington Metropolitan Police Department. The technology has resulted in the recovery of weapons and other evidence and has allowed emergency personnel to more quickly render aid to injured persons.

3. Violent Crime Wireless Intercept and Tracking Team (VC WITT)

The ability to track and locate cell phones in the possession of subjects and victims is an invaluable tool in solving abductions and other violent crimes, as well as in apprehending fugitives. VC WITTs were established to provide WITT equipment and to train SAs in the use of this equipment and the survey process.

4. Child Abduction Rapid Deployment Teams

In October 2005, the FBI created eight Child Abduction Rapid Deployment teams. Each team is regionally located to establish a nationwide rapid response capability in the hours immediately following a child abduction. These teams consist of experienced SAs who provide technological, analytical, behavioral, and investigative resources to resolve child abduction cases quickly. The FBI is working to ensure that each FBI Field Office has at least one SA trained specifically in child abduction matters.

5. Registered Sex Offender Locator Tool (ReSOLT)

ReSOLT is a database that maps the locations of registered sex offenders. This information is used, along with comparisons of this information to ChoicePoint records, to identify registered and unregistered sex offenders in the vicinity of a child abduction and to assist in identifying unregistered sex offenders.

132. At a crime summit held by the Police Executive Research Forum in August 2006, more than 50 cities were represented by mayors, police chiefs, and other public officials. Both during the summit and in the final report, a recurring theme was that these local officials believe that *hometown* security has been sacrificed to *homeland* security. In your written testimony, you tell us that the FBI shifted resources away from criminal investigative programs to support counterterrorism and counterintelligence efforts. As Senator Feinstein noted at the hearing, you are opening far fewer criminal cases and funding for criminal case agents has also decreased.

a. The FBI's counterterrorism capabilities are obviously critical in today's world, but how do we make sure the FBI does not neglect its traditional criminal justice priorities, especially in light of the increasingly urgent problem of violent crime?

Response:

The FBI has allocated its resources to ensure priorities are addressed in all its programs, including the criminal programs. We have established policies regarding resource allocation, we monitor resource use within each program to ensure that the most serious crime problems are addressed, and we ensure valid reasons exist for the diversion of resources from lower priority programs to higher priorities. The FBI remains committed to working alongside our Federal, state, and local law enforcement partners to effectively and aggressively investigate violent crime.

b. Similarly, are there ways that the federal government can help state and local authorities make their existing federal dollars go further?

Response:

The FBI has many investigative tools that local law enforcement can take advantage of to better use their Federal dollars, as do other Federal law enforcement agencies. Providing task force officers to FBI-led task forces allows state and local law enforcement departments to save in overtime pay and vehicle costs. A local department can avail itself of violent crime and gang crime analysis functions by sharing criminal intelligence and source development through the FBI's NGIC, FIGs, and the PPP initiative. In joint investigations, the FBI's Evidence Response Teams can be used to collect evidence so that forensic laboratory expenses, crime scene and court appearance overtime, and equipment usage costs are incurred by the Federal government. If a case warrants, state and local agencies use Federal resources such as WMD and Hazardous Materials response teams, bomb detection assets, wireless interception, and command post operations to augment investigative capabilities.

In addition to this investigative assistance, the Federal government can also sometimes provide direct financial assistance. For example, resources provided by DOJ's Asset Forfeiture Fund allow the FBI's Safe Streets Task Force (SSTF) initiative to reimburse state and local overtime, vehicle leases, and other equipment used by full-time Task Force Officers participating in SSTFs. In addition, on average 80% of all forfeited proceeds are returned to the state and local police departments that participated in the investigations leading to the forfeitures.

133. Senator Kohl raised with you the fact that cuts in federal funding for programs like COPS grants and juvenile justice and prevention programming have exacerbated our violent crime problem. These cuts also have contributed to the perception that the federal government has largely abandoned state and local law enforcement agencies in their fight to combat violent crime. Do you support increased federal funding for COPS and the Byrne/Justice Assistance Grant programs?

Response:

The FBI is not involved in funding decisions for either COPS or Byrne/Justice Assistance Grant programs and defers to DOJ with respect to this inquiry.

134. As you may know, this committee recently held an oversight hearing on the Department of Justice Civil Rights Division. At that hearing, we heard complaints that this administration has stepped back from vigorous enforcement of civil rights laws. According to the FBI website, the FBI's fifth-highest priority is to protect civil rights, yet your written testimony did not address what the FBI is doing in this area. What is the FBI doing to police civil rights violations?

Response:

The FBI conducts preliminary investigations of every credible civil rights allegation brought to its attention. No civil rights cases are unaddressed.

The mission of the FBI's Civil Rights Program (CRP) is to enforce Federal civil rights statutes and to ensure that civil rights are not abridged. The FBI's fifth priority is the CRP, behind only counterterrorism, counterintelligence, cyber crime, and public corruption. Approximately 152 FBI SAs address civil rights matters throughout the FBI's 56 Field Offices, a staffing level the FBI has maintained since 9/11 while other criminal program staffing levels have shrunk. FBI civil rights investigations resulted in 230 indictments and informations and 176 convictions in FY 2006.

The four CRP subprograms are hate crimes, "color of law," human trafficking, and Freedom of Access to Clinical Entrances (FACE) Act enforcement. In FY 2006, the FBI initiated 1,524 civil rights investigations. Hate crimes comprised 24% of this total, while "color of law" investigations made up approximately 62% of the total. The number of human trafficking investigations initiated increased from 3 in FY 1996 to 126 in FY 2006, and the proactive measures employed by field offices to address this crime problem are expected to result in continued increases. FACE Act violations comprise approximately 1% of all civil rights cases investigated by the FBI.

Law enforcement officers are more effective investigators when they understand the crimes they are investigating. In addition to their investigative responsibilities, FBI Field Offices are required to initiate and maintain liaison contacts and to provide training to state and local law enforcement organizations and the communities they serve. Civil Rights training is provided to new FBI SAs, experienced SAs in the field, and National Academy classes composed of law enforcement officers from around the country and the world. During FY 2006, the FBI's Civil Rights Unit (CRU) developed and initiated a PEI to provide training and program assistance to the field, sponsoring training for FBI supervisors, coordinators, and investigators that focused on the entire range of civil rights matters. During FY 2007, the CRU will again sponsor this type of civil rights training; eight PEI on-site visits will be conducted by CRU at various field offices.

Pursuant to a human trafficking initiative implemented in October 2005, FBI Field Offices conducted threat assessments, joined or established human trafficking task forces or working groups, and established contact with non-governmental organizations to address human trafficking issues. This initiative resulted in the opening of 126 human trafficking cases, 96 indictments and informations, and 65 convictions during FY 2006.

The FBI's Cold Case Civil Rights Era Initiative was designed to address previously unresolved civil rights cases. Pursuant to this initiative, FBI Field Offices worked with state and local authorities to identify, reopen, and expeditiously investigate unsolved and/or inadequately addressed hate crimes that occurred before 1970. Thirty-nine potential cases involving 51 victims have been identified; five of these cases meet the criteria for case initiation and are currently under investigation.

The FBI believes the excellent results produced by these initiatives demonstrates our commitment to the protection of civil rights. Following are some specific case examples of this commitment from 2006.

- Eight Houston, Texas, area subjects were indicted in December 2005 after recruiting and smuggling into the U.S. young females, including juveniles, from Honduras and El Salvador, then forcing them to work in Houston-area bars and restaurants. As of May 2006, 98 victims had been identified and five defendants had entered guilty pleas.

- Four members of the notorious "Avenues" Hispanic street gang in Los Angeles, California, were convicted in August 2006 of conspiring to violate the civil rights of African Americans who were assaulted or murdered for being on the gang's "turf." One victim was shot while waiting for a bus, and another was shot while looking for a parking space. All four defendants received life sentences.

- A San Antonio, Texas, couple received jail sentences in May 2006 for forced labor and human trafficking offenses. The 12-year-old victim was smuggled into the U.S. and forced to provide child care and perform domestic duties. She was hit, slapped, and kicked by the defendants, and not permitted to attend school.

- Norman Weslin, convicted of a FACE Act violation in 1996, was indicted for a FACE Act violation in May 2006 after being arrested by Bellevue, Nebraska, police for criminal trespass and obstruction in April 2006 at the Abortion and Contraceptive Clinic of Nebraska in Bellevue, Nebraska. He is awaiting trial.

- Officers from the Wilson County, Tennessee, Sheriff's Office engaged in a nearly two-year conspiracy to assault inmates, causing the death of one. They attempted to cover up their conduct by filing false reports and charges and by withholding medical care from their victims. A police sergeant was convicted of conspiracy against rights and deprivation of rights under color of law, including a finding of death resulting from failure to provide medical care, and sentenced to life in prison in July 2006.

- Jacob and Gabriel Laskey pled guilty to Federal hate crimes in August 2006 in relation to a 2002 incident in which the brothers threw rocks containing carved images of Nazi swastikas during evening services of the Temple Beth Israel in Eugene, Oregon, breaking two stained glass windows.

- Two Chattanooga Police Department officers were charged with conspiracy to violate civil rights in March 2006 and have agreed to plead guilty. The FBI began investigating in January 2006 after learning that wallets taken from members of the Latino community during routine traffic stops were missing cash when returned to them.

135. According to news reports, two U.S. citizens, Muhammad and Jaber Ismail, were denied entry into the U.S. for more than five months, forced to wait in Pakistan until they were cleared by the Department of Homeland Security. Both the *San Francisco Chronicle*, on August 26, 2006, and the *New York Times*, on August 28, 2006, reported that the

government would not allow the men back into the country unless and until they agreed to FBI interrogations in Pakistan. These articles indicated the FBI was directly involved in the matter and that FBI agents insisted at least one of the men take a polygraph test and allow himself to be interrogated without representation before either man would be cleared to return to the United States. The *New York Times* article also reported that the two men were not immediately informed as to why they were unable to enter the country, but instead were initially advised that there was a problem with their passports and then later told by the U.S. embassy in Pakistan that their inability to enter the country was a mistake. The *New York Times* story states that based upon the advice of the embassy, the two booked a second set of tickets to return to the U.S., only to be rebuffed at the airport again. Their lawyers allege that they were not contacted by the FBI until after their second attempt to return to the U.S., which itself was weeks after their original flight was to have left.

a. Are the allegations in these news reports true? Please specify any inaccuracies.

b. What, if any, was the extent of the FBI's involvement in this matter? Under what legal authority did it proceed?

c. Was the Ismails' entrance into the United States ever conditioned upon consent to interrogations without representation or on taking a polygraph test?

d. Why did it take five months to resolve this matter?

e. Have any charges been filed against Muhammad or Jaber Ismail?

f. Has the FBI ever been involved in a situation where a U.S. citizen is denied entry into the United States pending cooperation with FBI investigations?

<u>Response to subparts a through f</u>:

Pursuant to the longstanding DOJ policy against disclosing non-public information concerning pending law enforcement and litigation matters, we are unable to provide a response at this time.

136. The DOJ Inspector General's July 2005 report on the FBI's foreign language translation program indicates that the FBI's digital audio collection systems have limited storage capacity and that audio sessions are sometimes deleted or automatically archived to make room for new incoming audio sessions. While the report makes clear that no

unreviewed counterterrorism or Al Qaeda sessions had been deleted, it indicates that counterintelligence recordings are still being deleted and archived without first being reviewed. The report indicates, in fact, that six of eight offices tested deleted unreviewed counterintelligence materials. The report also states that once these sessions are archived it is difficult to determine whether the material has been reviewed.

a. Has the FBI acted on the recommendation from the Inspector General's office to establish controls to prevent unreviewed audio materials from being deleted, or is it still the practice that the FBI deletes some unreviewed counterintelligence materials?

b. What is the FBI doing to ensure that this does not continue to happen in the future?

Response to subparts a and b:

The FBI has acted on all of the suggestions of the July 2005 OIG report, and in October 2006 the OIG was satisfied with the FBI's progress and closed all action items. The FBI has focused a great deal of attention on improving the availability of all sessions in the digital collection systems and continues to look for ways to increase the time online for the sessions that it collects. The FBI has also remedied the problem through better guidance to system administrators, upgrading memory capacity and creating an "archive history" for all sessions removed from the system. Although unreviewed materials are still being removed from the online system, they are easily accessed and are still available in the archive. With additional linguists, the FBI has made significant progress in addressing a greater percentage of foreign language materials.

Questions Posed by Senator Schumer

137. As you confirmed to the Senate Committee on the Judiciary on December 6, 2006, only 33 of 12,000 FBI Special Agents are proficient in Arabic. Of these, only six have Arabic language skills rated "advanced proficiency."

a. Do you agree that for the FBI's counterterrorism work to be effective, more agents need to be proficient in Arabic?

b. In your view, what percentage and what number of the FBI's agents should be proficient in Arabic for the agency's counterterrorism work to be effective?

c. Can you commit to a date by which the FBI will have the percentage of Arabic-proficient agents needed for effectiveness in counterterrorism?

d. Please explain what specific steps, if any, the FBI is taking to raise the percentage of agents who have proficiency or advanced proficiency in Arabic.

Response to subparts a through d:

As we stated in our response to Question 68, above, the FBI's counterterrorism work has been extremely effective because of the synergies achieved between SAs, IAs, language analysts, and contract linguists. The FBI has 267 linguists who are proficient in Arabic and who support SAs by accompanying them to interviews and providing native knowledge of history, culture, religion, and geography. The interactions among these dedicated professionals has been highly productive.

As discussed in the responses to Questions 68 and 127, above, the FBI is also aggressively pursuing the recruitment and training of SAs and other professional staff who are proficient in Arabic and numerous other high priority foreign languages to enhance the FBI's ability to support its counterterrorism, counterintelligence, criminal, and international law enforcement outreach missions.

138. Earlier this year, the Inspector General reported that nearly 1 in 3 intelligence analyst positions at the FBI were not filled. The FBI was reportedly aiming to hire 880 new intelligence analysts by the end of this year, yet your testimony states that the FBI hired only 370 analysts in FY 2006.

a. How many intelligence analyst positions at the FBI remain to be filled, and can you commit to a date by which all of these positions will be filled?

Response:

The FBI has a funded staffing level of 2,579 IAs, with an onboard complement of 2,209 IAs. Currently, we have 66 new IAs who have completed the background process and are waiting to receive letters of appointment to the FBI. We anticipate bringing 33 of these IAs on board in February 2007. Additionally, 154 IA applicants are in our background investigation process, and we expect that this number will yield 75 to 80 new IAs, who will be eligible for hire in FY 2007. We are continuing our efforts to recruit and hire top-level candidates to the FBI and are working to develop new ways to attract these applicants to the specific job skills and backgrounds needed to fill our remaining vacancies through a targeted recruitment approach.

b. What percentage of intelligence analysts left FBI employment in FY 2006?

Response:

In FY 2006, the overall attrition rate of FBI IAs was 9%, including individuals who were removed, who retired, and who left the IA position but remained with the FBI. Excluding retirements and removals, the attrition rate for IAs leaving the FBI was 4.3%.

139. Depositions in a recent lawsuit filed by Bassem Youssef, the FBI's highest-ranking Arab-American agent, have revealed that many top FBI officials do not know the difference between Sunni and Shi'a Islam.

a. Do you think that top FBI officials should have a basic understanding of Islam and of Middle Eastern cultures?

b. What specific steps, if any, are you taking to remedy the current situation and to ensure that top FBI officials have a basic understanding of Islam and of Middle Eastern cultures?

Response to subparts a and b:

It is important that all investigators understand the dynamics that shape the terrorist threat facing our country. The FBI has made it a priority to ensure that our work force understands the bases of violent Islamic extremist ideologies, and has placed particular emphasis on understanding Muslim culture and the Islamic religion. This is evidenced by the counterterrorism and cultural training made available to our employees. This training teaches us to interact better with Muslim communities and to build the trust critical to effective community policing. Within the counterterrorism program, the provision to our counterterrorism workforce of the correct tools and relevant knowledge is one of our highest priorities. CTD's current senior leaders have acquired this familiarity through their daily work, their past interactions with Muslim communities during field assignments, and study in this area. These leaders are also knowledgeable regarding terrorists' operational methods and their criminal activities, neither of which depend on Islamic ideology. Because management and leadership qualities are as important as substantive expertise, it is also important that CTD managers come to their jobs with lengthy and in-depth experience managing high-profile investigative and intelligence efforts.

Since 9/11, the FBI's counterterrorism program has grown quickly and is the FBI's top investigative priority. This rapid growth has been fueled by a reallocation of our best investigators, managers, and leaders to the counterterrorism mission. We have also refocused our recruiting and hiring to attract individuals with skills critical to our counterterrorism and intelligence missions. These new recruits have included hundreds of IAs, translators, and SAs.

140. In April 2005, a Department of Justice Inspector General review of eight FBI field offices, conducted over three days, found that three of these offices failed to review their high-priority FISA interceptions within 24 hours.

a. Please state the FBI's current rule regarding how quickly FISA interceptions must be reviewed.

Response:

FBI policy is that FISA intercepts in the highest priority counterterrorism and counterintelligence cases (those in which the subject potentially presents a direct threat of violent terrorist activity) will be reviewed within 24 hours. Additional information in response to this inquiry is classified and is, therefore, provided separately.

b. Please describe what is entailed by such a review.

Response:

A review is completed when the linguist or analyst determines whether a session contains a threat to safety and/or security or contains actionable intelligence. If the reviewer determines there is a threat or actionable intelligence contained in the session, this information is immediately reported to parties that can act on the information.

c. Please explain what specific steps, if any, you are taking to clarify the rule on reviewing FISA interceptions and to ensure that field offices are abiding by this rule.

Response:

The FBI disseminated policy in 2004 and in 2006 reiterating the rule that a session is not considered reviewed until the threat information/actionable intelligence or lack thereof has been determined. This policy is reinforced through repeated FISA training.

141. As you know, the United Kingdom has a domestic agency, known as MI5, that is devoted to counter-intelligence and national security. Some have called for the creation of a similar agency in the United States.

a. Do you think that creating an agency like MI5 would make our domestic counterterrorism efforts more effective?

b. What would be the costs and benefits of using an MI5 model instead of our current counterterrorism model?

Response to subparts a and b:

In the more than 5 years since the attacks of 9/11/01, the FBI has evolved from a law enforcement agency focused on investigating crimes after the fact into an intelligence and law enforcement organization focused largely on preventing terrorist attacks. We have entered an era of unprecedented information sharing among the law enforcement and intelligence communities and we are continuing to build on our success in strengthening our intelligence capabilities. Experience has taught the FBI that there are no neat dividing lines distinguishing criminal, terrorist, and foreign intelligence activities. Criminal, terrorist, and foreign intelligence organizations and activities are often interrelated or interdependent. FBI files contain numerous examples of investigations in which information sharing between counterterrorism, counterintelligence, and criminal intelligence efforts and investigations was essential to the FBI's ability to protect the United States from terrorists, foreign intelligence activities, and criminal efforts. Some cases that begin as criminal cases become counterterrorism cases, and vice versa. The FBI must sometimes initiate parallel criminal and counterterrorism or counterintelligence cases to maximize the FBI's ability to identify, investigate, and address threats to the United States. Often, the success of these cases is entirely dependent on the free flow of information between the respective investigations, investigators, and analysts.

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 9/11/01, 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, etc.) 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 (9/11 Commission) and the report of the Commission on the Intelligence Capabilities of the United States Regarding WMD (WMD Commission) agree that the FBI should retain its domestic intelligence responsibility. Similarly, in its March 2005 report, "Transforming the FBI: Progress and Challenges," the NAPA Panel on FBI Reorganization 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 9/11/01. 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 NSB, which combines the capabilities, resources, and missions of the Counterterrorism Division, the Counterintelligence Division, and the Directorate of Intelligence under one leadership umbrella. The NSB will build on the FBI's strengths, ensure the integration of national security intelligence and investigations, promote the development of a national security workforce, and facilitate a new level of coordination with others in the Intelligence Community.

142. In September 2006, the Department of Justice Inspector General released a report concluding that the mail and phone calls of terrorists in American prisons are not being adequately monitored. The Inspector General recommended that the FBI "develop and reinforce procedures for interacting with the Bureau of Prisons regarding international terrorist inmates, including monitoring of inmates, intelligence gathering, and sharing of information and intelligence."

a. In order to resolve its recommendation to the FBI, the Office of the Inspector General asked that the FBI provide, by December 1, 2006, an update on the status of improvements to the FBI's Correctional Intelligence Initiative. Did the FBI provide this information to the IG by the deadline of December 1, 2006? Please provide me with a copy of this update on the Correctional Intelligence Initiative.

Response:

Attached as Enclosure E is the FBI's update regarding the status of completed and pending improvements regarding the Correctional Intelligence Initiative (CII), highlighting those enhancements or accomplishments that will directly assist the BOP.

b. What agency has the lead responsibility for preventing terrorist recruitment and investigating possible terrorist activity in federal prisons?

Response:

The NJTTF has the lead regarding terrorism matters in correctional institutions, including U.S. BOP facilities. The NJTTF directly addresses this tasking through the CII, which is designed to detect, deter, and disrupt efforts by terrorist or extremist groups to radicalize or recruit in Federal, state, and local prisons. All Federal prisons are directly included in the CII program, and BOP intelligence staff are primary partners in this nationwide initiative.

c. Do you think it would be helpful to establish a high-level task force to improve coordination between the FBI and BOP to address issues associated with individuals suspected and convicted of terrorism in federal custody? The current strategy of BOP participation on local Joint Terrorism Task Forces does not seem to be effective.

Response:

As discussed above, the NJTTF has the designated lead for addressing this issue and is taking active steps to continually expand and improve the CII program. These efforts include ensuring an effective intelligence partnership between the FBI and BOP both at the agency level, as well as at the local correctional institution level. This CII partnership between the FBI and BOP receives active executive support from both agencies, and BOP intelligence staff directly assigned to the NJTTF have comprehensive access to FBI information systems. Intelligence sharing protocols and FBI training for BOP intelligence staff are continually being improved. We believe the NJTTF is the correct "high-level task force" to directly address and manage this issue.

143. The DOJ Inspector General has reported that detention center personnel receive only a single page of information when a terrorist suspect is sent into their custody. In one shocking incident, staff at the Metropolitan Correctional Center in New York learned only from a news report that one of their inmates was a high-level al Qaeda operative trained in martial arts and urban warfare. What specific steps, if any, are you taking to improve information sharing between the FBI and BOP to ensure that the FBI is providing the BOP with the information that prison staff need to safely manage terrorist inmates?

Response:

Foremost in our efforts to ensure a fully effective intelligence partnership with the BOP is the comprehensive access to FBI intelligence information resources afforded BOP staff assigned to the NJTTF and to a number of local JTTFs. We have recently provided IA training to BOP intelligence staff, and we will continue to provide this training as appropriate. We are also in the process of developing additional instructions to all FBI field offices emphasizing intelligence sharing procedures with BOP facilities.

144. As you know, the FBI is also responsible for monitoring inmates who are under Special Administrative Measures (SAMs). Do you think that this fact creates a disincentive for agents to identify incoming terrorist suspects as needing SAMs or other restrictions?

Response:

We believe monitoring of inmates in Special Administrative Measures (SAM) status is actually very much to the advantage of SAs working related issues because SAM status eliminates many administrative burdens, such as those associated with seeking frequent subpoenas for inmate telephone calls and correspondence coverage.

145. I previously asked you about reports of FBI personnel's non-compliance with the Attorney General's guidelines on to confidential informants. To address these concerns, you pledged that new training would be implemented as a part of the Confidential Human Source Re-engineering Project by the fall 2006. Has that training been implemented? If not, please explain why and provide a deadline for when it will be implemented.

Response:

The formal training regarding the Confidential Human Source Re-engineering Project has not yet been implemented. For the past two years, the DI Human Source Re-engineering Team has worked to revise and simplify policies and processes associated with the management of confidential human sources. The principal results of this effort are the December 2006 AG Guidelines, consolidated FBI policy, and the Validation Standards Manual that flows from the AG Guidelines and ODNI validation standards. These extensively cross-referenced documents have been developed to standardize processes and ensure agency-wide compliance in terms of source management, operation, administration, and validation. Although we originally anticipated beginning training in the fall of 2006, we had to revise our training schedule because much of our time was devoted to revising the draft AG Guidelines. Only after the revised those Guidelines were signed in mid-December 2006 could detailed planning for the required training program begin. We plan to deliver this training beginning in April 2007.

The training phase of the DI's Re-engineering Project is being addressed by the Policy Implementation Team, which is composed of representatives from the FBI's Training and Development Division and DI, as well as contractors from the MITRE Corporation. The core team is augmented by an attorney from the FBI's OGC, an IA from the Criminal Investigations Branch, a member of the NSB's Communications Unit, and confidential file room personnel from the Washington Field Office. This team works in close coordination with a team representing the IT system (Delta) that is being designed in order to ensure consistency between the IT piece and the policy implementation piece and to facilitate the administration of the re-engineered source management processes.

The implementation plan includes Bureau-wide training for all employees (FBIHQ and the field) who are involved in human source matters. Most immediately, this plan proposes an initial three-day train-the-trainer conference on 4/15-27/07 (two consecutive sessions) for all Human Sources Coordinators and other confidential file room personnel. FBIHQ entities with a role in HUMINT will also be required to attend one of these sessions. The training is designed to be very interactive, consisting of an overview of the Human Source Re-engineering Project, presentations on the new and old AG Guidelines, a detailed presentation on the new validation standards policy and manual, inspection implications, and integrated case scenarios.

The newly trained trainers will be responsible for training personnel in their respective field offices and others who work with HUMINT (such as SACs, ASACs, Chief Division Counsel, and IAs) will receive revised blocks of instruction during management and program conferences. The New Agents Training curriculum is also being revised to accommodate training in this regard.

146. I note that your written responses to my questions from the May 2006 oversight hearing were submitted for clearance in July 2006. At that time, you stated that it was too early to determine the value of the FBI's new wInsight software tool to improve tracking of project costs.

a. Is the wInsight program now fully functional?

Response:

Yes. The wInsight software suite used by the FBI's Sentinel Program became fully operational in October 2006. Since then, wInsight has been available to multiple Sentinel managers to access data and analyze Sentinel's EVM performance through the FBI's unclassified intranet.

b. If yes, please state whether the wInsight tool is meeting the FBI's expectations and requirements for project cost tracking.

c. If it is not yet fully functional, when do you expect that it will be sufficiently implemented to determine whether the Inspector General's concerns have been resolved?

<u>Response to subparts b and c</u>:

The wInsight tool is meeting the FBI's expectations. The Sentinel EVM System includes wInsight as a primary EVM data collection and performance analysis tool. The Sentinel EVM system has proven to be an excellent means of capturing accrued costs and the value of work accomplished, months before they appear in an invoice from Lockheed Martin. This gives the FBI an early view into work accomplished versus work planned in terms of value associated with that work.

EVM data is briefed to the FBI Director weekly and to the DOJ's Department Investment Review Board monthly. EVM data is also provided at least quarterly to the eight Congressional committees and/or Subcommittees that have Sentinel oversight. In addition, as it becomes available, EVM data is provided to GAO auditors, DOJ's OIG, and DOJ EVM auditors.

147. The progress of the FBI's Sentinel case management system has been closely watched by the Senate Committee on the Judiciary, especially given the failure of the FBI's prior attempt to create such a system. The Inspector General's newest report on Sentinel, issued in December 2006, expressed continued concern that the cost of Sentinel in FY 2007 will force the FBI to reprogram funds intended for other purposes.

a. Do you expect this to happen?

b. If you do have to divert other funds to pay for Sentinel, how will that affect the FBI's ability to accomplish its mission?

<u>Response to subparts a and b</u>:

The FBI has determined that no reprogramming will be required for FY 2006 Sentinel operations. The funding requested in the President's FY 2007 budget will fund O&M for Phase 1 and most of the system development, training, and program management costs for Phase 2. If there are additional Phase 2 costs beyond the $100 million in the President's budget, the FBI will work with DOJ, OMB, and Congress to redirect existing funds where available or request additional funding as needed. Funding for Phases 3 and 4 and for the remainder of O&M for all Phases will be requested in future budget submissions. As noted in the response to the OIG, the FBI evaluates the operational impact of any proposed reprogramming and takes that impact into consideration in all reprogramming decisions. The FBI routinely provides this impact assessment and other relevant information to DOJ, OMB, and Congress.

148. The campaign season and midterm elections of November 7, 2006, were marred by many instances of wrongdoers cynically attempting, probably with some success, to intimidate or deceive voters headed to the polls. According to media reports, these attempts ranged from calls to Virginia voters wrongly telling them that they were not registered, to deceptive flyers distributed by the Ehrlich and Steele campaigns in southern Maryland, to an armed man who harassed Hispanic voters outside a polling place in Arizona. I believe that the Department of Justice should be using all available means to respond to these despicable tactics.

a. How many investigations, if any, is the FBI conducting that pertain to questionable or illegal tactics used during the midterm election of November 7, 2006 and the campaign season leading up to it?

Response:

Specific facts indicating that a violation has occurred are required in order for the FBI to initiate an investigation into allegations of election-related crimes. The initiation of each investigation must be supported by DOJ's Public Integrity Section, Election Crimes Branch, or the Criminal Section of the Civil Rights Division. As a result, the FBI does not initiate investigations related to "questionable" tactics; only allegations involving violations of applicable federal law. Between 1/1/06 and 11/30/06, the FBI opened 38 formal investigations involving alleged federal election law violations related to activity leading up to and surrounding the 11/7/06 election. These investigations encompass allegations of campaign finance violations, ballot fraud, voter intimidation, and voter fraud.

b. Please list all completed or ongoing FBI investigations, if any, into tactics used during the campaigns or elections of November 7, 2006, and for each case give the location and nature of the conduct being investigated.

Response:

Longstanding DOJ policy generally precludes the FBI from commenting on the existence or status of ongoing investigations. In addition to protecting the privacy interests of those affected, the policy serves to avoid disclosures that could provide subjects with information that might result in the destruction of evidence, witness tampering, or other activity that would impede the FBI's investigation.

The following election crime investigations related to the 11/7/06 national election were opened by the FBI on or after 1/1/06 and closed on or before 12/22/06.

- Diebold software theft: investigation by the Baltimore Division into the possible theft of Diebold Election Systems, Inc., electronic voting machine software.
- Ohio State Medical Association (OSMA) Political Action Committee (PAC) embezzlement: investigation by the Cincinnati Division regarding allegations of an $83,000 embezzlement from the OSMA PAC and related false filings with the Federal Election Commission.
- Lieberman "denial of service" website attack: investigation by the New Haven Division regarding allegations of an attempted "denial of service" attack on Senator Joseph Lieberman's official Internet website immediately prior to the Democratic primary in August 2006.
- Multiple voting referral (Galesburg, Illinois, Election Department): investigation by the Springfield Division of allegations of multiple voting by a specifically identified individual.
- Harrington felon voting: investigation by the Tampa Division of taunting letters from a convicted felon who claimed to be regularly voting, despite his previous disqualifying federal felony conviction.

c. Please explain why the FBI is not investigating the incident in which the Ehrlich and Steele campaigns in Maryland brought groups of people from Pennsylvania on November 7, 2006, and paid them to distribute fliers designed to create the false impression that Ehrlich and Steele are members of the Democratic party.

Response:

Longstanding DOJ policy generally precludes the FBI from commenting on the existence or status of ongoing investigations. In addition to protecting the privacy interests of those affected, the policy serves to avoid disclosures that could provide subjects with information that might result in the destruction of evidence, witness tampering, or other activity that would impede the FBI's investigation.

Questions Posed by Senator Durbin

CHALABI INVESTIGATION

149. In your written testimony you discussed the FBI's counterintelligence work, but there is one item of great interest to this Committee that you did not discuss – whether the FBI is investigating allegations that Administration officials leaked classified information to Ahmed Chalabi, and that Chalabi passed this information to Iran.

In November 2005, Mr. Chalabi visited the United States and met with a number of high-ranking Administration officials. At the time, Senator Leahy, Senator Kennedy and I wrote a letter to Attorney General Gonzales asking about the FBI's inquiry into Mr. Chalabi's alleged misconduct. In response, we received a January 24, 2006 letter stating, "Based on longstanding Department of Justice and Federal Bureau of Investigation policy, we generally do not confirm or deny the existence of investigations."

It is my understanding that, in the past, the Justice Department has confirmed to Congress and the public the existence of specific investigations, particularly if the matter under investigation if of great public significance. I hope you would agree that the allegations in question are very significant. The Department has also provided briefings on pending investigations to Senators and staff. If the mere existence of such an investigation is too sensitive for public release, this information can be provided in a confidential form.

a. Is the FBI investigating the alleged leak of classified information to Ahmed Chalabi, as well as the claim that Mr. Chalabi gave this information to Iran? If yes, can the FBI provide a briefing to me or my staff on the status of the investigation?

b. If there is an ongoing investigation, has the FBI interviewed Mr. Chalabi? If not, why did the FBI not interview Mr. Chalabi when he was in the U.S. in November 2005?

c. Was the FBI notified that Mr. Chalabi was visiting the U.S. in November 2005? If Mr. Chalabi is under investigation, do you think it was appropriate for high-ranking Administration officials to meet with him?

Response to subparts a-c:

The responses to these questions are classified and are, therefore, provided separately.

WAR CRIMES ACT

150. One provision of the recently-enacted Military Commissions Act retroactively revises the War Crimes Act.

a. Since 2001, has the FBI opened any investigations into alleged violations of the War Crimes Act?

Response:

A review of FBI records indicates that, since 2001, the FBI has opened seven investigations related to war crimes, as that term is used in the War Crimes Act (18 U.S.C. § 2441). Three of these cases have been closed and the other four remain open in varying states of investigation. None has reached the point of readiness for indictment regarding any war crime.

b. If so, will any of these investigations be affected by the retroactive revisions to the War Crimes Act in the Military Commissions Act?

Response:

Section 6 of the Military Commissions Act of 2006 amended the War Crimes Act (18 U.S.C. § 2441) in certain respects. Specifically, it amended the definition of "war crimes" to include conduct that constitutes, under specified circumstances, a grave breach of common Article 3 of the Geneva Conventions. (18 U.S.C. § 2441(c)(3).) It also added a new section, "Common Article 3 violations," that addresses common Article 3 treaty violations in detail. (18 U.S.C. § 2441(d).) Section 6 made most of those amendments retroactive to 11/26/97.

At this point, there is no indication that any of the above-referenced investigations will be affected by these amendments. All indications at this point are that the matters under investigation relate to facts that constitute offenses notwithstanding the amendments to the War Crimes Act.

RENDITION

151. According a recent *MSNBC* report, Col. Britt Mallow, the former commander of the Defense Department's Criminal Investigation Task Force, and Mark Fallon, the task force's chief investigator, claim that the FBI suggested sending a Guantanamo detainee "to another country, such as Egypt or Jordan, where he could be interrogated with techniques the FBI could not legally use." Is this report accurate?

<u>Response</u>:

We are not familiar with the MSNBC report referenced in the question, and we are unaware that any FBI employee suggested sending any detainee to another country where the detainee would be subject to interrogation techniques that the FBI could not use. To the contrary, the FBI employees who have been deployed to Guantanamo have been instructed that they are to use only techniques that could be used in the United States. No employee has reported any knowledge of FBI mistreatment of detainees. Moreover, the DOJ OIG is conducting an investigation of the FBI's treatment of detainees.

As to the particular incident referenced in the question, while we are not familiar with the MSNBC report, we are aware that Guantanamo-assigned FBI personnel specifically and expressly objected to the notion that a recalcitrant detainee could be removed to a foreign country so that the foreign country could use interrogation techniques that could not be used in Guantanamo.

ARAB-MUSLIM OUTREACH

152. According to "Building Trust, FBI 'At the Table' With Muslims," an article dated October 2, 2006, and posted on the FBI's website, "The FBI's Washington field office helped create an advisory council of Arab, Muslim, and Sikh leaders to improve relations with communities that might be helpful in the search for intelligence."

a. Please describe the activities of the advisory council.

<u>Response</u>:

The advisory council conducts meetings to discuss a range of issues including problem trends, hate crimes, and concerns about the USA PATRIOT Act. In addition to meetings being held at the Washington Field Office, discussions are also conducted at various mosques in the Washington Metropolitan area. The advisory council members have participated in conferences, forums, and town hall meetings to discuss issues and develop best practices in the community, and the FBI has realized investigative gains as a result of these interactions.

b. How often does the advisory council meet?

<u>Response</u>:

The advisory council meets on a bi-monthly basis.

c. When was the most recent time the advisory council met?

<u>Response</u>:

The most recent meeting occurred on 1/11/07.

d. Has the FBI established other advisory councils in other areas, especially those with large Arab, Muslim, and South-Asian American populations?

<u>Response</u>:

In addition to the Washington Field Office, Multi-Cultural Advisory Committees (MCACs) have been established by the FBI's Baltimore, Charlotte, Los Angeles, and New York Divisions.

153. How many times have you met with Arab, Muslim and South-Asian American community leaders since 9/11? When was your most recent meeting?

<u>Response</u>:

FBI officials have met frequently with community leaders at both the national and local level since the attacks of 9/11/01. Twice a year the FBI Director meets with national leaders from the Arab, Muslim, Sikh, and South Asian American communities. These national leaders also meet quarterly with the AD of the FBI's Office of Public Affairs (OPA) and with the Community Relations Unit. In addition to face-to-face meetings, conference calls are held periodically.

The national community leaders have also communicated via secure video teleconference with the Community Outreach Specialists and Media Coordinators in all 56 FBI field offices regarding FBI media operations and identified how FBI field offices can contact local organizations in this community when issues involving their constituencies arise. As a result of these exchanges, the value and frequency of dialogue has improved both nationally and locally.

The most recent meeting between the FBI's OPA AD and national leaders from the Arab, Muslim, Sikh, and South Asian American communities occurred via conference call on 1/10/07. During this call, the parties established what was expected from both the FBI and the various community leaders during 2007.

The Director and members of his executive staff, including the OPA AD, also met with national leaders from the American-Arab and Muslim communities on 11/1/06 to discuss expanding the FBI's partnership with the Arab-American/ Muslim community. As a result of that meeting, national leaders are in the process of developing a strategy to encourage community members at the local level to participate in more Citizen's Academies. The FBI has also been in discussion with the Vice President of the Islamic Society of North America to schedule tours and cultural training for FBI SAs at the All Dulles Area Muslim Society Center and to coordinate the introduction of the Community Executive Seminar Training program to the local organizations by the national leaders.

At the local level, FBI Field Office SACs and Division Community Outreach Specialists meet regularly with local community leaders. Field offices engage with these leaders in face-to-face meetings, conference calls, and town hall meetings to discuss issues and develop best practices in the community. Through these frequent interactions, partnerships have developed and have resulted in the creation of advisory committees. FBI field offices such as the Los Angeles Division and Washington Field Office have established MCACs that consist of community leaders from a variety of cultural and religious backgrounds. The MCACs reach out to the communities most impacted by 9/11 and assist in educating them about the FBI's mission and in dispelling misconceptions about the FBI. The MCACs also educate the FBI about their cultures and the issues most important to them.

FBI FOREIGN LANGUAGE ABILITIES

154. On March 10, 2004, I sen[t] you a letter requesting information about the FBI's foreign language abilities. In response, I received an April 19, 2004 letter from Special Agent Roderick Beverly, which I have attached. I would appreciate an update.

a. Attachment A to the 4/19/04 letter is a chart entitled "FBI Foreign Language Resources." Please provide an updated version of this chart.

<u>Response</u>:

Please see our response to Question 16, which includes the updated chart (provided as Enclosure A).

b. On page 6 of the 4/19/04 letter, in response to question #8, Mr. Beverly mentions a number of initiatives to provide advanced Arabic training for Special Agents, including, Middlebury College, the Department of State's Foreign Service Institute, and a pilot program at the University of Jordan in Amman. Please provide an update on these initiatives. How many FBI Special Agents have received training in each of these programs?

<u>Response</u>:

A total of 124 SAs have received training in the programs mentioned in Mr. Beverly's letter. In FY 2004, eight SAs attended Middlebury College's Arabic summer immersion program and another 39 received survival or full-time Arabic training at commercial language schools. In FY 2005, two SAs attended Middlebury's Arabic program, and another 41 received survival or full-time training. In FY 2006, four SAs attended Middlebury, and 30 received survival or full-time training. For FY 2007, seven SAs have submitted applications to attend Middlebury, and 65 have applied for survival, full-time, or maintenance training in Arabic. Twelve of these applications are for training at the Foreign Service Institute. Approval of these training requests will depend on available funding.

A pilot six-week pilot program was held at the University of Amman in Jordan in the spring of 2004 to help two SAs develop higher levels of proficiency in Arabic. While the pilot was successful, subsequent events in Jordan have prevented us from continuing this training.

Since Mr. Beverly's letter, the FBI has made additional efforts to raise the number of SAs who have working proficiency in Arabic. Please see our response to Question 127, above, for more information on those efforts.

c. On pages 6-7 of the 4/19/04 letter, in response to question #9, Mr. Beverly indicates that the FBI is developing five Listening Summary Translations Examinations and a Verbatim Translation Examination. Please provide an update.

Response:

Listening Summary Translation Exams in Farsi and five Arabic dialects (Egyptian, Iraqi, Levantine, Algerian, and Yemeni) were completed in FY 2005 and are being administered to SA applicants. Verbatim Translation Examinations in 16 languages (including Arabic, Farsi, Hindi, Turkish, Pashto, and Urdu) have been available since FY 2005 and are administered to individuals applying for translator positions.

FBI COMPUTER CAPABILITY: SENTINEL FUNDING

155. I read with interest and concern various news accounts in early December describing uncertain funding circumstances for developing and deploying the FBI's Sentinel desktop case management system. While I am optimistic that this project for achieving the long-delayed Virtual Case File capability is proceeding on solid footing, the potential consequences of funding shortfalls on achieving expected milestones, remaining on schedule, and keeping costs within budget are troubling.

I understand the FBI needs $150 million in FY 2007 to continue the Sentinel project. I note that previously the FBI obtained permission to use $97 million from its fiscal 2005 budget for the Sentinel program, including about $29 million from its counter-terrorism division, intelligence-related activities and its cyber division. I share the concerns expressed that diverting substantial funds from such mission-critical areas could begin eroding the FBI's operational effectiveness.

A recent Justice Department Inspector General report (Audit Report 07-03; December 2006) explained that in addition to the $100 million for Sentinel in the President's 2007 budget request, the FBI would need an additional $56.7 million to bridge the gap between requested funds and FY 2007 requirements. Concern was expressed that an FY 2007 appropriation of less than $100 million could result in an unprecedented level of reprogramming of FBI resources to fund Sentinel.

a. As the Sentinel project proceeds, what are the implications for achieving expected milestones and for meeting financial obligations if 2007 funding is not in place and operations are governed by a continuing funding resolution?

Response:

Please see our response to Question 9, above.

b. Is additional fund reprogramming being contemplated to secure the $57 million? What are the specific sources of the funds you have identified that would be drawn upon to address the shortfall? What impact would that effort have on meeting other critical mission capabilities and operational priorities?

Response:

Please see the response to Question 65b, above.

c. What contractual problems would the FBI encounter in the Sentinel development effort if sufficient funding levels are not available? What contingency plans are in place to mitigate any schedule slippage? Are there cost implications of any delays in the project?

Response:

Please see the response to subpart a, above.

FBI/DHS Fingerprint Database Integration

156. As we mark over a decade since integration of the IAFIS (FBI) and IDENT (INS, now DHS) databases was initially urged by Congress (and over 15 years since these two databases were originally conceptualized) how realistic is it today that the goal is within reach?

I was pleased to review the July 2006 report of the Inspector General indicating that reconciliation of the divergent fingerprint systems (2-print vs. 10-print) had finally been accomplished. It appears, however, that we still lack full integration, and may not achieve full integration until December 2009.

a. What is the current status of the integration effort between the fingerprint databases of the FBI's IAFIS system and Homeland Security's IDENT system?

__Response__:

The FBI, DHS, and DOS have agreed to pursue interoperability, forming a multi-agency Interoperability Integrated Project Team that has developed a program to demonstrate that enhanced interoperability of existing systems can be achieved. Part of this program focuses on a reciprocal exchange of data subsets pursuant to a shared data prototype called the interim Data Sharing Model (iDSM), which allows each agency to hold a read-only copy of fingerprint images from the other agency and to perform biometric-based searches of the other agency's data. On 9/3/06 the iDSM was successfully deployed with over a million fingerprint images and plans to add additional data sets. Practical success was demonstrated on 10/18/06 and 10/22/06, when the Boston Police Department used iDSM to identify arrest subjects as individuals also of interest to ICE, which issued detainers on these subjects. The Dallas County Sheriff's Office, which initiated the use of iDSM on 11/1/06, has also identified arrest subjects as of interest to ICE, and detainers were additionally issued on these subjects.

b. What is the prognosis for achieving fuller integration and cross-matching capabilities between IDENT and IAFIS?

__Response__:

While agencies are working to enhance the interoperability of existing systems through activities such as the iDSM for short-term gains, they are concurrently making longer-term plans for future systems. Through the National Science and Technology Council's Subcommittee on Biometrics, the FBI is leading a multi-agency process to develop a "system of systems" framework that aims to enhance both interoperability and privacy protection. This framework is driving multi-agency plans for upcoming RDT&E standards and privacy activities and will provide the foundation for agencies as they design their next generation systems, such as the FBI's Next Generation Identification (NGI) multi-biometric system.

c. Are there steps that could be taken to expedite the integration? If so, please describe. If not, please explain.

__Response__:

Past and ongoing efforts of the NSTC Subcommittee on Biometrics have improved core biometric technologies so that enhanced integration is becoming possible. The Subcommittee's more recent interoperability efforts were initiated to expedite the planning and implementation of future, better integrated, systems. The FBI will also continue to enhance its existing system for short-term interoperable gains, such as improving IAFIS response times for civil submissions from US-VISIT and DOS. The full interoperability of IDENT/IAFIS will be delivered using an incremental approach, with benefits to state and local law enforcement and national security being realized each year.

NATIONAL INSTANT CRIMINAL BACKGROUND CHECK SYSTEM FAILURE

157. As we mark over a decade since integration of the IAFIS (FBI) and IDENT (INS, now DHS) databases was initially urged by Congress (and over 15 years since these two databases were originally conceptualized) how realistic is it today that the goal is within reach?

Response:

Please see the response to Question 156, above.

158. News reports in early December 2006 revealed that the National Instant Criminal Background Check System operated by the FBI to quickly screen gun buyers' backgrounds for criminal activity crashed several times over a two day span. This system generally receives between 30,000 and 50,000 requests for background checks on a daily basis and processes the requests within 30 minutes. It was on the blink for up to a half-hour at times. An FBI spokesman blamed a technical glitch for the problem. It was unclear when it would be fixed.

According to the media accounts, "the outages potentially allowed people to buy firearms without being screened if sellers gave up on making the required check." It is my understanding that no firearms were sold during the periods the system was malfunctioning.

a. Please confirm my understanding about the lack of any sales during the periods that the system was malfunctioning.

Response:

Please see the response to Question 75b, above.

b. What policies are in place and used to ensure that a system failure does not allow Federal Firearms Licensees to dispense with the obligation to run the mandatory check in advance of completing a sales transaction? What directives or other guidance are provided to Federal Firearms Licensees for handling transactions when the electronic system is inaccessible?

Response:

18 U.S.C. § 922(t)(5) provides that a licensee who knowingly transfers a firearm and knowingly fails to comply with the provisions of Section 922(t)(1) with respect to the transfer may be subject to the revocation or suspension of the license for up to six months and a civil fine of not more than $5,000. Federal law (18 U.S.C. § 922(t)(1)) and regulation (27 C.F.R. § 478.102) prohibit Federal Firearms Licensees from transferring firearms without contacting the NICS. Pursuant to 28 C.F.R. § 25.6(i), federal firearms licensees "are required to record the system response, whether provided by the FBI NICS Operations Center or a [point of contact], on the appropriate ATF form for audit and inspection purposes, under 27 C.F.R. Part 178 record keeping requirements. The FBI NICS Operations Center will always include an NTN and associated 'Proceed,' 'Delayed,' or 'Denied' determination."

c. What preventative steps have been instituted to reduce the frequency of systems failures? Are other initiatives in progress or being planned to help limit the likelihood of system shutdown? Are there remedial backups in place to address problems such as the one recently experienced?

Response:

Please see the responses to Questions 75c and 112, above.

ENCLOSURE A

QUESTION 16

THE FBI'S
FOREIGN LANGUAGE RESOURCES

As of 12/31/2006 Attachment to question # 137.

FBI Foreign Language Resources

Language	On-Board as of 04/15/2004			Hired in FY 2004			Hired in FY 2005			Hired in FY 2006			Hired in FY 2007 (YTD) (As of 12/31/2006)			Current On-Board Resource			Projected to Yet Hire in FY07, Jan 1 - Sep 30 **		
	SALP	LA	CLP	SALP	LA	CLP	SALP	LA	CLP	SALP	LA	CLP	SALP	LA	CLP	SALP	LA	CLP	SALP %	LS	CLP
Arabic	21	65	151	3	12	20	4	9	19	0	17	62	1	13	23	35	95	172	0	2	6
Farsi	10	13	45	2	1	6	0	0	5	1	6	11	0	1	4	0	18	49	0	1	2
Hindi	0	4	6	0	0	3	0	0	10	0	3	3	0	0	0	0	6	8	0	0	0
Kurdish	0	0	6	0	0	4	0	0	1	0	0	1	0	0	0	0	0	4	0	1	0
Pashto	0	1	7	0	0	1	0	0	3	0	0	1	0	0	0	0	0	7	0	0	0
Turkish	0	1	9	0	0	8	0	0	2	0	2	2	0	0	1	1	2	8	0	2	1
Urdu/Punjabi	0	7	21	3	1	7	2	0	9	0	3	11	0	6	4	1	13	33	0	1	2
Total Hired: Middle Eastern Languages Listed Above	31	91	245	8	14	49	6	9	49	1	31	91	1	20	32	37	134	281	0	7	11
Total Hired: All Languages	-	-	-	124	30	120	108	15	181	69	112	205	1	55	78	-	-	-	-	45	25
Total On-Board: All Languages *	**1196**	**408**	**820**	**-**	**387**	**835**	**1662**	**372**	**944**	**1442**	**448**	**821**	**-**	**-**	**-**	**1476**	**487**	**888**	**1476**	**532**	**913**

* Note that the total of On-Board linguists does not necessarily equal the total of the previous year plus the number hired due to attrition.
SALP = Special Agents Language Program
LA = Language Analysts
CLP = Contract Linguist Personnel

% Estimate unknown

** NOTE that due to current budget and and hiring uncertainties, these numbers are only estimates.

ENCLOSURE B

QUESTION 58

5/19/04 ELECTRONIC COMMUNICATION
SUBJECT: TREATMENT OF
PRISONERS AND DETAINEES

(Rev. 01-31-2003)

Serial 86
m mcr

FEDERAL BUREAU OF INVESTIGATION

Precedence: PRIORITY **Date:** 05/19/2004

To: All Divisions **Attn:** ADIC
AD
DAD
SAC
CDC

From: General Counsel
Contact: Donald Klein (202) 324-0605

Approved By: Pistole John S
Caproni Valerie E

Drafted By: Klein Donald J
Matsumoto Lisa K

Case ID #: (U) 66F-HQ-A1258990

Title: (U) Treatment of Prisoners and Detainees

Synopsis: (U) In light of the widely publicized abuses at the Abu Ghraib prison, Iraq, this EC reiterates and memorializes existing FBI policy with regard to the interrogation of prisoners, detainees, or persons under United States control (collectively "detainees"). These guidelines serve as a reminder of existing FBI policy that has consistently provided that FBI personnel may not obtain statements during interrogations by the use of force, threats, physical abuse, threats of such abuse or severe physical conditions. In addition, this EC sets forth reporting requirements for known or suspected abuse or mistreatment of detainees.

Details: (U) FBI personnel posted abroad come into contact with detainees in a variety of situations. Persons being detained or otherwise held in the custody of the United States are entitled to varying levels of procedural rights depending upon their situation or category of detention (*e.g.*, unlawful combatant, prisoner of war). Although procedural rights, such as <u>Miranda</u> rights, do not apply in all situations overseas, certain minimum standards of treatment apply in all cases.

Applicability: (U) FBI personnel and personnel under FBI supervision deployed in Iraq, Guantanamo Bay, Cuba, Afghanistan or any other foreign location where similar detention and interrogation issues arise are to follow FBI policies and guidelines for the treatment of detainees.

FBI Policy: (U) "It is the policy of the FBI that no attempt be made to obtain a statement by force, threats, or promises." FBI Legal Handbook for Special Agents, 7-2.1 (1997). A person's status determines the type and extent of due process rights accorded by the FBI, such as right to counsel or advisement of rights. Regardless of status, all persons interrogated or interviewed by FBI personnel must be treated in accordance with FBI policy at all times. It is the policy of the FBI that no interrogation of detainees, regardless of status, shall be conducted using methods which could be interpreted as inherently coercive, such as physical abuse or the threat of such abuse to the person being interrogated or to any third party, or imposing severe physical conditions. *See*, FBI Legal Handbook Section 7-2.2.

Joint Custody or Interrogation: (U) FBI personnel who participate in interrogations with non-FBI personnel or who participate in interrogations of persons detained jointly by FBI and non-FBI agencies or entities shall at all times comply with FBI policy for the treatment of persons detained. **FBI personnel shall not participate in any treatment or use any interrogation technique that is in violation of these guidelines regardless of whether the co-interrogator is in compliance with his or her own guidelines**. If a co-interrogator is complying with the rules of his or her agency, but is not in compliance with FBI rules, FBI personnel may not participate in the interrogation and must remove themselves from the situation.

Reporting of Violations: (U) If an FBI employee knows or suspects non-FBI personnel has abused or is abusing or mistreating a detainee, the FBI employee must report the incident to the FBI on-scene commander, who shall report the situation to the appropriate FBI headquarters chain of command. FBI Headquarters is responsible for further follow up with the other party.

LEADS:

Set Lead 1 (INFO)

ALL RECEIVING OFFICES

(U) Distribute to all personnel.

Set Lead 2 (INFO)

COUNTERTERRORISM

AT WASHINGTON, DC

(U) To be distributed to all FBI personnel who are now, or in the future are, detailed to Iraq, Guantanamo Bay, Cuba, or Afghanistan or other foreign locations in which similar detention and interrogation issues may arise.

♦♦

Enclosure C

Question 88

The Attorney General's Guidelines Regarding the Use of FBI Confidential Human Sources

THE ATTORNEY GENERAL'S GUIDELINES REGARDING THE USE OF FBI CONFIDENTIAL HUMAN SOURCES

TABLE OF CONTENTS

I. GENERAL PROVISIONS

A. PURPOSE AND SCOPE

1. The purpose of these Guidelines is to set policy for all Department of Justice (DOJ) personnel regarding the use of all Confidential Human Sources, as further defined below, that are operated by the Federal Bureau of Investigation (FBI) in any of the FBI's investigative programs or other authorized information collection activities.

2. These Guidelines are issued under the authority of the Attorney General as provided in Title 28, United States Code, Sections 509, 510, and 533.

3. These Guidelines are mandatory and supersede: the Attorney General's Guidelines Regarding the Use of Confidential Informants (May 30, 2002), to the extent that they apply to the FBI; the Attorney General Procedure for Reporting and Use of Information Concerning Violations of Law and Authorization for Participation in Otherwise Illegal Activity in FBI Foreign Intelligence, Counterintelligence or International Terrorism Intelligence Investigations (August 8, 1988), to the extent that it applies to assets; and the Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection (October 31, 2003) ("NSIG"), to the extent that they are inconsistent with these Guidelines.[1] These

[1]However, techniques whose use is authorized for validating assets, as outlined in the Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection, to identify potential assets, to collect information to maintain the cover or credibility of assets, or to validate assets (including determining suitability or credibility) may continue to be utilized in relation to Confidential Human Sources in connection with activities related to threats to the national security.

Guidelines do not supersede otherwise applicable ethical and legal obligations of Department of Justice attorneys, which can, in certain circumstances (for example, with respect to contacts with represented persons), have an impact on FBI conduct.

4. These Guidelines apply to the use of a Confidential Human Source in a foreign country only to the extent that the Confidential Human Source is reasonably likely to testify in a domestic case.

5. These Guidelines do not limit the ability of the FBI to impose additional restrictions on the use of Confidential Human Sources.

6. All DOJ personnel have a duty of candor in the discharge of their responsibilities pursuant to these Guidelines.

7. These Guidelines shall be effective 180 days after they are approved by the Attorney General. However, to the extent provided in FBI policy: (i) activities commenced under pre-existing guidelines may be continued and completed in conformity with such pre-existing guidelines, notwithstanding the approval by the Attorney General and effectiveness of these Guidelines, and (ii) restrictions on the use of human sources under pre-existing guidelines which are not perpetuated by these Guidelines need not be observed following the Attorney General's approval of these Guidelines, even in relation to activities commenced under pre-existing guidelines, if the requirements of these Guidelines for such activities are satisfied. To the extent that paragraph III(A)(3)(f) cannot be fully implemented within 180 days, the FBI and the National Security Division will establish a protocol to

govern the review of sources who would otherwise be subject to that paragraph. The FBI shall adopt such measures as may be needed to effect an orderly and expeditious transition to the new Guidelines, without disruption or impediment to ongoing activities within their scope. The FBI shall keep the Deputy Attorney General, the Assistant Attorney General of the Criminal Division, and the Assistant Attorney General for National Security informed of such measures as directed by the Deputy Attorney General.

B. DEFINITIONS

1. "Special Agent in Charge" or "SAC" – the FBI Special Agent in Charge of an FBI Field Office (including an Acting Special Agent in Charge), except that the functions authorized for Special Agents in Charge by these Guidelines may also be exercised by the Assistant Director in Charge in an FBI Field Office headed by an Assistant Director, and by FBI Headquarters officials designated by the Director of the FBI.

2. "Federal Prosecuting Office" or "FPO" – any of the following Department of Justice components:

    a. The United States Attorneys' Offices;

    b. The Criminal Division;

    c. The National Security Division ("NSD");

    d. Any other litigating component of the Department of Justice with authority to prosecute federal criminal offenses, including the relevant sections of the Antitrust Division, Civil Division, Civil Rights Division, Environmental and Natural Resources Division, and the Tax Division.

3. "Chief Federal Prosecutor" or "CFP" – the head of an FPO.

4. "FPO Attorney" – an attorney employed by, or working under the direction of, an FPO.

5. "Confidential Human Source Coordinator" – a supervisory FPO Attorney designated by the CFP to facilitate compliance with these Guidelines.

6. "FPO participating in the conduct of an investigation" – any FPO employing or directing an FPO Attorney assigned to a matter whose approval is necessary pursuant to these Guidelines, or whose approval was sought or obtained regarding any investigative or prosecutorial matter including the issuance of a search or arrest warrant, electronic surveillance order, subpoena, indictment or other related matter.

7. "Confidential Human Souree" – any individual who is believed to be providing useful and credible information to the FBI for any authorized information collection activity, and from whom the FBI expects or intends to obtain additional useful and credible information in the future, and whose identity, information or relationship with the FBI warrants confidential handling.

8. "Senior Leadership Source" – a Confidential Human Source who is in a position to exercise significant decision-making authority over, or to otherwise manage and direct, the unlawful activities of the participants in a group or organization involved in unlawful activities that are:

a. nationwide or international in scope; or

b. deemed to be of high significance to the FBI's criminal investigative priorities, even if the unlawful activities are local or regional in scope.[2]

9. "High-Level Government or Union Source" – a Confidential Human Source who is either (a) in relation to the federal government or the government of a state, the chief executive, the official next in succession to the chief executive, or a member of the legislature, or (b) a president, secretary-treasurer or vice president of an international or national labor union or the principal officer or officers of a subordinate regional entity of an international or national labor union.[3]

10. "Tier 1 Otherwise Illegal Activity" — any activity that:

a. would constitute a misdemeanor or felony under federal, state, or local law if engaged in by a person acting without authorization; and

b. that involves -

(i) the commission, or the significant risk of the commission, of any act of violence by a person or persons other than the Confidential Human Source;[4]

---

[2]Such organizations shall include, but are not limited to: any La Cosa Nostra Family, Eurasian Organized Crime Group, or Asian Criminal Enterprise which is recognized by FBI Headquarters; and any domestic or international Terrorist Organization, which is recognized by FBI Headquarters.

[3]The term "regional entity" shall not include a local union or a group of local unions, such as a district council, combined together for purposes of conducting collective bargaining with employers.

[4]Bookmaking that is significantly associated with, or substantially controlled by, organized crime ordinarily will be within the scope of this definition. Thus, for example, where bookmakers have a financial relationship with members or associates of organized crime, and/or

(ii) corrupt conduct, or the significant risk of corrupt conduct, by an elected public official or a public official in a high-level decision-making or sensitive position in federal, state, or local government;

(iii) the manufacturing, importing, exporting, possession, or trafficking of controlled substances in a quantity equal to or exceeding those quantities specified in United States Sentencing Guidelines § 2D1.1(c)(1);

(iv) financial loss, or the significant risk of financial loss, in an amount equal to or exceeding those amounts specified in United States Sentencing Guidelines § 2B1.1(b)(1)(I);[5]

(v) a Confidential Human Source providing to any person (other than an FBI agent) any item, service, or expertise that is necessary for the commission of a federal, state, or local offense, which the person otherwise would have difficulty obtaining; or

(vi) a Confidential Human Source providing to any person (other than an FBI agent) any quantity of a controlled substance, an explosive, firearm, or

---

use members or associates of organized crime to collect their debts, the conduct of those bookmakers would create a significant risk of violence, and would therefore fall within the definition of Tier 1 Otherwise Illegal Activity.

[5]The citations to the United States Sentencing Guidelines (USSG) Manual are to the 2005 Edition. The references herein to particular USSG Sections are intended to remain applicable to the most closely corresponding USSG level in subsequent editions of the USSG Manual in the event that the cited USSG provisions are amended. Thus, it is intended that subsection (iii) of this paragraph will remain applicable to the highest offense level in the Drug Quantity Table in future editions of the USSG Manual, and that subsection (iv) of the paragraph will remain applicable to dollar amounts that, in future editions of the USSG Manual, trigger sentencing enhancements similar to that set forth in the current section 2B1.1(b)(1)(I). Any ambiguities in this regard should be resolved by the Assistant Attorney General for the Criminal Division.

other dangerous weapon, or other item that poses an immediate and significant threat to public safety, with little or no expectation of its recovery by the FBI.

11. "Tier 2 Otherwise Illegal Activity" - any other activity that would constitute a misdemeanor or felony under federal, state, or local law if engaged in by a person acting without authorization.

12. "Fugitive" – an individual:

    a. for whom a federal, state, or local law enforcement agency has placed a wanted record in the FBI's National Crime Information Center (other than for a traffic or petty offense); or

    b. for whom a federal warrant has been issued; and

    c. for whom the law enforcement agency is willing, if necessary, to seek his or her extradition to its jurisdiction.

13. "Human Source Review Committee" or "HSRC" – A committee convened pursuant to these Guidelines to review various matters under these Guidelines as set forth below in paragraph III (A).

14. "National Security Investigation" – A national security investigation as defined in Part VIII.Q of NSIG.

15. "International Terrorism Investigation" – An investigation relating to international terrorism, whether conducted under NSIG, under the Attorney General's Guidelines on General Crimes, Racketeering Enterprise and Terrorism Enterprise

Investigations (May 30, 2002), or under other guidelines issued by the Attorney General.

C. PROHIBITION ON COMMITMENTS OF IMMUNITY BY THE FBI

The FBI does not have any authority to make any promise or commitment that would prevent the government from prosecuting a Confidential Human Source for criminal activity that is not authorized pursuant to Section V below or that would limit the use of any evidence by the government, without the prior written approval of the FPO that has primary jurisdiction to prosecute the Confidential Human Source for such criminal activity. An FBI Agent must exercise due diligence to avoid giving any person the erroneous impression that he or she has any such authority.

D. MAINTAINING CONFIDENTIALITY

1. Obligation

DOJ Personnel have an obligation to maintain as confidential the identity of any Confidential Human Source. Consistent with that obligation, DOJ personnel shall not disclose the identity of a Confidential Human Source or information that Source has provided that would have a tendency to identify the Source unless disclosure is appropriate under one of the exceptions referenced below in paragraph D (4).

2. Security of Material

If the FBI provides DOJ personnel with any material containing:

a. the identity of a Confidential Human Source;

b. information that may possibly identify the Source; or

c. information that the Source has provided;

such material must be secured in a manner consistent with its security markings or classifications, when not in the direct care and custody of DOJ personnel.

3. **Continuing Obligation**

DOJ personnel have a continuing obligation after leaving employment with the Department of Justice to maintain as confidential the identity of any Confidential Human Source and the information that Source provided, unless disclosure is appropriate under one of the exceptions referenced below in paragraph D (4).

4. **Exceptions**

a. Notwithstanding paragraph I (D) (1), DOJ personnel may make appropriate disclosures:

i. to FBI Agents who need to know the identity of the Source in order to perform their official duties. However, an FPO must coordinate with the FBI Agent directing the Source to obtain the required approval of the FBI-SAC or his or her designee prior to such disclosure;

ii. to other law enforcement, intelligence, immigration, diplomatic, and military officials who need to know the identity to perform their official duties, subject to the prior approval of the FBI-SAC or his or her designee;

iii. when the Confidential Human Source has agreed to testify in a grand jury or judicial proceeding.

b. All DOJ personnel must disclose the identity of a Confidential Human Source, and the information that Source has provided, when required by court order, law, regulation, these Guidelines or other Department of Justice policies.

5. **Disclosures to Confidential Human Sources**

DOJ personnel must exercise due diligence to avoid disclosing any confidential investigative information to a Confidential Human Source (e.g., information relating to electronic surveillance, search warrants, indictments and other charging documents, or the identity of other actual or potential informants), other than what is necessary and appropriate for operational reasons.

E. EXCEPTIONS AND DISPUTE RESOLUTION

1. Whenever an FBI SAC, a CFP, or the designee of an FBI SAC or CFP, believes that extraordinary circumstances exist that warrant an exception to any provision of these Guidelines, or whenever there is a dispute between or among entities (other than a dispute with the Assistant Attorney General (AAG) of either the Criminal Division or National Security Division of the Department of Justice) regarding these Guidelines, an exception must be sought from, or the dispute shall be resolved by, the AAG for the Criminal Division or the National Security Division (whichever is appropriate) or his or her designee.

2. Whenever there is a dispute with the AAG for either the Criminal Division or National Security Division of the Department of Justice, such dispute shall be resolved by the Deputy Attorney General or his or her designee.

3. The Deputy Attorney General, or his or her designee, shall hear appeals, if any, from decisions of the Assistant Attorneys General of the Criminal Division and the National Security Division.

4. Any exception granted or dispute resolved pursuant to this paragraph shall be documented in the FBI's files.

F. RIGHTS OF THIRD PARTIES

Nothing in these Guidelines is intended to create or does create an enforceable legal right or private right of action by a Confidential Human Source or any other person.

G. COMPLIANCE

1. Within 60 days of the approval of these Guidelines by the Attorney General, the FBI shall submit an implementation plan to the respective Assistant Attorneys General for the Criminal Division and the National Security Division of the Department of Justice for review. The plan must address all the requirements imposed upon the FBI by these Guidelines.

2. Within 60 days of the approval of these Guidelines, the FBI in conjunction with the Criminal Division of the Department of Justice, shall establish a Human Source Review Committee to perform the functions set forth in Section III (A) below.

3. Within 60 days of the approval of these Guidelines, each FPO shall designate one or more supervisory FPO Attorneys to serve as "Confidential Human Source Coordinators," whose duties shall include:

   a. coordinating the responsibilities of the FPO under these Guidelines;

b. serving as a point of contact for the FBI for all matters pursuant to these Guidelines; and

c. approving matters pursuant to these Guidelines on behalf of the FPO when no other FPO Attorney has been assigned or when the assigned FPO Attorney is unavailable.

4. Each CFP and FBI-SAC shall implement comprehensive periodic training of its respective personnel regarding these Guidelines.

5. Each CFP shall coordinate with the appropriate FBI SAC to develop procedures to maximize the accessibility and availability of the FPO's Confidential Human Source Coordinators.

II. VALIDATION OF A CONFIDENTIAL HUMAN SOURCE

A. INITIAL VALIDATION

1. General

All FBI Confidential Human Sources must be subjected to the validation process as provided in these Guidelines and other FBI policies.

2. Time Limits

The FBI, in consultation with the Assistant Attorneys General of the Criminal Division and the National Security Division of the Department of Justice, shall establish reasonable time limits for subjecting a Source to the Initial Validation process that are compatible with these Guidelines and other FBI policies.

3. **Required Information**

In opening a Confidential Human Source, an FBI Agent shall document information pertaining to that Source and forward it to an appropriate FBI Supervisor for an Initial Validation. At a minimum, an FBI Agent shall provide the following information to facilitate the Initial Validation process:

a. basie identifying information that establishes the person's true identity, or the FBI's efforts to establish the individual's true identity;

b. a photograph of the person (when possible);

c. whether the person has a criminal history, is reasonably believed to be the subject or target of a pending criminal investigation, is under arrest, or has been charged in a pending prosecution;

d. the person's motivation for providing information or assistance, including any consideration sought from the government for this assistance;

e. any promises or benefits, and the terms of such promises or benefits, that are given a Confidential Human Source by the FBI, FPO or any other law enforcement agency (if known, after exercising reasonable efforts); and

f. any other information that is required to be documented in the Confidential Human Source's file pursuant to these Guidelines and FBI policies, including but not limited to, the instructions provided to the Confidential Human Source.

B. INSTRUCTIONS

1. In opening a Confidential Human Source, at least one FBI Agent, along with one additional Agent or other government official present as a witness, shall review with the Confidential Human Source instructions as required by these Guidelines and other FBI policies. At a minimum, these instructions must indicate that:

   a. information provided by the Confidential Human Source to the FBI must be truthful;

   b. the Confidential Human Source's assistance and the information provided are entirely voluntary;

   c. the United States Government will strive to protect the Confidential Human Source's identity but cannot guarantee that it will not be divulged;

   d. the Confidential Human Source must abide by the instructions of the FBI and must not take or seek to take any independent action on behalf of the United States Government.

2. The following additional instructions shall also be reviewed with a Confidential Human Source if applicable to the particular circumstances of the Confidential Human Source:

   a. The FBI on its own cannot promise or agree to any immunity from prosecution or other consideration by a FPO, a state or local prosecutor, or a Court in exchange for the Confidential Human Source's cooperation, because the decision to confer any such benefit lies within the exclusive discretion of the FPO and the Court. However, the FBI will consider (but not necessarily act upon) a request by the Confidential Human Source to advise the appropriate FPO, the state or local prosecutor, or Court of the nature and extent of his or her assistance to the FBI;[6]

b. The Confidential Human Source has not been authorized to engage in any criminal activity and has no immunity from prosecution for any unauthorized criminal activity;[7]

c. The Confidential Human Source is not an employee of the United States Government and may not represent himself or herself as such;[8]

d. The Confidential Human Source may not enter into any contract or incur any obligation on behalf of the United States Government, except as specifically instructed and approved by the FBI;[9]

e. The FBI cannot guarantee any rewards, payments, or other compensation to the Confidential Human Source;

---

[6] This instruction should be provided if there is any apparent issue of criminal liability or penalties that relates to the Confidential Human Source.

[7] This instruction should be provided to any Confidential Human Source who is not authorized to engage in otherwise illegal activity. See paragraph V (B)(3) for instructions that must be provided to a Confidential Human Source who is, in fact, authorized to engage in otherwise illegal conduct.

[8]This instruction should be provided to <u>all</u> Confidential Human Sources <u>except</u> under those circumstances where the Source has previously been, and continues to be, otherwise employed by the United States Government.

[9]This instruction should be provided to <u>all</u> Confidential Human sources <u>except</u> under those circumstances where the Source is otherwise authorized to enter a contract or incur an obligation on the behalf of the United States.

f. In the event that the Confidential Human Source receives any rewards, payments, or other compensation from the FBI, the Source is liable for any taxes that may be owed; and

g. No promises or commitments can be made, except by the United States Department of Homeland Security, regarding the alien status of any person or the right of any person to enter or remain in the United States.[10]

3. The content and meaning of each of the foregoing instructions must be clearly conveyed to the Confidential Human Source. Immediately after these instructions have been given, the FBI Agent shall require the Confidential Human Source to acknowledge his or her receipt and understanding of the instructions. The FBI Agent, and the additional Agent or other government official present as a witness, shall document that the instructions were reviewed with the Confidential Human Source and that the Source acknowledged the instructions and his or her understanding of them. As soon as practicable thereafter, an FBI Supervisor shall review and, if warranted, approve the documentation.

4. The instruction and documentation procedures shall be repeated to the Confidential Human Source whenever it appears necessary or prudent to do so, and, in any event, at least annually.

[10] This instruction should be provided if there is any apparent issue of immigration status that relates to the Confidential Human Source.

C. ANNUAL VALIDATION REVIEW

1. Each Confidential Human Source's file shall be reviewed at least annually consistent with these Guidelines and other FBI policies.

2. The FBI shall establish procedures to ensure that all available information that might materially alter a prior validation assessment, including, but not limited to, information pertaining to unauthorized illegal activity by the Confidential Human Source, is promptly reported to an FBI Supervisor and then recorded and maintained in the file of the Confidential Human Source.

III. SPECIAL APPROVAL REQUIREMENTS

A. DEFINED CATEGORIES OF SOURCES

1. Required Early Approval

Within 60 days of utilizing a Confidential Human Source who meets any of the following definitions, the FBI must seek written approval, in accordance with the relevant provisions set forth in paragraph III (A)(3) below, for the continued use of the Source unless an FPO Attorney has existing oversight of a Source because the Source has agreed to testify in a federal criminal prosecution:

a. "Senior Leadership Source" -- a Confidential Human Source as defined in paragraph I (B)(8), above;

b. "Privileged or Media Source" -- A Confidential Human Source who is under the obligation of a legal privilege of confidentiality or affiliated with the media;

c. "High-Level Government or Union Source" – A Confidential Human Source as defined in paragraph I (B)(9), above.

2. **Long-Term Sources**

When a Confidential Human Source has been registered for more than five consecutive years, and to the extent such a Source remains open, every five years thereafter, the FBI must seek written approval, in accordance with the relevant provisions set forth in paragraph III (A)(3) below, for the continued use of the Source.

3. **Approval Process**

All FBI requests seeking approval for the continued use of a Confidential Human Source who meets any of the definitions set forth in paragraphs III (A)(1) & (2) above, <u>except</u> those Sources providing information for use in an international terrorism investigation, national security investigation, or other activity under NSIG, shall be reviewed and determined by a Human Source Review Committee (HSRC).

a. Composition of the HSRC - - At least one HSRC shall be established by the FBI and the Criminal Division of the Department of Justice. The Chairperson of each HSRC shall be an FBI Agent at or above the level of Deputy Assistant Director (or its equivalent). The membership of each HSRC shall include: two FBI Agents, and two attorneys from the FBI's Office of General Counsel, as designated by the Chairperson; and five FPO Attorneys designated by the AAG for the Criminal Division. One of the five FPO Attorneys shall be a Deputy AAG from the Criminal Division, and at least two of the remaining FPO Attorneys shall each be from a U.S. Attorney's Office and have relevant experience in organized crime matters. In addition, an FPO Attorney designated by the Assistant Attorney General for National Security shall be a member of the HSRC, but shall not be considered to be a voting member for purposes of determining whether continued use of a Source under review should be approved.

b. Access to FBI Information - - During the approval process, the HSRC shall have access to all relevant FBI information pertaining to the use of the Confidential Human Source under consideration, including any Annual Validation Reports. However, the identity of the Confidential Human Source will not be disclosed to the HSRC unless the Chairperson of the HSRC determines that compelling reasons exist to warrant such a disclosure.

c. Time Limit - - The HSRC approval process shall be completed no more than 45 days after the FBI has submitted a request seeking approval for the continued use of a Confidential Human Source. While the request is pending with the HSRC, the FBI shall be permitted to continue to utilize the Confidential Human Source.

d. Notice to FPO - - After a final decision has been made by the HSRC, the HSRC shall consider whether to provide notice of the decision to any appropriate FPO.

e. Disputes - - The HSRC shall recommend approval of the continued use of a Source only upon reaching a consensus, provided that whenever the FBI, an FPO, or a HSRC Member disagrees with the final decision of the HSRC, it may seek review and reconsideration of that decision pursuant to the Exceptions and Dispute Resolution section, paragraph I (E) above. While the dispute is pending resolution, the FBI shall be permitted to continue to utilize the Confidential Human Source.

f. Sources Providing Information for Use in International Terrorism Investigations, National Security Investigations, or Other Activities under NSIG - - No Confidential Human Source who is providing information for use in international terrorism investigations, national security investigations, or other activities under NSIG shall be referred to the HSRC for review. Instead, the FBI shall provide notice to the National Security Division within 60 days of FBI Headquarters' approval of the continued use of any such Confidential Human Source who is subject to the enhanced review provisions of the FBI's Confidential Human Source Validation Standards Manual. Confidential Human Sources who meet any of the definitions set forth in paragraphs III(A)(1) & (2) shall be subject to enhanced review. The Assistant Attorney General for National Security shall designate FPO Attorneys to review the notices and associated information pursuant to the following process:

i. Upon request by the designated FPO Attorney, the FBI shall make available at FBI Headquarters to the designated FPO Attorney Validation Reports regarding the Confidential Human Source. If the Validation Reports do not permit the FPO Attorney to conduct a meaningful analysis of the propriety of continuing to use the Confidential Human Source, the FPO Attorney may ask for additional information regarding the Confidential Human Source. The identity of the Confidential Human Source shall not be disclosed to the designated FPO Attorney unless the Assistant Director or a Deputy Assistant Director of the Division that is utilizing the Confidential Human Source determines that compelling reasons exist to warrant such a disclosure. With the exception of a request for the identity of the Confidential Human Source, all requests by the FPO Attorney for further information pertaining to a Confidential Human Source shall be satisfied within a reasonable period of time. Failure to provide such information may be grounds for the National Security Division to recommend that the Deputy Attorney General disapprove continued use of the Confidential Human Source. If the Director of the FBI and the Assistant Attorney General for National Security do not agree whether information sought is reasonably necessary in order for the FPO Attorney to conduct a meaningful analysis of the propriety of continuing to use the Confidential Human Source, any such dispute shall be resolved by the Deputy Attorney General.

ii. The designated FPO Attorney may consult with other designated FPO Attorneys and with the Assistant Attorney General for National Security concerning the continued use of the Confidential Human Source. If the Assistant Attorney General for National Security does not object to the FBI's continued use of the Confidential Human Source, no further action shall be taken. If the Assistant Attorney General for National Security objects to the FBI's continued use of the Confidential Human Source, the Assistant Attorney General shall forward a recommendation to the Deputy Attorney General that continued use of the Confidential Human Source be disapproved. While the dispute is pending resolution before the Deputy Attorney General, the FBI shall be permitted to continue to utilize the Confidential Human Source.

B. FEDERAL PRISONERS, PROBATIONERS, PAROLEES, AND SUPERVISED RELEASEES

1. Consistent with extant Department of Justice requirements, the FBI must receive the approval of the Criminal Division's Office of Enforcement Operations ("OEO") prior to utilizing as a Confidential Human Source an individual who is in the custody of the United States Marshals Service or the Bureau of Prisons, or who is under Bureau of Prisons supervision. <u>See</u> U.S.A.M. § 9-21.050.

2. Prior to utilizing a federal probationer, parolee, or supervised releasee as a Confidential Human Source, an FBI Supervisor shall determine whether the use of that person in such a capacity would violate the terms and conditions of the person's probation, parole, or supervised release. If the FBI Supervisor has reason to believe that it would violate such terms and conditions, prior to using the person as a Confidential Human Source, the FBI Supervisor or his or her designee must obtain the permission of a federal probation, parole, or supervised release official with authority to grant such permission, which permission shall be documented in the Confidential Human Source's files. If such permission is denied or it is inappropriate for operational reasons to contact the appropriate federal official, the FBI may seek to obtain authorization for the use of such individual as a Confidential Human Source from the Court then responsible for the individual's probation, parole, or supervised release, provided that the FBI first consults with the FPO for that District.

3. If an FPO is participating in the conduct of an investigation by the FBI in which a federal probationer, parolee, or supervised releasee would be utilized as a

Confidential Human Source or would be working with a federal probationer, parolee, or supervised releasee in connection with a prosecution, the FBI shall notify the FPO Attorney assigned to the current matter prior to using the person as a Confidential Human Source.

C. CURRENT OR FORMER PARTICIPANTS IN THE WITNESS SECURITY PROGRAM

1. Consistent with extant Department of Justice requirements, the FBI must receive the approval of OEO and the sponsoring FPO Attorney (or his or her successor) prior to utilizing as a Confidential Human Source a current or former participant in the Federal Witness Security Program, provided further that the OEO will coordinate such matters with the United States Marshals Service. See U.S.A.M. § 9-21.800.

2. If an FPO is participating in the conduct of an investigation by the FBI in which a current or former participant in the Witness Security Program would be utilized as a Confidential Human Source or would be working with a current or former participant in the Witness Security Program in connection with a prosecution, the FBI shall notify the FPO Attorney assigned to the matter prior to using the person as a Confidential Human Source.

D. STATE OR LOCAL PRISONERS, PROBATIONERS, PAROLEES, OR SUPERVISED RELEASEES

1. Prior to utilizing a state or local prisoner, probationer, parolee, or supervised releasee as a Confidential Human Source, an FBI Supervisor shall determine whether the use of that person in such a capacity would violate the terms and

conditions of the person's incarceration, probation, parole, or supervised release. If the FBI Supervisor has reason to believe that it would violate such terms and conditions, prior to using the person as a Confidential Human Source, an FBI Supervisor or his or her designee must obtain the permission of a state or local prison, probation, parole, or supervised release official with authority to grant such permission, which permission shall be documented in the Confidential Human Source's files. If such permission is denied or it is inappropriate for operational reasons to contact the appropriate state or local official, the FBI may seek to obtain authorization for the use of such person as a Source from the state or local court then responsible for the person's incarceration, probation, parole, or supervised release.

2. If an FPO is participating in the conduct of an investigation by the FBI in which a state or local prisoner, probationer, parolee, or supervised releasee would be utilized as a Confidential Human Source or would be working with a state or local prisoner, probationer, parolee, or supervised releasee in connection with a prosecution, the FBI shall notify the FPO Attorney assigned to the matter prior to using the person as a Confidential Human Source.

E. FUGITIVES

1. Except as provided below, an FBI Agent shall not initiate communication with a current or former Confidential Human Source who is a fugitive.

2. An FBI Agent is permitted to communicate with a current or former Confidential Human Source who is a fugitive:

a. if the fugitive Source initiates the communication;

b. if the communication is part of a legitimate effort by the FBI to arrest the fugitive; or

c. if approved, in advance whenever possible, by a Supervisor of any federal, state, or local law enforcement agency that has a wanted record for the individual in the NCIC and, in the case of a federal warrant, by the FPO for the issuing District.

3. An FBI Agent who communicates with a Confidential Human Source who is a fugitive must promptly report such communication to the appropriate federal, state or local law enforcement agency, and any other law enforcement agency having a wanted record for the individual in the NCIC, and must document those communications in the Confidential Human Source's files.

IV. RESPONSIBILITIES REGARDING CONFIDENTIAL HUMAN SOURCES

A. NO INTERFERENCE WITH AN INVESTIGATION OF A CONFIDENTIAL HUMAN SOURCE

DOJ personnel shall not interfere with or impede any criminal investigation or arrest of a Confidential Human Source. DOJ personnel shall not reveal to a Confidential Human Source any information relating to an investigation of the Source, including confirming or denying the existence of such an investigation, unless authorized to do so by the Chief Federal Prosecutor or his or her designee, after consultation with the appropriate FBI SAC or his or her designee.

B. PROHIBITED TRANSACTIONS AND RELATIONSHIPS

1. DOJ personnel directing or overseeing the direction of a Confidential Human Source shall not:

   a. exchange gifts with a Confidential Human Source;

   b. provide the Confidential Human Source with anything of more than nominal value;

   c. receive anything of more than nominal value from a Confidential Human Source; or

   d. engage in any business or financial transactions with a Confidential Human Source.

2. Unless authorized pursuant to paragraph IV (B)(3) below, any exception to this provision requires the written approval of an FBI Supervisor, in advance whenever possible, based on a finding by the FBI Supervisor that the event or transaction in question is necessary and appropriate for operational reasons. This written finding shall be maintained in the Confidential Human Source's files.

3. DOJ personnel directing or overseeing the direction of a Confidential Human Source shall not socialize with that Source, except to the extent necessary and appropriate for operational reasons.

4. If an FPO is participating in the conduct of an investigation that is utilizing an FBI Confidential Human Source or working with a Confidential Human Source in connection with a prosecution, the FBI shall provide written notification to the FPO Attorney assigned to the matter, in advance whenever possible, if the FBI

approves an exception under paragraph IV (B) or if an FBI Agent socializes with a Confidential Human Source in a manner not permitted under paragraph IV(B)(2) & (3).

C. MONETARY PAYMENTS

1. General

Monies that the FBI pays to a Confidential Human Source in the form of fees and rewards shall be commensurate with the value, as determined by the FBI, of the information or assistance the Source provided to the FBI. The FBI's reimbursement of expenses incurred by a Confidential Human Source shall be based upon actual expenses incurred, except that relocation expenses may be made based on an estimate of the expenses.

2. Prohibition Against Contingent Payments

Under no circumstances shall any payments to a Confidential Human Source be contingent upon the conviction or punishment of any individual.

3. Approval for Payments

The FBI shall establish a written delegation of authority for approval of payments to Confidential Human Sources. The delegation of authority shall establish the level of approval required when single payments, aggregate annual payments, and total aggregate payments meet or exceed specific threshold amounts. The threshold amounts and approval authority are subject to periodic review and amendment as deemed appropriate by the FBI Director.

4. Documentation of Payment

The payment of any FBI funds to a Confidential Human Source shall be witnessed by at least one FBI Agent and another government official. In the event of extraordinary circumstances that must be documented in the Source's file, only one witness shall be required. Immediately after receiving a payment, the Confidential Human Source shall be required to sign or initial, and date, a written receipt.[11] At the time of the payment, the FBI Agent or other government official shall advise the Confidential Human Source that the monies may be taxable income that must be reported to appropriate tax authorities. Thereafter, the FBI shall document the payment and the advice of taxability in the FBI's files. The documentation of payment shall specify whether the payment is for services or expenses.

5. Accounting and Reconciliation Procedures

The FBI shall establish accounting and reconciliation procedures to comply with these Guidelines. The FBI procedures shall ensure that the FBI accounts for all funds paid to a Confidential Human Source subsequent to the issuance of these Guidelines.

6. Coordination with Prosecution

If an FPO Attorney is participating in the conduct of an investigation or prosecution that is utilizing an FBI Confidential Human Source who is expected

---

[11] The Confidential Human Source may sign or initial the written receipt by using a pseudonym which has been previously approved and documented in the Source's files and designated for use by only one Confidential Human Source.

to testify, the FBI shall coordinate with the FPO attorney, in advance if practicable, any payment of monies to the Confidential Human Source pursuant to paragraph IV(C)(3) above. If the payment is to be made for services and if the FPO Attorney objects to the payment, no payment will be made until the dispute has been resolved in accordance with Section I. E. above.

V. AUTHORIZATION OF OTHERWISE ILLEGAL ACTIVITY

A. GENERAL PROVISIONS

1. The FBI shall not authorize a Confidential Human Source to engage in any activity that otherwise would constitute a criminal violation under federal, state, or local law if engaged in by a person acting without authorization, except as provided in the authorization provisions in paragraph V(B) below.
2. The FBI is never permitted to authorize a Confidential Human Source to:
   a. participate in any act of violence except in self-defense;[12] or
   b. participate in an act designed to obtain information for the FBI that would be unlawful if conducted by a law enforcement agent (e.g., breaking and entering, illegal wiretapping, illegal opening or tampering with the mail, or trespass amounting to an illegal search).

B. AUTHORIZATION PROCEDURES

1. Written Authorization

[12]The Source may take reasonable measures of self-defense in an emergency to protect his or her own life or the lives of others against wrongful force.

a. Tier 1 Otherwise Illegal Activity must be authorized by an FBI SAC and the appropriate CFP, in advance and in writing for a specified period, not to exceed 90 days, except that, with respect to all international terrorism investigations, national security investigations, or other activities under NSIG, upon request of the FBI and at the discretion of the appropriate CFP, the Otherwise Illegal Activity may be authorized for a period of up to one year.

b. Tier 2 Otherwise Illegal Activity must be authorized by an FBI SAC in advance and in writing for a specified period, not to exceed 90 days.

c. The written authorization by the FBI SAC and/or CFP of Otherwise Illegal Activity shall be as narrow as reasonable under the circumstances as to the unlawful activity's scope, geographic area, duration and other related matters.

d. For purposes of this paragraph, <u>except</u> with respect to all international terrorism investigations, national security investigations, or other activities under NSIG, the "appropriate Chief Federal Prosecutor" is the CFP that:

    i. is participating in the conduct of an investigation by the FBI that is utilizing the Confidential Human Source or is working with the Confidential Human Source in connection with a prosecution;

    ii. would have primary jurisdiction to prosecute the Otherwise Illegal Activity that would constitute a violation of federal law; or

iii. is located where the Otherwise Illegal Activity is to occur, and it only constitutes a violation of state or local law.

e. With respect to all international terrorism investigations, national security investigations, or other activities under NSIG, the appropriate Chief Federal Prosecutor is the AAG of the NSD, or designee. Within 60 days after these Guidelines are approved by the Attorney General, the AAG of the NSD shall identify designees for purposes of this paragraph, which may include DOJ personnel outside the NSD.

2. Findings

a. The FBI SAC and the CFP who authorize the Otherwise Illegal Activity must make a finding, which shall be documented in the Confidential Human Source's files, that the illegal activity is:

i. necessary either to -

A. obtain information or evidence essential for the success of an investigation that is not reasonably available without such activity, including circumstances in which the Confidential Human Source must engage in the illegal activity in order to maintain his credibility and thereby obtain the information or evidence, or

B. prevent death, serious bodily injury, or significant damage to property; and

ii. that the benefits to be obtained from the Confidential Human Source's participation in the Otherwise Illegal Activity outweigh the risks.

b. In making these findings, the FBI SAC and the CFP shall consider, among other things:

i. the importance of the investigation;

ii. the likelihood that the information or evidence sought will be obtained;

iii. the risk that the Confidential Human Source might misunderstand or exceed the scope of his authorization;

iv. the extent of the Confidential Human Source's participation in the Otherwise Illegal Activity;

v. the risk that the FBI will not be able to closely monitor the Confidential Human Source's participation in the Otherwise Illegal Activity;

vi. the risk of violence, physical injury, property damage, or financial loss to the Confidential Human Source or others; and

vii. the risk that the FBI will not be able to ensure that the Confidential Human Source does not realize undue profits from his or her participation in the Otherwise Illegal Activity.

3. **Instructions**

a. If a Confidential Human Source is authorized to engage in Otherwise Illegal Activity, at least one FBI Agent, along with one additional government official present as a witness, shall review with the Confidential Human Source written instructions that:

i. the Confidential Human Source is authorized only to engage in the specific conduct set forth in the written authorization and not in any other illegal activity (the Chief Federal Prosecutor's written authorization should be read to the Confidential Human Source unless it is not feasible);

ii. the Confidential Human Source's authorization is limited to the time period specified in the written authorization;

iii. under no circumstance may the Confidential Human Source:

A. participate in an act of violence (except in self-defense);

B. participate in an act designed to obtain information for the FBI that would be unlawful if conducted by a law enforcement agent (e.g., breaking and entering, illegal wiretapping, illegal opening or tampering with the mail, or trespass amounting to an illegal search);

C. If applicable: participate in an act that constitutes obstruction of justice (e.g., perjury, witness tampering, witness intimidation, entrapment, or the fabrication, alteration, or destruction of evidence);

D. If applicable: initiate or instigate a plan or strategy to commit a federal, state, or local offense;

iv. if the Confidential Human Source is asked by any person to participate in any illegal activity other than the specific conduct set forth in the written authorization, or learns of plans to engage in such illegal activity, the Source must immediately report the matter to the FBI Case Agent; and

v. participation in any illegal activity other than the specific conduct set forth in the written authorization could subject the Confidential Human Source to criminal prosecution.

b. Immediately after these instructions have been given, the Confidential Human Source shall be required to sign or initial, and date, a written acknowledgment of the instructions.[13] If the Confidential Human Source refuses to sign or initial the written acknowledgment, the FBI Agent, and the additional Agent or other government official present as a witness, shall document that the instructions were reviewed with the Confidential Human Source and that the Source acknowledged the instructions and his

[13] The Confidential Human Source may sign or initial the written acknowledgment by using a pseudonym which has been previously approved and documented in the Confidential Human Source's files and designated for use by only one Confidential Human Source.

or her understanding of them. As soon as practicable thereafter, an FBI Supervisor shall review and, if warranted, approve the documentation.

4. **Precautionary Measures**

Whenever the FBI has authorized a Confidential Human Source to engage in Otherwise Illegal Activity, the FBI must take all reasonable steps to:

a. monitor closely the activities of the Confidential Human Source;

b. minimize the adverse effect of the Otherwise Illegal Activity on innocent persons; and

c. ensure that the Confidential Human Source does not realize undue profits from his or her participation in the Otherwise Illegal Activity.

5. **Suspension of Authorization**

Whenever the FBI cannot, for legitimate reasons unrelated to the Confidential Human Source's conduct (e.g., unavailability of the Case Agent), comply with the precautionary measures described above, it shall immediately:

a. suspend the Confidential Human Source's authorization to engage in Otherwise Illegal Activity until such time as the precautionary measures can be complied with;

b. inform the Confidential Human Source that his or her authorization to engage in any Otherwise Illegal Activity has been suspended until that time; and

c. document these actions in the Confidential Human Source's files.

6. **Revocation of Authorization**

a. If an FBI Agent has reason to believe that a Confidential Human Source has failed to comply with the terms of the authorization of Otherwise Illegal Activity, the FBI Agent shall immediately:

i. revoke the Confidential Human Source's authorization to engage in Otherwise Illegal Activity;

ii. inform the Confidential Human Source that he or she is no longer authorized to engage in any Otherwise Illegal Activity;

iii. comply with the notification requirement of paragraph VI (B) below;

iv. determine whether the Confidential Human Source should be closed pursuant to Section VII; and

v. document these actions in the Confidential Human Source's files.

b. Immediately after the Confidential Human Source has been informed that he or she is no longer authorized to engage in any Otherwise Illegal Activity, the Confidential Human Source should sign or initial, and date, a written acknowledgment that he or she has been informed of this fact.[14] If the Confidential Human Source refuses to sign or initial the written acknowledgment, the FBI Agent who informed the Confidential Human Source of the revocation of authorization shall document the refusal, and the source's oral acknowledgment of the information if such oral

[14] The Confidential Human Source may sign or initial the written acknowledgment by using a pseudonym which has been previously approved and documented in the Confidential Human Source's files and designated for use by only one Confidential Human Source.

acknowledgment is provided. As soon as practicable thereafter, an FBI Supervisor shall review the written acknowledgment or documentation of refusal.

7. **Renewal and Expansion of Authorization**

a. If the FBI seeks to re-authorize any Confidential Human Source to engage in Otherwise Illegal Activity after the expiration of the authorized time period, or after revocation of authorization, the FBI must first comply with the procedures set forth above in paragraphs V(B)(1)-(3).

b. If the FBI seeks to expand in any material way a Confidential Human Source's authorization to engage in Otherwise Illegal Activity, the FBI must first comply with the procedures set forth above in paragraphs V (B)(1)-(3).

8. **Emergency Authorization**

a. In exceptional circumstances, an FBI SAC and the appropriate CFP may orally authorize a Confidential Human Source to engage in Tier 1 Otherwise Illegal Activity without complying with the documentation requirements of paragraphs V (B)(1)-(3) above, when they each determine that a highly significant and unanticipated investigative opportunity would be lost were the time taken to comply with these documentation requirements, and that the circumstances support a finding required pursuant to paragraph V (B)(2). In such an event, the documentation requirements, as well as a written justification for the oral authorization, shall be completed within 72 hours or as soon as practicable following the oral approval and maintained in the Confidential Human Source's files.

b. In extraordinary circumstances, an FBI SAC may orally authorize a Confidential Human Source to engage in Tier 2 Otherwise Illegal Activity without complying with the documentation requirements of paragraphs V(B)(1)-(3) above when he or she determines that a highly significant and unanticipated investigative opportunity would be lost were the time taken to comply with these requirements. In such an event, the documentation requirements, as well as a written justification for the oral authorization, shall be completed within 72 hours or as soon as practicable following the oral approval and maintained in the Confidential Human Source's files.

9. Designees

The FBI SAC and the CFP may agree to designate particular individuals at the supervisory level in their respective offices to carry out the approval functions assigned to them in Section V.

10. Record Keeping Procedures

a. The FBI shall maintain a file for each Confidential Human Source containing all the written authorizations, findings and instructions regarding Tier 1 Otherwise Illegal Activity, as required under Section V(B) of these Guidelines.

b. At the end of each calendar year, the FBI shall report to the Assistant Attorneys General of the Criminal Division and the National Security

Division the total number of times each FBI Field Office authorized a Confidential Human Source to engage in Otherwise Illegal Activity, and the overall nationwide totals.

c. If requested, the FBI shall provide to the Assistant Attorneys General of the Criminal Division and the National Security Division a copy of any written authorization, finding or instruction issued pursuant to Section V(B) of these Guidelines.

VI. SPECIAL NOTIFICATION REQUIREMENTS

A. NOTIFICATION OF INVESTIGATION OR PROSECUTION

1. If an FBI Agent has reasonable grounds to believe that the alleged felonious activity of a current or former Confidential Human Source is, or is expected to become, the basis of a prosecution or investigation by an FPO or a state or local prosecutor's office, the FBI Agent must immediately notify a Confidential Human Source Coordinator or the assigned FPO Attorney of that individual's status as a current or former Confidential Human Source. However, with respect to a former Confidential Human Source whose alleged felonious activity is, or is expected to become, the basis of a prosecution or investigation by a state or local prosecutor's office, no notification obligation shall arise unless the FBI Agent has reasonable grounds to believe that the Confidential Human Source's prior relationship with the FBI is material to the prosecution or investigation.

2. Whenever such a notification occurs, the Confidential Human Source Coordinator or the assigned FPO Attorney shall notify the CFP. The CFP and FBI SAC, with the concurrence of each other, shall notify any other federal, state or local prosecutor's office or law enforcement agency that is participating in the investigation or prosecution of the Confidential Human Source.

B. NOTIFICATION OF UNAUTHORIZED ILLEGAL ACTIVITY

1. If an FBI Agent has reasonable grounds to believe that a Confidential Human Source has engaged in unauthorized criminal activity (other than minor traffic offenses), the FBI shall promptly notify a Confidential Human Source Coordinator or the assigned FPO Attorney. In turn, the Confidential Human Source Coordinator or assigned FPO Attorney shall notify the following FPOs of the Confidential Human Source's criminal activity and his or her status as a Confidential Human Source:

    a. the FPO in whose District the criminal activity primarily occurred, unless a state or local prosecuting office in that District has filed charges against the Confidential Human Source for the criminal activity and there is no basis for federal prosecution in that District;

    b. the FPO Attorney, if any, who is participating in the conduct of an investigation that is utilizing the Confidential Human Source or is working with the Confidential Human Source in connection with a prosecution; and

c. the FPO Attorney, if any, who authorized the Confidential Human Source to engage in Otherwise Illegal Activity pursuant to paragraph V(B) above.[15]

2. Whenever such notifications are provided, the Chief Federal Prosecutor(s) and the FBI SAC, with the concurrence of each other, shall notify any state or local prosecutor's office that has jurisdiction over the Confidential Human Source's criminal activity and that has not already filed charges against the Confidential Human Source for the criminal activity of the fact that the Confidential Human Source has engaged in such criminal activity. The CFP(s) and the FBI SAC(s) are not required, but may with the concurrence of each other, also notify the state and local prosecutor's office of the person's status as a Confidential Human Source.

C. NOTIFICATION REGARDING CERTAIN FEDERAL JUDICIAL PROCEEDINGS

The FBI shall immediately notify an appropriate Confidential Human Source Coordinator or the assigned FPO Attorney whenever an FBI Agent has reasonable grounds to believe that:

1. a current or former Confidential Human Source has been called to testify by the prosecution in any federal grand jury or judicial proceeding;
2. the statements of a current or former Confidential Human Source have been, or will be, utilized by the prosecution in any federal judicial proceeding; or

[15] Whenever such notifications to FPOs are provided, the FBI must also comply with the Annual Validation Review requirements described above in paragraph (II)(C)(2).

3. an FPO Attorney intends to represent to a Court or jury that a current or former Confidential Human Source is or was a co-conspirator or other criminally culpable participant in any criminal activity.

D. PRIVILEGED OR EXCULPATORY INFORMATION

1. If an FPO is participating in the conduct of an investigation by the FBI that is utilizing a Confidential Human Source or working with a Confidential Human Source in connection with a prosecution, the FBI shall notify the FPO Attorney assigned to the matter, in advance whenever possible, if the FBI has reasonable grounds to believe that a Confidential Human Source will obtain or provide information that is subject to, or arguably subject to, a legal privilege of confidentiality belonging to someone other than the Confidential Human Source.
2. Whenever an FBI Agent knows or reasonably believes that a current or former Confidential Human Source has information that is exculpatory as to a target of a federal, state or local investigation, or as to a defendant (including a convicted defendant) in a federal, state or local case, the FBI Agent shall disclose the exculpatory information either to the assigned FPO Attorney that is participating, or had participated, in the conduct of the investigation or to a Confidential Human Source Coordinator.
3. In turn, the assigned FPO Attorney or Confidential Human Source Coordinator shall disclose the exculpatory information to all affected federal, state and local authorities. In the event the disclosure would jeopardize the security of a Confidential Human Source or seriously compromise an investigation, the FPO

Attorney or Confidential Human Source Coordinator shall refer the matter to the HSRC for consideration, except such matters with respect to an international terrorism investigation, national security investigation, or other activity under NSIG shall be referred to the AAG of the NSD or designee.

E. LISTING A CONFIDENTIAL HUMAN SOURCE IN AN ELECTRONIC SURVEILLANCE APPLICATION

1. The FBI shall not name a Confidential Human Source as a named interceptee or a violator in an affidavit in support of an application made pursuant to 18 U.S.C. § 2516 for an electronic surveillance order unless the FBI believes that:

    a. omitting the name of the Confidential Human Source from the affidavit would endanger that person's life or otherwise jeopardize an ongoing investigation; or

    b. the Confidential Human Source is a bona fide subject of the investigation based on his or her suspected involvement in unauthorized criminal activity.

2. In the event that a Confidential Human Source is named in an electronic surveillance affidavit under paragraph VI (E)(1) above, the FBI must inform the FPO Attorney making the application and the Court to which the application is made of the actual status of the Confidential Human Source.

F. RESPONDING TO REQUESTS FROM FPO ATTORNEYS REGARDING A CONFIDENTIAL HUMAN SOURCE

1. In any criminal matter arising under, or related to, these Guidelines, upon request by an appropriate FPO Attorney, the FBI shall promptly provide the FPO Attorney

all relevant information concerning a Confidential Human Source, including whether he or she is a current or former Confidential Human Source for the FBI.

2. If the FBI SAC has an objection to providing such information based on specific circumstances of the case, he or she shall explain the objection to the FPO making the request and any remaining disagreement as to whether the information should be provided shall be resolved pursuant to the Exceptions and Dispute Resolution section, paragraph I (E).

G. EXCEPTIONS TO THE SPECIAL NOTIFICATIONS REQUIREMENTS

The Director of the FBI, with the written concurrence of the Deputy Attorney General, may withhold any notification required pursuant to paragraphs VI (A)-(F) if it is determined that the identity, position, or information provided by the Confidential Human Source warrants extraordinary protection for sensitive national security reasons. Any such determination shall be documented and maintained in the Confidential Human Source file, along with the concurrence of the Deputy Attorney General.

H. FILE REVIEWS

If the FBI discloses any information about a Confidential Human Source to a FPO pursuant to paragraphs VI (A)-(F), the FBI SAC and the CFP shall consult to facilitate any review and copying of the Confidential Human Source's files by the FPO that might be necessary for an FPO Attorney to fulfill his or her disclosure obligations.

I. DESIGNEES

An FBI SAC and a CFP may, with the concurrence of each other, designate particular individuals in their respective offices to carry out the functions assigned to them in paragraphs VI (A)-(H).

VII. CLOSING A CONFIDENTIAL HUMAN SOURCE

A. GENERAL PROVISIONS

If the FBI determines that a Confidential Human Source should be closed for cause or for any other reason the FBI shall promptly:

1. close the individual;
2. document the reasons for the decision to close the individual as a Confidential Human Source in the Confidential Human Source's files;
3. if the Confidential Human Source can be located, notify the Confidential Human Source that he or she has been closed as a Confidential Human Source and document that such notification has been provided in the same manner as set forth in paragraph (II)(B)(3), except that, if the Confidential Human Source refuses to acknowledge his receipt and understanding of the notification, the FBI shall document the refusal; and
4. if the Confidential Human Source was authorized to engage in Otherwise Illegal Activity pursuant to paragraph V(B), immediately revoke that authorization under the provisions of paragraph V (B)(6).

B. DELAYED NOTIFICATION TO A CONFIDENTIAL HUMAN SOURCE

The FBI may delay providing the notification to the Confidential Human Source described above in paragraph of VII (A)(3) during the time such notification might jeopardize an ongoing investigation or prosecution or might cause the flight from prosecution of any person. If the decision is made to delay providing a notification, that decision and the reasons supporting it must be documented in the Confidential Human Source's files.

C. CONTACTS WITH FORMER CONFIDENTIAL HUMAN SOURCES CLOSED FOR CAUSE

Absent exceptional circumstances that are approved by an FBI Supervisor, in advance whenever possible, an FBI Agent shall not initiate contact with or respond to contacts from a former Confidential Human Source who has been closed for cause. When granted, such approval shall be documented in the Confidential Human Source's files.

D. COORDINATION WITH FPO ATTORNEYS

If an FPO is participating in the conduct of an investigation that is utilizing an FBI Confidential Human Source or the FPO is working with a Confidential Human Source in connection with a prosecution, the FBI shall coordinate with the FPO Attorney assigned to the matter, in advance whenever possible, regarding any of the decisions described in paragraphs VII (A)-(C).

Date: 12-13-06

ALBERTO R. GONZALES
ATTORNEY GENERAL

ENCLOSURE D

QUESTION 96

8/25/06 LETTER
FROM DOJ AAG MOSCHELLA
TO THE HONORABLE F. JAMES SENSENBRENNER

U.S. Department of Justice

Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

August 25, 2006

The Honorable F. James Sensenbrenner, Jr.
Chairman
Committee on the Judiciary
U.S. House of Representatives
Washington, D.C. 20515

Dear Mr. Chairman:

This is to advise you of our strong opposition to H.R. 4132, the "Law Enforcement Cooperation Act of 2005," as reported by the Committee.

H.R. 4132 would amend the federal criminal code to impose fines and up to five years of incarceration upon any "officer or employee" of the Federal Bureau of Investigation (FBI or Bureau) who obtains information that a "confidential informant or other individual" has committed a serious violent felony that violates state or local law, and knowingly fails to promptly inform the state's chief law enforcement officer and local prosecutor. The bill also requires the officer or employee to notify the Attorney General that such information has been provided.

Inside information, through the management of cooperators and informants who are within, or on the immediate periphery of, the target criminal or terrorist organization, is key to the success of many of the FBI's investigations. The Attorney General's Guidelines provide legally sound and time-tested protocols by which the FBI coordinates with local law enforcement and reports serious crime by informants to the appropriate local authorities. The Guidelines require the U.S. Attorney and the FBI Special Agent in Charge to engage in a coordinated decision-making process through which senior law enforcement officials have an opportunity to consider such factors as the seriousness of the crime and the significance of the investigation in which an informant is being used. The FBI is greatly strengthening its internal procedures for tracking the recruitment and use of its human sources in order to ensure that this requirement, and all other requirements of the Attorney General's Guidelines, are strictly carried out. In addition, there is ample federal guidance requiring federal agencies to share criminal investigative information with their state and local counterparts. The FBI has actively followed these directives since their issuance after September 11, 2001, as part of the FBI's National Information Sharing Strategy. Indeed, active and effective law enforcement information sharing is underway at both the national and regional levels (through the National Data Exchange System known as "N-DEX" and the Regional Data Exchange System, or "R-DEX, respectively).

We believe that H.R. 4132, instead of having the intended effect of encouraging greater cooperation, would impede the progress we have made in fostering more effective federal, State and local law enforcement information-sharing and cooperation. The proposal would shift the primary focus of the FBI agent in the field away from recruiting sources capable of obtaining actionable intelligence to an emphasis on recruiting "safe" sources who are less likely to expose the agent to reportable criminal offenses.

Moreover, the legislation would significantly upset the delicate balance, achieved through decades of Supreme Court and federal case law, concerning whether an injured party has a justiciable claim against the United States under the Federal Tort Claims Act (FTCA) for the actions of FBI officials in failing to intervene or report criminal activity. The discretionary function exception of the FTCA, which currently provides broad protection against tort liability of the United States for such actions, would be undermined by this proposal, should an FBI agent violate the reporting requirement and a victim suffer harm at the hands of a confidential source, over whom the agent had no control. This could lead to unwarranted payments of substantial sums of public funds for damages even if the United States could not have prevented the harm.

The Department also notes that the reporting obligation contemplated by H.R. 4132 is without precedent or analog in State or federal law. The closest reference is the common law crime of failing to report criminal conduct. We note, however, that challenges to such prosecutions have encountered both evidentiary problems and constitutional challenges. As a result, virtually every jurisdiction in the country has included an element of active concealment in the proof required for a conviction *See, e.g.*, misprision of a felony, codified in federal law at 18 U.S.C. § 4.

In addition to lacking critical elements of proof, the bill fails to limit the proposed reporting requirement to only the most serious crimes, or to impose any standard of credibility, reliability, or weight with respect to the underlying report or allegation of criminal conduct. Section 3559 of title 18 includes crimes where no violence has occurred, such as firearms possession in furtherance of a drug trafficking offense, and also contains attempt, conspiracy, and solicitation provisions. As a result, H.R. 4132 would expose an FBI employee to a felony conviction, and up to five years imprisonment, for example, for failing to report a mere suggestion, by a non-credible source, that another person is thinking of robbing a local liquor store with a gun. No matter how lacking in credibility or viability the allegation might be, the agent would be obligated to pass it on in order to protect him or herself from criminal culpability. Such reporting not only would involve needless expenditure of both federal and local officer time and energy, it could also jeopardize federal criminal investigations, particularly those involving undercover agents and/or informants. The bill grants the FBI agent (or employee) no discretion to elect not to report the serious violent felony based on the agent or employee's professional judgment that greater harm will come to those who reported it.

As a final matter, we note that there have been no public hearings on H.R. 4132, which would allow the Committee to receive testimony from law enforcement personnel and other information concerning the myriad of problems raised by the bill.

We appreciate the opportunity to bring our views to your attention. The Office of Management and Budget has advised that there is no objection to the presentation of these responses from the standpoint of the Administration's program and that enactment of H.R. 4132 would not be in accord with the program of the President. If we may be of additional assistance, please do not hesitate to contact this office.

Sincerely,

William E. Moschella

William E. Moschella
Assistant Attorney General

cc: The Honorable John Conyers, Jr.
Ranking Minority Member

ENCLOSURE E

QUESTION 142a

1/25/07 LETTER
FROM CTD AD BILLY
TO ASSISTANT IG PRICE

U.S. Department of Justice

Federal Bureau of Investigation

In Reply, Please Refer to
File No.

January 25, 2007

The Honorable Paul A. Price
Assistant Inspector General
Office of the Inspector General
Evaluation and Inspection Division
Department of Justice
Suite 6100
1425 New York Avenue, NW
Washington, D.C. 20530

RE: OIG Recommendation 14, Status Update

Dear Mr. Price:

This letter is in response to the Office of the Inspector General (OIG) review of the "Federal Bureau of Prisons' Monitoring of Mail for High-Risk Inmates", A-2005-006, specifically Recommendation number 14. This Recommendation states "The FBI should continue to develop and reinforce procedures for interacting with the Bureau of Prisons (BOP) regarding international terrorist inmates, including monitoring of inmates, intelligence gathering, and sharing information and intelligence." The FBI agrees with this Recommendation and will continue to develop procedures regarding information sharing with BOP.

The FBI provided you with a letter dated September 22, 2006 in which we outlined our continuing efforts to improve and expand information sharing with the BOP. The purpose of this letter to provide you with a status report regarding our ongoing efforts.

Central to the success of the Correctional Intelligence Initiative (CII) is effective training for correctional staff in the skills necessary to accomplish the program goals. The following training initiatives have recently been completed or are well under way:

1. During the week of December 4-8, 2006, the FBI Center for Intelligence Training in Quantico, VA provided Intelligence Analyst Training for 20 BOP staff assigned as Special Investigative Agent and Linguists from ADX

Florence, Colorado; Intelligence Officers and Intelligence Research Specialists from the Joint Intelligence Sharing Initiative (JISI); the BOP's Chief of Intelligence, Central Office; the Chief, Intelligence Analysts, and Linguists from the Counter Terrorism Unit, Martinsburg, WV; and the Deputy Chief of the Sacramento Intelligence Unit.

2. The FBI held the 2006 National CII Coordinators Conference on December 12-13 at the National Counter Terrorism Center in McClean, Virginia. This training was based on the "train the trainer" concept. CII Coordinators from each FBI field office who will conduct the outreach and training for all correctional agencies within their geographical area, to include BOP facilities were in attendance.

3. An electronic communication (EC) issued on December 7, 2006 which directed all FBI field offices to develop formalized CII Outreach and Training Plans by March 1, 2007. Field offices were directed to include target dates, performance measures, CII program updates, and required reporting dates.

Progress continues to be made in the following areas:

- Continued FBI support of BOP intelligence needs with regard to vetting and screening of contractors and volunteers, information on terrorist offenders entering BOP custody, and special monitoring of BOP offenders under Special Administrative Measures (SAMs) controls.
- Continued comprehensive access to FBI resources through BOP staff assigned to the National Joint Terrorism Task Force (NJTTF) and respective JTTFs.
- FBI support to the new BOP Counterterrorism Unit (CTU) recently opened in Martinsburg, WV. Specifically, the FBI will assess the staffing of two personnel and identify necessary databases to support the mission.
- Provide guidance to all FBI field offices to clarify and expand intelligence sharing initiatives regarding terrorism matters between the FBI, BOP, and other state, county, and private correctional agencies.
- Provide continued CII training at various state, regional and national conferences. Completed CII training at recent conferences which BOP attended have included the 2006 Major Gang Task Force National Training Conference in Indianapolis, IN on September

12, 2006; FBI Boston regional training conference on September 28, 2006; and the FBI Atlanta regional conference on December 18, 2006. A CII presentation will also be made at the pending American Correctional Association (ACA) Winter Conference in Tampa on January 24, 2007, and as well as the scheduled National JTTF Conference during fiscal year 2007.

- The FBI will continue to support BOP efforts regarding internal intelligence training by providing speakers and resources as appropriate.

We believe the above noted steps will help ensure that the FBI continues our current emphasis on our ever-expanding intelligence partnership with the BOP regarding terrorism matters.

Sincerely,

Joseph Billy, Jr.
Assistant Director
Counterterrorism Division