



**Congressional Affairs Office**  
**Congressional Contacts**

ALL INFORMATION CONTAINED  
HEREIN IS UNCLASSIFIED EXCEPT  
WHERE SHOWN OTHERWISE

Date Entered:   Briefing  Hearing  Other  FOC

Event Date:

Subject:

CAO Contact Person:

DOJ Notification:  DOJ Date/Time:

FBI Participants:

Other Participants:

Committees /Subcommittees:

Members/Staff:

b6  
b7C

**Details of Briefing:**

(S)

b1

**Follow Up Action:**



**U.S. Department of Justice**  
**Office of Legislative Affairs**

Office of the Assistant Attorney General

*Washington, D.C. 20530*

October 3, 2005

The Honorable Pat Roberts  
Chairman  
Select Committee on Intelligence  
United States Senate  
Washington, D.C. 20510

Dear Mr. Chairman:

This responds to your letter of May 6, 2005, posing questions arising from the April 27, 2005, appearance of FBI director Robert Mueller before the Committee concerning the impact of the USA PATRIOT Act on intelligence community operations and national security investigations. We have enclosed responses to those questions.

Thank you for the opportunity to present our views. Please do not hesitate to call upon us if we may be of additional assistance. The Office of Management and Budget has advised us that from the perspective of the Administration's program, there is no objection to submission of this letter.

Sincerely,

A handwritten signature in cursive script that reads "William E. Moschella".

William E. Moschella  
Assistant Attorney General

Enclosure

cc: The Honorable John D. Rockefeller IV  
Vice Chairman

EFF Section 215-116

**Responses of the Federal Bureau of Investigation  
Based Upon the April 27, 2005 Hearing Before the  
Senate Select Committee on Intelligence  
Regarding the USA PATRIOT Act**

**Questions Posed by Vice Chairman Rockefeller**

The following questions request the Department of Justice's and FBI's comments on a number of specific provisions in Section 4 of S. 737, the Security and Freedom Enhancement Act of 2005, or SAFE Act. Section 4 of S. 737 would amend Section 501 of the Foreign Intelligence Surveillance Act. The current text of Section 501 was added by Section 215 of the PATRIOT Act. The questions will summarize the provisions of S. 737, § 4, but, of course, the full text of them in S. 737 should be considered.

**1. S. 737, § 4(b) - Orders**

S. 737, § 4(b), proposes adding a requirement to Section 501 of FISA that any order under it not contain a requirement that would be held unreasonable or privileged from disclosure if contained in a subpoena duces tecum issued by a U.S. court in aid of a grand jury investigation of espionage or international terrorism.

Please comment on the proposal. Please suggest alternative language, if any, that you believe would better ensure that Section 501(c) orders do not require unreasonable or privileged disclosures.

**Response:**

The Department's views regarding the proposed SAFE Act were provided by letter dated July 12, 2005, from Attorney General Gonzales to Senator Specter, Chairman of the Senate Judiciary Committee. While this letter is not limited to a discussion of Section 4 of the proposed Act, that discussion can be found at pages 5-9 of the letter. We have attached the letter for your convenience.

**2. S. 737, § 4(c) - Nondisclosure**

S. 737, § 4(c), proposes amending the provision of Section 501 on nondisclosure. In addition to permitting disclosure to an attorney in order to obtain legal advice regarding the order, the proposed amendment would establish an initial 180-day limit on nondisclosure to others. It would provide that the FBI or other designated FBI official may apply to the FISA court for an order extending nondisclosure for an additional, renewable 180 days. Among the standards for an extension would be that disclosure would seriously endanger U.S. national security by alerting a target, a target's

associates, or a foreign power to the Government's interest.

Please comment on the proposal, including your assessment of whether there is a legitimate interest of recipients of Section 501 orders in advising customers, in the absence of a national security reason, that records pertaining to them have been provided to the Government. Please suggest alternative language, if any, that you believe would better address the concern that is the subject of the proposed amendment.

Response:

Please see the response to Question 1, above.

3. S. 737, § 4(d) - Judicial Review

S. 737, § 4(d), proposes amending Section 501 of FISA by providing for judicial review of orders for production under that section. Page 6 of the Attorney General's and FBI Director's statement states that the Department of Justice is willing to support an amendment to Section 215 (Section 501 of FISA) that clarifies that an order may be challenged in court.

Please comment on the specific language for judicial review proposed in this section. Please suggest alternative language, if any, that you believe would better provide procedures for judicial review.

Response:

Please see the response to Question 1, above.

4. S. 737, § 4(e) - Use of information

S. 737, § 4(e), proposes adding a new provision to Section 501 of FISA on the use of information obtained pursuant to a Section 501 order. Among other matters, the proposed new provision would require a pretrial or prehearing disclosure to an individual whenever the United States intends to enter into evidence, in any court or agency proceeding against that individual, a tangible thing or information obtained pursuant to a Section 501 order. The "aggrieved person" would then have an opportunity to move to suppress the evidence on the ground that it had been obtained in violation of the Constitution or laws of the United States.

Please comment on the proposal for disclosure and judicial review of the use in formal proceedings of things or information obtained pursuant to Section 501 orders. Please suggest alternative language, if any, that you believe would better address the objective of the proposed amendment.

**Response:**

Please see the response to Question 1, above.

**Questions Posed by Senator Wyden**

**5. Mr. Mueller, in explaining your previous remarks to the Senate Judiciary Committee, (in which you said that the FBI has obtained library records in intelligence investigations after "discreet inquiries" by agents) you said that you were referring to incidents in which librarians contacted the FBI to report suspicious behavior. Have there been any cases in which these inquiries were initiated by FBI agents? If so, do you know how many?**

**Response:**

Many aspects of investigations are recorded and centrally reported (including investigation results such as arrests, indictments, and asset forfeitures, as well as investigative techniques such as the use of informants, consensual monitoring, and electronic surveillance). However, not all investigative details are reported, and the FBI does not track whether Special Agents have initiated any "discreet inquiries" of libraries in intelligence investigations.

**6. Mr. Mueller, in your response to my question about what the FBI needs to initiate an investigation, you said that the FBI does not have a standard of proof. Please elaborate on your response. What must the FBI have in order to begin an investigation? What standard must be met in order to obtain a FISA warrant? What standard must be met in order to issue a National Security Letter? I would appreciate an unclassified response.**

**Response:**

*The Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection ("NSI Guidelines") dated 10/31/03, provide the framework for the FBI's national security investigations. The NSI Guidelines allow the FBI to use all lawful investigative techniques to protect the United States from international terrorism and espionage. These Guidelines direct that all FBI investigative activities must conform with the Constitution and all applicable statutes, executive orders (EOs), and regulations.*

The NSI Guidelines authorize three levels of FBI investigative activity (threat assessments, preliminary investigations, and full investigations), and provide clear and concise predication requirements for each level of authorized FBI investigative activity. Those specific predicates are found in the classified portions of the NSI Guidelines. (They are classified because they relate to

intelligence activities or intelligence sources or methods.)

Surveillance orders and search warrants under the Foreign Intelligence Surveillance Act (FISA) and National Security Letters (NSLs) are important tools that are used in FBI national security investigations. The government may seek authority to conduct FISA surveillance or searches if foreign intelligence gathering is a *significant purpose* of the surveillance or search. (50 U.S.C. § 1804(a)(9)(B) regarding electronic surveillance and § 1823(a)(7)(B) regarding physical searches). The government is obligated to demonstrate to an Article III judge sitting on the FISA Court that there is *probable cause* to believe that the target is a foreign power or an agent of a foreign power and that the facilities or premises sought to be monitored or searched are being used by the foreign power or agent of the foreign power. (50 U.S.C. § 1805(a)(3) and 50 U.S.C. § 1824(a)(3).)



Outside the Scope

#### Questions Posed by Senator Mikulski

**There are a lot of concerns among the American people about guarding their privacy even as the federal government tries to protect the nation's security. We need to address these concerns as clearly and as completely as possible.**

**Please elaborate on the answers that you gave to my questions at the Committee hearing on April 27, in a manner that would be clear to the American public. When I use the word "spy" here I mean to include the various methods that intelligence agencies use to obtain information about or from individuals.**

**7. Which agencies with intelligence authority in the federal government can "spy on" U.S. citizens or place them under surveillance?**

**8. Please detail the circumstances under which such "spying" or surveillance can occur.**

**9. Please list the categories of information federal agencies can collect in carrying out such surveillance.**

10. What safeguards are in place in the law and in federal agency policy to protect U.S. persons from unauthorized and/or illegal spying? Please specify which of these safeguards are applicable to the FBI, the CIA, the NSA, and any other part of DoD intelligence.

11. Director Mueller testified that generally the CIA and NSA "are not allowed to spy on or to gather information on American citizens, but that there are limited exceptions to that." Please elaborate.

Response to Questions 7-11:

Every law enforcement entity within the United States (state, local, tribal, and federal) has the authority to engage in at least some forms of surveillance. Surveillance is the most basic of all law enforcement techniques and can range from activity to which no reasonable person would object and few would characterize as "spying" (such as a police officer observing a drug sale on the street) to highly sophisticated electronic surveillance, which might be characterized by some as "spying."

The U.S. Intelligence Community (USIC) includes the Office of the Director of National Intelligence, Central Intelligence Agency, National Security Agency, National Geospatial-Intelligence Agency, National Reconnaissance Office, FBI, Defense Intelligence Agency, and intelligence elements of the Departments of Defense, State, Treasury, Homeland Security (which includes the U.S. Coast Guard), and Energy. EO 12333 (1981) provides the primary guidance regarding the USIC members' authority to conduct investigations in the U.S. EO 12333, Part 2.4, states in part:

Agencies within the Intelligence Community shall use the least intrusive collection techniques feasible within the United States or directed against United States persons abroad. Agencies are not authorized to use such techniques as electronic surveillance, unconsented physical searches, mail surveillance, physical surveillance, or monitoring devices unless they are in accordance with procedures established by the head of the agency and approved by the Attorney General. Such procedures shall protect constitutional and other legal rights and limit use of such information to lawful governmental purposes.

For an explanation of the authorities possessed by other members of the USIC, those entities should be consulted directly.

Within the FBI, Attorney General (AG) Guidelines provide the framework for the use of the various surveillance techniques. Without providing classified information, we note that different types of investigations are conducted under the AG's Guidelines on General Crimes, Racketeering Enterprise, and Terrorism Enterprise Investigations (hereafter "General Crimes Guidelines") and under the AG's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection (hereafter "NSI Guidelines"): preliminary inquiries and full investigations are conducted under the General Crimes Guidelines, whereas threat assessments, preliminary investigations, and full investigations are conducted under the NSI Guidelines. As the level of predication increases, the surveillance techniques available include more intrusive techniques. Put differently, if the FBI possesses very little information that a person is involved in wrongdoing, the techniques available to investigate the person pursuant to the General Crimes Guidelines or the NSI Guidelines are generally limited to non-intrusive techniques (e.g., review of public source information and FBI files). On the other hand, if the FBI has significant information that a person is a terrorist, spy, or racketeer, more intrusive techniques are available including, for example, the ability to ask a court for authority to conduct electronic surveillance.

Under the General Crimes Guidelines, absent predication to open an investigation (i.e., facts tending to suggest that a crime has been, is being, or is about to be committed), the FBI can attend public events and engage in surveillance at those events only for the purpose of detecting or preventing terrorism or assessing a threat to national security. Even in those very restrictive circumstances, the FBI is limited to collecting information that is observable by the general public.

The "categories" of information the FBI can collect through surveillance, whether in connection with a criminal investigation or a national security investigation, are limited primarily by what is being investigated and the scope of FBI's legal authority. For example, if the FBI is investigating a person who is suspected of being a loan shark, the FBI could engage in physical surveillance (to watch him collect payments and to see with whom he appears to be splitting his proceeds), it could use a grand jury subpoena to obtain his bank records (to see if cash is flowing in and out of his accounts and whether his finances appear consistent with his standard of living), and it could, with the approval of a court through an ex parte order issued pursuant to 26 U.S.C. § 6103, obtain his tax records to further determine whether he was declaring income consistent with the apparent value of his loan-sharking operation and his standard of living. If the FBI could demonstrate probable cause and satisfy the other requirements for obtaining a Title III wiretap, we could listen to his telephone conversations as provided in the Title III order. That order would not, however, permit us to listen to his children talk to their friends (unless they were talking about their father's loan-sharking business). In short, we could collect a substantial amount information on the



suspect and his finances.

On the other hand, if the FBI were investigating the same person for violating 18 U.S.C. § 247, under which it is unlawful to intentionally destroy religious property, most of the information we could collect on the suspected loan shark would be unavailable to us. We would almost certainly be unable to obtain the suspect's tax records, as there is almost no possibility they would be relevant to the question of whether he destroyed religious property. If the only crime being investigated were an 18 U.S.C. § 247 violation, we could not obtain Title III electronic surveillance coverage of his home telephone, because 18 U.S.C. § 247 is not a crime that can be investigated using this technique. We are highly likely to talk to neighbors and friends to gather information concerning the suspect's attitude toward the attacked religion, a line of questioning that would be inappropriate during investigation of a suspected loan shark. Further, if we had information that injuries were sustained during the destruction of religious property, we might seek the suspect's emergency room or other medical records for the relevant period. In contrast, medical records on the suspected loan shark would likely not be relevant and therefore could not be obtained.

Safeguards in place to protect U.S. persons from unauthorized surveillance arise from both law and policy. The most protective safeguard is provided by the United States Criminal Code: it is a felony to engage in unauthorized wire, oral, or electronic surveillance (18 U.S.C. § 2511); a misdemeanor to install a pen register without authority (18 U.S.C. § 3121); a felony to conduct electronic surveillance under color of law except as provided by statute (50 U.S.C. § 1809); and a felony to conduct a search under color of law for foreign intelligence information except in compliance with FISA (50 U.S.C. § 1827). Additionally, EO 12333 authorizes the FBI to conduct intelligence activities within the United States in accordance with "such regulations as the Attorney General may establish" using the "least intrusive means feasible." As indicated above, the AG has issued guidelines that govern the FBI's conduct in both national security investigations and criminal investigations. Both sets of guidelines require that all FBI investigative activities conform with the Constitution and applicable statutes, EOs, and regulations.

The safeguards applicable to national security investigations provide an example of the safeguards applicable to all investigations. The FBI may obtain electronic surveillance or physical search orders from the Foreign Intelligence Surveillance Court (FISC) to monitor suspected terrorists or spies only if gathering foreign intelligence is a significant purpose of the surveillance or search and there is probable cause to believe both that the suspected terrorist or spy is an agent of a foreign power (as defined by 18 U.S.C. § 1801(b)(1)) and that the facilities or premises sought to be monitored or searched are being used or are about to be used by an agent of a foreign power. FISA also requires that any authorized

surveillance or search be conducted pursuant to "minimization" procedures approved by the AG and the FISC. Those procedures limit the FBI's acquisition, retention, and dissemination of communications involving U.S. persons. All FISA orders include a requirement of compliance with those procedures.

FISA pen register and trap and trace devices are minimally invasive preliminary investigative tools and are also quite useful to FBI intelligence investigators. Pursuant to FISA, the FBI can obtain a FISA pen register/trap and trace order if "the information likely to be obtained is foreign intelligence information not concerning a United States person or is relevant to an ongoing investigation to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution." (50 U.S.C. § 1842(c)(2)). These devices record addressee data on incoming and outgoing communications, such as the telephone numbers that call, or are called by, other telephone numbers. While these are not used to record the substantive content of communications, they do provide important information regarding the frequency and duration of the contacts between a subject and his confederates.

In addition, NSLs may be issued to obtain telephone and electronic communications records from telephone companies and Internet Service Providers (pursuant to the Electronic Communications Privacy Act), records from financial institutions (pursuant to the Right to Financial Privacy Act), and information from credit bureaus (pursuant to the Fair Credit Reporting Act) when this information is relevant to an FBI national security investigation.

Finally, as has been discussed in detail during USA PATRIOT Act hearings, the FBI may apply for a Section 215 order from the FISC requiring production of any tangible thing, such as a business record, if the item is relevant to an ongoing authorized FBI national security investigation. Through March 30, 2005, the FBI has used Section 215 to obtain orders directing the production of drivers' license records, public accommodation records, apartment leasing records, credit card records, and subscriber information for telephone numbers captured through court-authorized pen register and trap and trace devices. Greater privacy protections apply to Section 215 orders used in national security investigations than apply to the instruments used to obtain similar information in routine criminal investigations. The FBI cannot use Section 215 of the USA PATRIOT Act to gather even the most innocuous information (e.g., a copy of a driver's license) without prior judicial approval. Section 215 also explicitly provides that investigations of U.S. persons conducted under that authority may not be conducted solely on the basis of activities protected by the First Amendment. In contrast, basic documentary evidence gathered during a criminal investigation is generally obtained through the use of grand jury subpoenas, which are issued by

U.S. Attorney's Offices with no judicial oversight, unless the recipient moves to quash or the U.S. Attorney's Office needs the help of the court to enforce compliance.

ALL INFORMATION CONTAINED  
HEREIN IS UNCLASSIFIED  
DATE 04-13-2012 BY 65179 DMH/STP/MJS

# **ENCLOSURE**

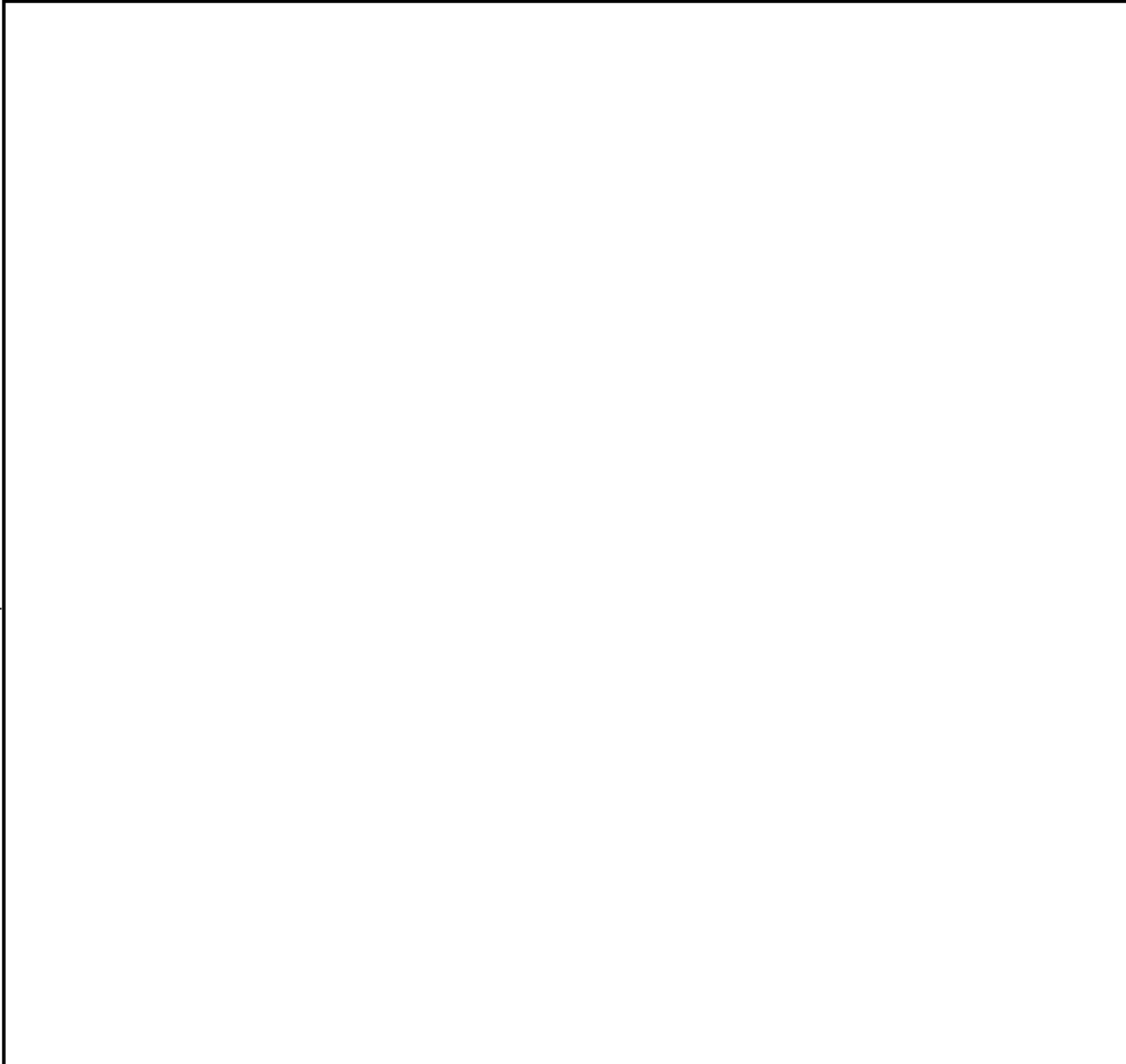
## **QUESTIONS 1-4**

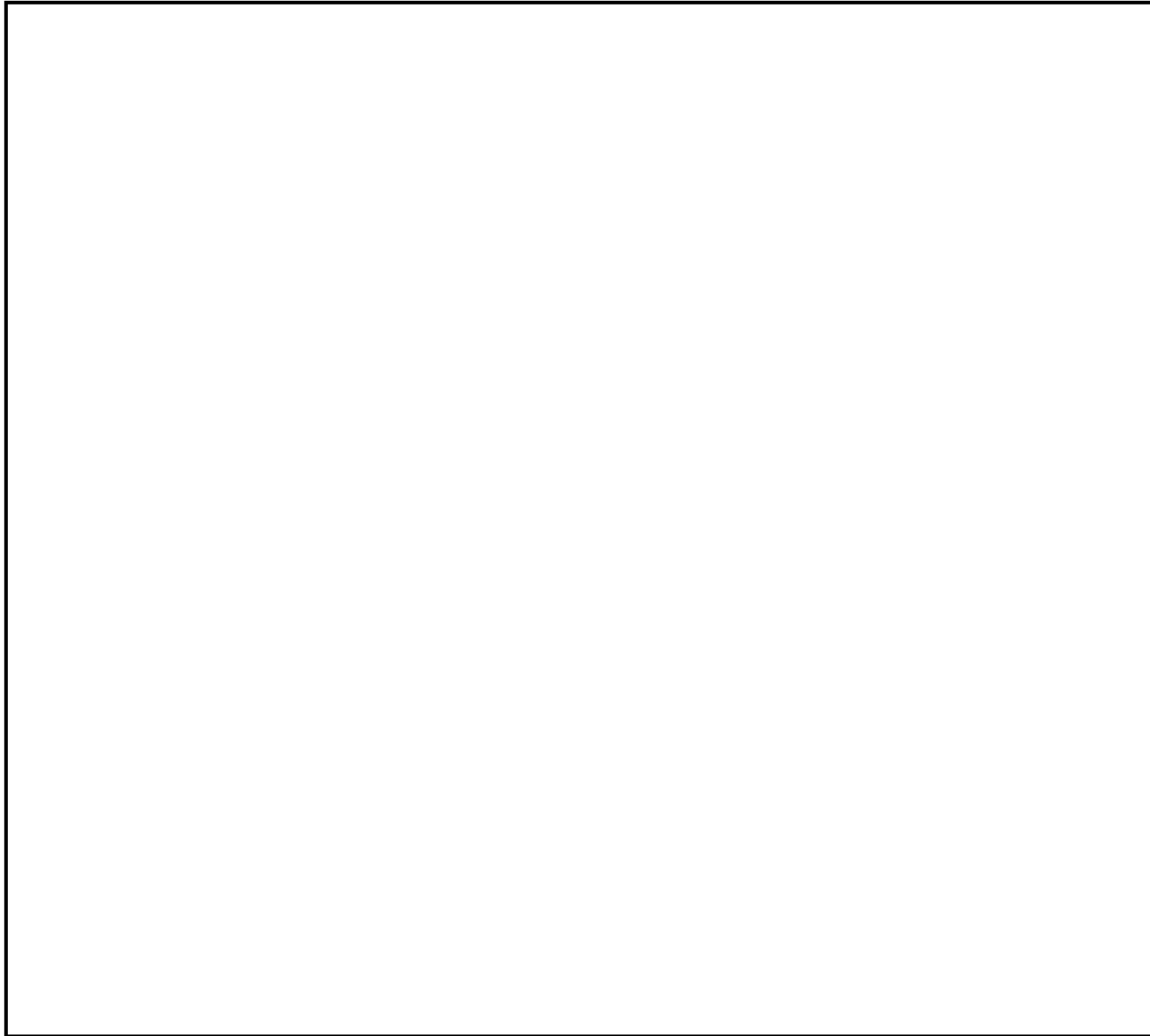
**7/12/05 SAFE Act Views Letter**

**Responses of the Federal Bureau of Investigation  
Based Upon the April 21, 2005 Hearing Before the  
Senate Select Committee on Intelligence  
Regarding Practical Application of the USA PATRIOT Act**

Outside the Scope

**Questions Posed by Chairman Roberts**





**4. Does the FBI need administrative subpoena authority to further its national security investigations? How useful would a national security administrative subpoena provision be if it could only be used in emergency situations?**

**Response:**

The absence of authority to issue administrative subpoenas stands as an impediment to efficiently and effectively protect the country from terrorist attack. When the FBI needs records from third parties in order to advance our national security investigations, we can either use a national security letter or obtain an order issued by the FISC pursuant to PATRIOT Act Section 215. Although both are effective means of obtaining materials, neither is as efficient as an administrative subpoena would be. One of the biggest challenges we face is the

need to make the most effective use of our human resources. We believe that if we had the authority to issue administrative subpoenas in national security investigations, the person-hours devoted to obtaining basic documents in our investigations would be significantly reduced without a corresponding decrease in the protection of civil liberties. The savings in person-hours would be realized because we would no longer need to routinely prepare paperwork appropriate for a submission to a court or to deal with the difficulties of serving a classified order on an uncleared document custodian (in the case of a 215 Order). Although a classified order can be served on an uncleared custodian, the process can be time-consuming, as some custodians are uncomfortable with the process used in that circumstance. This procedure can also impose added costs on the custodian if he or she wishes to obtain legal advice on whether it is appropriate, for example, to sign a trust receipt in lieu of obtaining a copy of the actual order.

Authorizing the FBI to use administrative subpoenas only in cases of "emergency" would provide the FBI with a mechanism to obtain documents when time is known to be of the essence, but it would not resolve the human resource issues nor the difficulties in dealing with classified documents. Moreover, it would introduce into the process the need for agents to ascertain on the spot whether a particular situation is an "emergency." Having to make that sort of decision creates the possibility of agents being second guessed no matter which way they proceed. Moreover, as a general rule, investigative tools are either available to agents or not available, with "emergency" provisions dictating only the process by which a tool can be used (see, e.g., 18 U.S.C. § 3125 (emergency pen register); 18 U.S.C. § 2518 (7) (emergency Title III authority); 50 U.S.C. § 1805 (f) (emergency FISA electronic surveillance)). It would be an anomaly, therefore, to grant the FBI the authority to issue administrative subpoenas only in an "emergency."

#### Questions Posed by Vice Chairman Rockefeller

**5. On May 24, 2004, the FBI issued a public apology to Brandon Mayfield and his family. In the course of the Committee's current PATRIOT Act hearings, the Committee has been told that in the last month or so, the Justice Department or the FBI notified Mr. Mayfield, or his counsel, that a FISA search of his home had been conducted.**

**Please provide a narrative, including a chronology, of the principal events concerning Brandon Mayfield. With respect to the search or searches, describe the authority under which it was or they were conducted, the factual representations that were made in support of the search or searches, the premise or premises that were searched, what was taken or copied, and when the search or searches were conducted.**



**7. Can you please provide us with descriptions of specific cases in which the FBI has sought a FISA order for “business records” under Section 215 of the USA PATRIOT Act since its passage?**

**a. First, as a matter of background, how many Section 215 orders have been obtained? How many are in the pipeline?**

**Response:**

As Attorney General Gonzales testified on April 5, 2005, the FBI had obtained 35 section 215 orders as of March 30, 2005.

Additional information responsive to this question is classified and is, therefore, provided separately.

**b. What kinds of records have been sought? From what kinds of organizations? In the context of what kinds of investigations?**



**Response:**

Attorney General Gonzales' April 5, 2005, testimony advised that the 35 section 215 orders obtained as of March 30, 2005, were for drivers' license records, public accommodation records, apartment leasing records, credit card records, and subscriber information, such as names and addresses for telephone numbers captured through court-authorized pen register and trap and trace devices.

Additional information responsive to this question is classified and is, therefore, provided separately.

**c. Please describe the two or three largest bod[ies] of records that have been obtained under a Section 215 order? The records of how many US persons were involved in those matters?**

**Response:**

This response is classified and is, therefore, provided separately.

**d. What steps does the FBI take to protect the privacy of U.S. persons whose records are acquired pursuant to a Section 215 order?**

**Response:**

As issued by the FISC, section 215 orders direct third-party recipients not to disclose the orders or their contents to any person except as necessary to produce the things required under the order. These orders also direct recipients not to disclose, except as necessary, that the FBI has obtained these things. DOJ has taken the position, however, that third-party recipient of a section 215 order may discuss the matter with an attorney. The non-disclosure requirement thus operates, in part, to protect the privacy of those whose records are sought through section 215 orders.

The FBI recognizes that the national security must be protected in such a manner as to fully honor individual civil liberties. Thus, while we have an obligation to gather and analyze information that is relevant to national security investigations, we are also obligated to protect the privacy of that information, particularly as it pertains to United States citizens. We are especially mindful of that obligation because investigative techniques typically result in the acquisition of both exculpatory information (which we use to clear innocent parties from suspicion) and inculpatory information (which is used to develop additional leads and, ultimately, for prosecution in appropriate cases). When we are able to narrow the focus of a request, we do so. When we are unable to narrow the focus of a request without losing the ability to obtain the information we need, we must exercise

discretion. The information obtained through our investigations must be maintained in a manner that both serves the nation's security interests and protects the privacy rights of U.S. citizens.

Additional information responsive to this question is classified and is, therefore, provided separately.

**8. We have been advised that the Director of the FBI has placed a heavy emphasis on the importance of acquiring FISA orders in pursuing terrorists and spies.**

**a. What is done to ensure that FISAs are sought according to reasonable priorities?**

**Response:**

This response is classified and is, therefore, provided separately.

**b. How is the productivity of a FISA order measured?**

**Response:**

The productivity of FISA coverage is measured qualitatively, which makes its measurement one of the most difficult aspects of FISA management. The value of foreign intelligence is measured by its contribution to the discovery of activity or information related to international terrorism, counterintelligence, or other threats to the national security that would not be otherwise detectable. This intelligence allows for better threat reporting, which in turn generates new leads and ultimately permits the development of operational information relevant to national security investigations.

**c. Who decides that a FISA order does not need to be renewed? Are there disincentives for FBI officials who must decide whether or not to pursue a FISA order renewal or a FISA order initiation?**

**Response:**

The FBI field office conducting an investigation and FISA program managers at FBI Headquarters decide jointly whether a particular FISA should be renewed based on their assessment of whether the FISA has been both productive and valuable to the overall investigation or whether it is likely to be in the future. Using their operational expertise, they balance the continued intrusion of the FISA technique against the potential for the collection of productive foreign intelligence.

Additional information responsive to this question is classified and is, therefore, provided separately.

**d. Please describe the specific role played by federal prosecutors in the FISA process today. Are prosecutors requesting FISA orders be sought to further criminal investigations?**

**Response:**

Federal prosecutors are not authorized to appear before the FISC and are not authorized to draft FISA applications. Accordingly, they cannot unilaterally decide to seek FISA coverage to advance criminal investigations.

Federal prosecutors do coordinate international terrorism investigations with FBI Agents from their earliest stages, and FBI Headquarters operational personnel meet regularly with the DOJ Criminal Division's Counterterrorism Section. This case coordination ensures that international terrorism investigators and criminal prosecutors are fully informed of investigative developments and that all appropriate investigative tools (including both national security and criminal tools) are brought to bear. While federal prosecutors have a role in investigations that may include FISA coverage, they may neither request FISA orders nor use FISA to avoid the Title III process. It is well understood throughout DOJ and within the FBI that FISA orders are available in national security investigations in order to gather foreign intelligence information in international terrorism and counterintelligence matters, not to conduct purely criminal investigations.

**e. What steps have been taken since September 11th to improve the process for post-collection processing and analysis for FBI FISA collection?**

**Response:**

Since September 11, 2001, the FBI has taken a number of steps to improve the post-collection processing and analysis of FISA data obtained through electronic surveillance (ELSUR). Primary among these is the development of the ELSUR Data Management System (EDMS). The FBI's FISA text collection is now primarily analyzed and translated using EDMS; eventually, all FISA audio and other data sources will be added to EDMS to create a common working environment for all FISA data.

The dual missions of EDMS are to implement a system architecture that vastly increases the FBI's ability to manage, analyze, and share FISA data and to integrate "best-of-breed" automated data analysis capabilities that greatly improve the efficiency with which investigators can develop leads and intelligence. EDMS serves as a comprehensive framework that integrates all FISA data collected by

the FBI, including digital media, telephone intercepts, audio recorded by microphones, and facsimile traffic, and facilitates the view and exploitation of this information from any FBI network computer. EDMS enhances the FBI's data management and sharing activities by providing a conduit for sharing appropriate data with other members of the USIC. Currently, all of the FBI's FISA email and other text intercepts are managed by EDMS. As the audio collection is added to the system, EDMS will not only greatly increase the productivity of the FBI's investigative, translation, and transcription efforts, but will also allow for a more effective and efficient exploitation and dissemination of collected intelligence.

The FBI has also instituted a process to ensure that all foreign language collection from FISAs is translated in accordance with clear priorities. The FBI's FISA Manager coordinates this and all other processes associated with FISA (including the FBI's compliance with USIC policy regarding priorities for FISA initiations) and serves as the primary liaison between OIPR and the FBI regarding FISA matters. The FISA Manager and DI's Language Services Section are working to create a universal report format that includes all of the data necessary to appropriately prioritize FISA assignments.

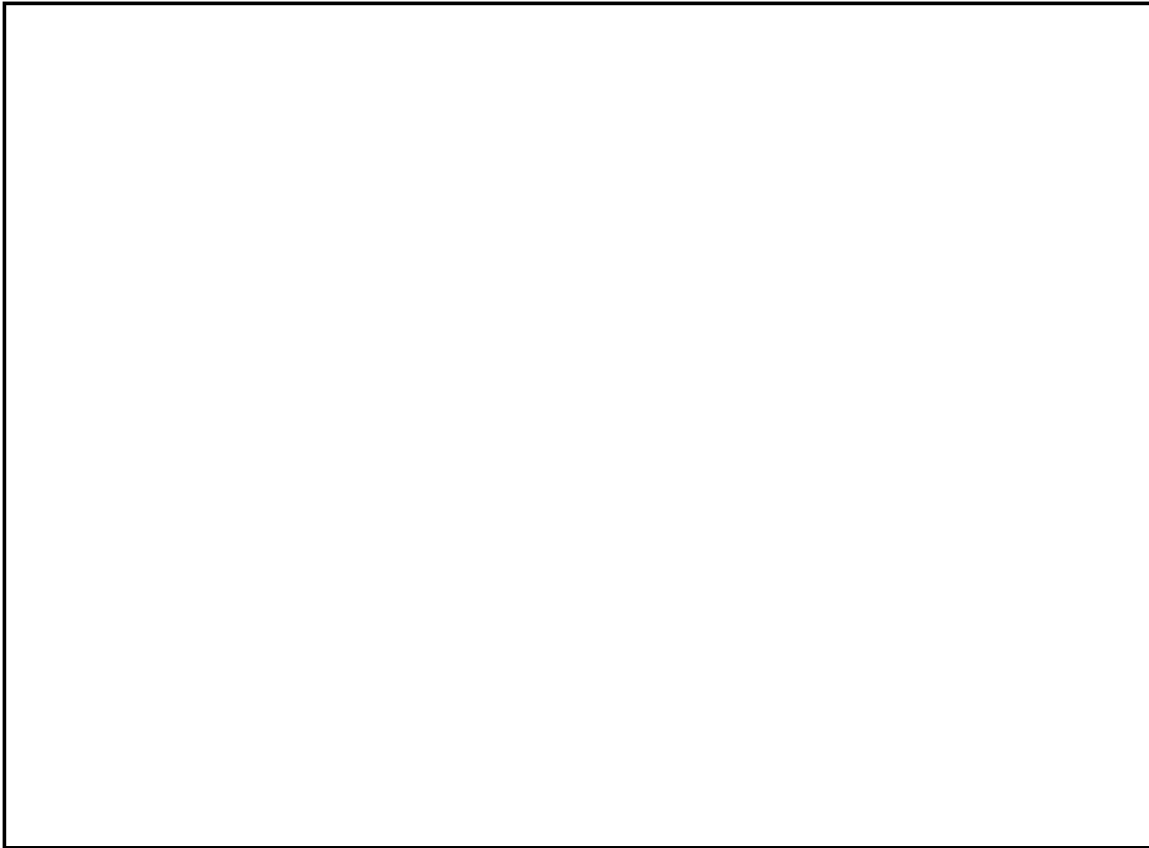
Prior to September 11, 2001, translation capabilities, like most other FBI programs, were decentralized and managed in the field. In order to provide centralized management and to increase the efficiency of the Foreign Language Program, the FBI created the Language Services Translation Center, which provides a command and control structure at FBI Headquarters to ensure that our translator resource base of over 1,300 translators, distributed across 52 field offices, is strategically aligned with intelligence priorities. This command and control structure is facilitated by a secure network that allows us to efficiently route FISA audio collection and translation tasks to any FBI field office.

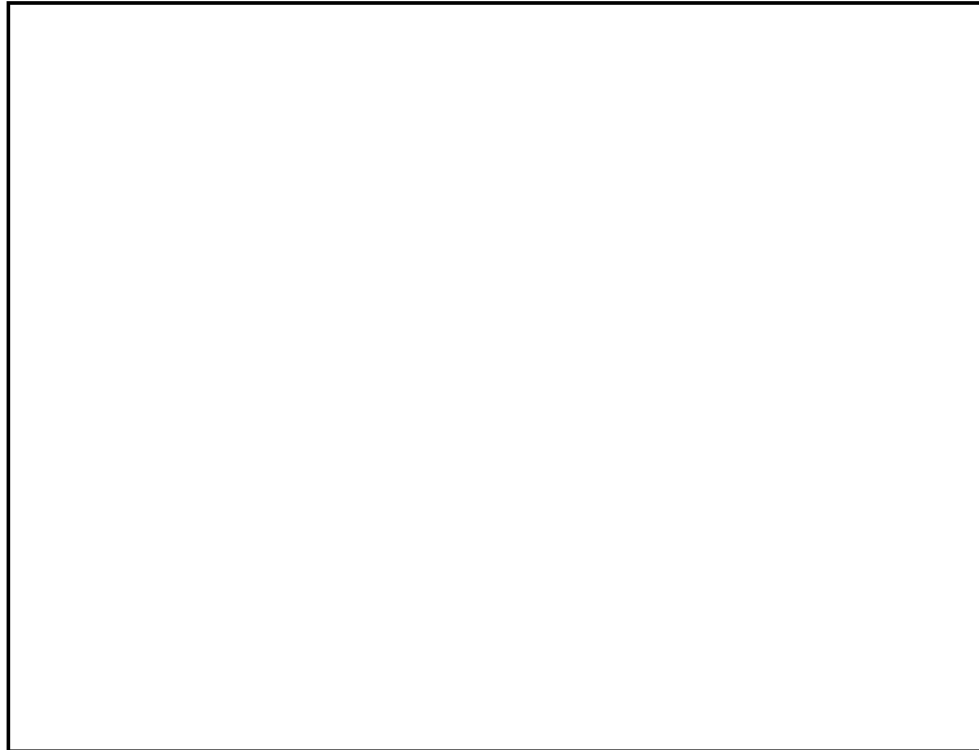
The FBI applies the intelligence priorities in the triage system used to review collected materials. This triage system provides for quick review of FISA collection by linguists in order to identify content requiring translation or summary. If a document or audio line contains a mixture of several languages, a linguist forwards this content to the appropriate linguists for review and summary. When intelligence collection contains English-language content, it is additionally routed through the FBI's English Monitoring Center for review and summary of pertinent English materials. This triage system allows FBI linguists to concentrate on the review, analysis, translation, and reporting of foreign language materials according to national security priorities.

Increased electronic connectivity has also streamlined the processing of FISA renewals to ensure the uninterrupted post-collection processing of data. The implementation of the FISA Management System has permitted the electronic transmission of FISA requests among FBI field offices, FBI Headquarters, and

DOJ's OIPR. The ability to e-mail classified FISAs, rather than sending multiple copies to field offices by means of secure facsimile, has expedited the renewal process.

As part of post-collection analysis, FISA-derived information is analyzed for its substantive content as well as for valuable location and biographical data. This analysis often results in actionable intelligence through which an integrated picture of an individual is developed, identifying the individual's potential terrorism associates, travel, meetings, logistical planning, operational activities, and, at times, future plans and intentions. The FBI provides FISA-derived information specific to overseas activities and operations to the CIA, the intelligence components of the Department of Defense, and the National Security Agency through an Intelligence Information Report (IIR) that is transmitted via operational cable. IIRs explain the importance of the FISA-derived information and request action by appropriate agencies. Since the establishment of an intelligence reporting mechanism within the FBI's CTD, more than 500 IIRs containing FISA information have been disseminated. Under appropriate circumstances, threat information obtained pursuant to FISA is provided in unclassified form to state and local governments.





**10. During the Committee's hearing on Tuesday, April 19, there was discussion about the PATRIOT Act's provisions concerning National Security Letters.**

**a. Please describe how the NSL provisions of the USA PATRIOT Act have been implemented by the FBI. How many NSLs have been obtained in counterterrorism investigations? When would a NSL be sought as opposed to a Section 215 "business record" FISA?**

**Response:**

The PATRIOT Act included amendments to FISA that altered the standard necessary to use NSLs. Prior to those amendments, the FBI could generally use an NSL only if specific and articulable facts indicated that the person to whom the records related was a foreign power or an agent of a foreign power. Put differently, the FBI had to reach a defensible determination that the target was a terrorist or spy before we could gather the basic information needed to determine whether the person was a terrorist or spy. As a result of the PATRIOT Act, an NSL is now available if the materials sought will be relevant to a national security investigation.

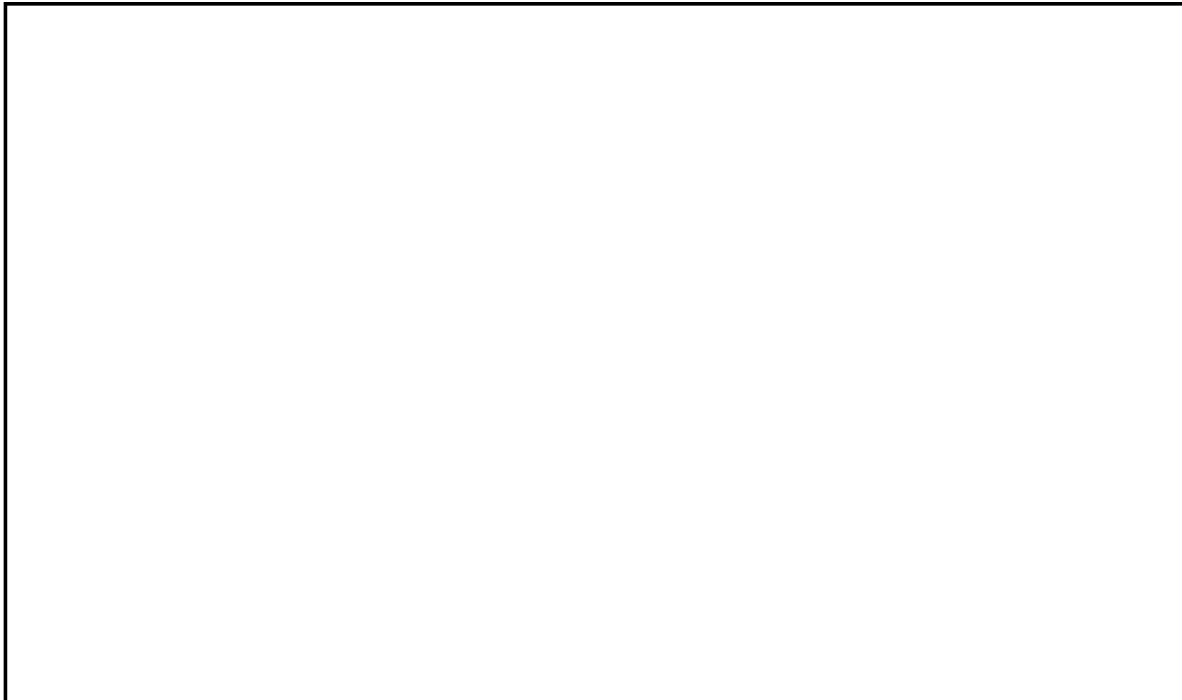
In order to implement these changes, the FBI's OGC issued FBI-wide guidance notifying investigators of the change in the standard for using NSLs (Electronic

Communication to the field, subject: "New Legislation, Revisions to FCI/IT Legal Authorities, National Security Letters," dated October 26, 2001). In addition, OGC revised the standard form used to obtain NSLs. The guidance and the new form made it clear that NSLs could be issued only when the information sought was relevant to a national security investigation.

NSLs may be used only to obtain certain information from wire and electronic communications service providers, financial institutions, and credit reporting companies, whereas section 215 orders can be used to obtain "any tangible things (including books, records, papers, documents, and other items)." As a general rule, because NSLs can usually be issued from the field office and are not classified, if an NSL can be used to obtain the documents needed for an investigation, then an NSL is used. If investigators are seeking documents not obtainable through an NSL, then a section 215 order is used. To date, the only exception to this general rule has been our practice of pairing a section 215 order with a FISA pen register/trap and trace to obtain subscriber information for all numbers dialed to or from the target telephone. In that instance, there is no loss of efficiency in using a section 215 order to obtain records that are also available through an NSL, because the pen register must be processed through FBI Headquarters in any event.

Outside the Scope

Additional information responsive to this question is classified and is, therefore, provided separately.



## **ENCLOSURE A**

### **QUESTION 1**

**MAY 6, 2005, LETTER FROM DOJ AAG MOSCHELLA  
TO SENATE SELECT COMMITTEE ON INTELLIGENCE**



## **ENCLOSURE B**

### **QUESTION 2**

**MAY 18, 2005, LETTER FROM DOJ AAG MOSCHELLA  
TO SENATE SELECT COMMITTEE ON INTELLIGENCE**

[REDACTED] (RMD)(FBI)

b6  
b7c

**From:** [REDACTED] (OCA) (FBI)  
**Sent:** Monday, August 22, 2005 6:54 AM  
**To:** [REDACTED] (OGC) (FBI); THOMAS, JULIE F. (OGC) (FBI); [REDACTED]

**Cc:**  
**Subject:** Conferee Letter on Patriot Reauthorization Letter  
**Attachments:** 8 17 05 Conferee letter on PATRIOT Reauthorization letter (JMM clean).doc  
**Importance:** High  
**Follow Up Flag:** Follow up  
**Due By:** Tuesday, August 23, 2005 10:00 AM  
**Flag Status:** Flagged

**UNCLASSIFIED**  
**NON-RECORD**

The attached confree letter is being provided for review. Provide comments, if any, to OCA. Please indicate if your division is in favor or opposed to the confree letter, as well as the reasons for your division's position. If your division opposes the confree letter fully or in part, but believes that it can be remedied by changes in the verbiage, please describe in detail what should be added, deleted, or changed, including recommendations for substitute language sufficient to correct the objectionable section(s).

Please E-mail your comments to [REDACTED] **Your comments should be prepared in Microsoft Word format** which is suitable for dissemination to DOJ and to congressional staff. Please send these comments to the OCA contact person as an attachment to your E-mail. If you have additional comments which are not suitable for dissemination, please include them in the body of your E-mail separate and apart from the attachment. If your division is not taking a position and has no comments, please send an E-mail to the OCA contact person stating such.

**DEADLINE 10am 8-23-05.** We appreciate your attention to this matter.

**UNCLASSIFIED**



**U.S. Department of Justice**

Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

July 1, 2005

The Honorable Arlen Specter  
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 April 5, 2005. The subject of the Committee's hearing was "Oversight of the USA PATRIOT Act."

We hope that this information is helpful to you. 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,

A handwritten signature in cursive script that reads "William E. Moschella".

William E. Moschella  
Assistant Attorney General

Enclosure

cc: The Honorable Patrick J. Leahy  
Ranking Minority Member

EFF Section 215-182

**Responses of the Federal Bureau of Investigation  
Based Upon the April 5, 2005 Hearing Before  
The Senate Judiciary Committee  
Regarding "Oversight of the USA PATRIOT Act"**

**Questions Posed By Senator Grassley**

1. Director Mueller, during your testimony before the U.S. Senate Committee on the Judiciary on April 5, 2004 you described ways in which the USA PATRIOT Act has assisted the FBI with its efforts in the war on terror. In particular, you made reference to criminal enterprises frequent involvement and reliance on smuggling operations and how the sharing of current intelligence, based on information sharing between criminal, counterterrorism, and counterintelligence efforts has identified corrupt foreign officials, extremist organizations, and illegitimate and quasi-legitimate businesses actively involved in smuggling operations.

Specifically, you stated that,

"Alien smugglers frequently use the same routes used by drug and contraband smugglers and do not limit their smuggling to aliens, smuggling anything or anyone for the right price. Terrorists can take advantage of these smuggling routes and smuggling enterprises to enter the U.S. and are willing to pay top dollar to smugglers. Intelligence developed in these cases also frequently identifies corrupt U.S. and foreign officials who facilitate smuggling activities."

How is the Federal Bureau of Investigation (FBI) working, coordinating, and de-conflicting with the Department of Homeland Security and other federal law enforcement agencies with primary jurisdiction in the area of alien and contraband smuggling as not to contribute to duplication in non-terrorist related investigations?

**Response:**

Information sharing is critical in today's criminal, counterterrorism (CT), and counterintelligence (CI) environments. In July 2004, the Human Smuggling and Trafficking Center (HSTC) was established in Washington, D.C. The Center is a multi-agency venture designed to integrate, share, and disseminate intelligence

---

*These responses are current as of 4/29/05.*

pertaining to human smuggling and trafficking. The FBI is a full partner in the HSTC, the basic purposes of which are to insure that human smuggling and trafficking information is expeditiously shared, that resources are focused to disrupt and dismantle these criminal enterprises once they are identified, and that the appropriate law enforcement agencies are made aware of any ancillary crimes (counterfeiting, identity theft, narcotics, etc.). The HSTC is supportive in nature, consisting primarily of: facilitating the dissemination of intelligence; preparing strategic assessments; identifying issues that would benefit from enhanced interagency coordination and/or attention; and coordinating or otherwise supporting agency and interagency efforts in appropriate cases. In order to be effective, frequent interaction between the HSTC and the various contributing agencies is essential. To facilitate this coordination, the FBI has assigned a Supervisory Special Agent (SSA) and an Intelligence Analyst (IA) to the HSTC. These individuals share with the HSTC FBI intelligence obtained from the FBI's field Divisions and disseminate intelligence received through the HSTC (from the other participating agencies) back to these Divisions.

The FBI has also designated an SSA at FBI Headquarters (FBIHQ) as a point of contact for human smuggling and trafficking matters. This individual will insure that all human smuggling and trafficking matters are handled expeditiously and that all involved agencies are fully informed and included as partners in these investigations. This individual will also insure there is no overlap with FBI terrorism investigations and, in the event this should occur, will mediate these matters to resolve redundancies.

In addition to its participation in the HSTC, the FBI is currently working with the Department of Homeland Security (DHS) to complete a Memorandum of Understanding (MOU) which delineates investigative cooperation, intelligence sharing/dissemination, and other pertinent policies and procedures in smuggling investigations. This MOU is not designed to delineate each agency's responsibilities, but to foster better information sharing and increased interagency cooperation and coordination.

---

*These responses are current as of 4/29/05.*

**2. Besides the Joint Terrorism Task Forces (JTTFs), what specific "joint endeavors" does TFOS participate in with the Department of Homeland Security and the Department of the Treasury?**

**Response:**

In addition to the Joint Terrorism Task Forces (JTTFs), the FBI's Terrorist Financing Operations Section (TFOS) participates with DHS and the Treasury Department in several key joint endeavors to combat terrorism financing. These include the following.

- The Foreign Terrorist Asset Targeting Group (FTAT-G) operates as part of the National Security Council's (NSC's) Office of Combating Terrorism. Pursuant to the NSC's November 2004 "Restructuring Plan" and as agreed by the agencies participating in the Terrorist Finance Policy Coordinating Committee (TF PCC), the FTAT-G is led by a management team that includes the FBI (serving as Director) and DHS's Immigration and Customs Enforcement (ICE) (serving as Deputy Director). Established in 2002 to replace the Foreign Terrorist Asset Tracking Center, the FTAT-G also includes representatives of the Department of Treasury (Treasury), the Department of State (DOS), and other agencies in the United States Intelligence Community (USIC). The FTAT-G collects, coordinates, and synthesizes intelligence on selected targets to support the deliberations of the TF PCC, which coordinates government efforts to identify, prioritize, assess, and assist foreign governments' financial systems that are vulnerable to terrorist exploitation.
- United States Government's participation in Financial Action Task Forces (FATFs) is coordinated by Treasury's Office of Terrorism and Financial Intelligence, and includes the FBI's participation in FATFs and FATF-Style Regional Bodies (FSRBs) worldwide. Through this participation, the FBI can integrate the Treasury designation process, and the many other tools available in the war on terrorism financing, in their investigative efforts. The FBI also coordinates directly with Treasury's Financial Crimes Enforcement Network (FinCEN) for the purpose of data exploitation in terrorism financing matters.
- Additionally, the FBI is active in ad hoc groups, chaired by Treasury, DHS, or the FBI, dealing with regional terrorism financing issues, methods of terrorist financing, and value transfer systems. Of particular note is a current FBI/DHS/Treasury working group that focuses on the identification of the Informal Value Transfer System (IVTS) structure in the United States and how IVTSs are used to transfer money in and out of the United States.

---

*These responses are current as of 4/29/05.*

**3. How is non-terrorist related information, which is developed by the FBI pursuant to terrorism related initiatives, funneled to other federal law enforcement agencies in order to avoid redundancy and overlap in non-terrorist related criminal investigations?**

**Response:**

Non-terrorist related information that may be developed in the course of terrorism investigations is first evaluated to determine whether it may predicate a criminal investigation. If it does, and if the information warrants a joint investigation with another federal law enforcement agency, the information is passed to that agency through the JTTFs established within each FBI Field Office, and a joint investigation is undertaken. If the information appears to be solely within the jurisdiction of another federal law enforcement agency, the information is passed to that agency for its action. The same procedures are used to communicate with state/local law enforcement officials when the information indicates a non-federal crime.

**4. How many non-terrorism related investigations and or investigative leads has the FBI farmed-out to other federal law enforcement agencies with primary jurisdiction in specific non-terrorism related crimes (i.e. alien smuggling, contraband smuggling, export control, counterfeiting, identity theft, etc.)?**

**Response:**

The FBI does not collect information on the number of investigative referrals made to other agencies. However, the FBI is cognizant that information received by the FBI may be of critical interest to other government agencies and/or local law enforcement organizations. The FBI disseminates appropriate information to any federal, state, or local government and/or law enforcement agency connected with a criminal or intelligence investigation. Although FBI records do not identify the agency receiving the information, the program and/or criminal activity involved, or the outcome of such referrals, the estimated criminal intelligence disseminations by Fiscal Year (FY) are as follows (these totals reflect the documents uploaded into the FBI's Automated Case Support system).

- FY 2001 - 8,387
- FY 2002 - 7,461
- FY 2003 - 7,477
- FY 2004 - 8,148

---

*These responses are current as of 4/29/05.*

5. Pursuant to the Terrorism Financing Memorandum of Agreement (MOA) signed between the DOJ and DHS in May 2003, the FBI was mandated to wage a seamless, coordinated campaign against terrorist sources of financing. However, I am concerned that the infighting with other agencies, including DHS, continues to impede our ability to halt terrorist financing.

a. How exactly has the FBI's ability to investigate and combat terrorism financing improved since that time? How many terrorism financing cases has the FBI successfully prosecuted since the signing of the MOA?

Response:

Since the Memorandum of Agreement (MOA) was signed, TFOS has strengthened its terrorism financing investigative efforts through enhanced analytic capabilities, improved coordination among FBI field offices and with our state/local partners, and expanded data exploitation.

Since 2003, the number of JTTFs has increased from 73 to the current total of 103 nationwide. The JTTFs allow FBI and DHS personnel to work side by side on a daily basis. In addition, TFOS has established Terrorist Financing Coordinators in the FBI's field offices where the JTTFs are located. These Coordinators are specifically tasked with determining the most efficient and effective means of leveraging our joint resources to deter terrorist financing. To further enhance these efforts, TFOS plans to provide on-site terrorist financing training at each field office by the end of calendar year 2005.

At FBIHQ, TFOS has established the Proactive Data Exploitation Unit (PDEU), a specialized team of Special Agents (SAs) and analysts who use advanced technology and data exploitation techniques to provide both reactive and proactive support to terrorism and terrorist financing investigations. As discussed further in response to Question 9c, below, PDEU has led an effort to expand the data available through the FBI's Investigative Data Warehouse (IDW).

According to figures provided by the Department of Justice (DOJ), 21 U.S. Districts are actively pursuing material support charges in 96 CT investigations. To date, 395 indictments related to terrorism have been brought, leading to 212 guilty pleas or convictions. DOJ does not differentiate terrorism cases based on financing issues from other terrorism cases, because there is a financial component to most terrorism investigations and prosecutions.

---

*These responses are current as of 4/29/05.*



**b. How has the FBI taken advantage of and preserved ICE's expertise and capabilities, to further promote the U.S. Government's federal law enforcement campaign against terrorism financing? What initiatives and measures has the FBI undertaken, since the signing of the MOA, to recruit, train, and retain legacy Customs Agents?**

**Response:**

To foster the positive working relationship between senior ICE management and the FBI, the JTTF program has invited DHS's law enforcement components to join any JTTF, particularly encouraging DHS/ICE senior management to facilitate the participation of legacy Customs agents in the JTTFs in order to gain the investigative expertise they have acquired through their years of conducting customs investigations. By successfully incorporating these senior ICE investigators into the JTTFs, both agencies' investigations are more efficient and effective.

The success of the MOA is best evidenced by the fact that 311 ICE Agents have since been assigned to the JTTFs and continue their terrorism financing work in those positions. For example, former Customs Service "Operation Green Quest" criminal cases with a nexus to terrorism were transitioned to appropriate JTTFs and the participating ICE JTTF members continue to play significant roles in the investigation, including as lead case agents. ICE investigations that develop links to terrorism will continue to be referred to the FBI through TFOS, and ICE and TFOS will continue to coordinate investigative initiatives to identify financial system vulnerabilities and links to terrorist financing and terrorism.

**6. It is my understanding that there is considerable in-fighting between TFOS and International Terrorist Operations Section (ITOS) which is hindering the FBI's ability to effectively combat international terrorist financing. What is the FBI doing to resolve these problems and coordinate their operations?**

**Response:**

TFOS and the two International Terrorist Operations Sections (ITOS I and II) work together seamlessly, on a daily basis, in every aspect of CT investigations to successfully combat international terrorism. Both TFOS and ITOS have personnel embedded in Integrated Threat Teams, which enhances the FBI's integrated, team approach to the war on terrorism. Any questions concerning the allocation of responsibilities are resolved by senior Counterterrorism Division (CTD) officials. Every FBI employee is aware of the importance of the work we do on behalf of the American people, and every part of the FBI, including all units within CTD, works diligently to contribute to the war on terrorism. It is clear to all FBI employees that there

---

*These responses are current as of 4/29/05.*

is no room for in-fighting and that the decisions made by senior managers are in the best interest of the FBI's war on terrorism, not in the interest of any particular section or unit.

**7. Given the fact that there has been only a limited number of convictions related to terrorism and the difficulty in proving Title 18 U.S.C. 2339A and 2339B (providing Material Support to terrorists), how has the FBI utilized and pursued other powerful criminal statutes under the USA PATRIOT Act, Title 31 Bank Secrecy Act; and, specifically, Title 18 U.S.C. 981, 982, 1956, 1957 & 1960 in making a comprehensive and coordinated effort to stop terrorism and the flow of money to terrorist and the networks that support them?**

**Response:**

In carrying out its CT mission, the FBI utilizes all available statutory authorities. The JTTFs have been able to harness the investigative knowledge of their agents, investigators, and analysts to fully employ the authorities provided by Congress to pursue terrorist organizations. The state and local law enforcement officials assigned to the JTTFs bring additional investigative resources that would otherwise be unavailable to the federal effort.

For example, on 2/17/05, a federal grand jury in Eugene, Oregon, returned a three count indictment against the U.S. branch of the Al-Haramain Islamic Foundation, Inc. (AHIF) and two of its officers. The indictment includes violations of 18 U.S.C. § 371 (conspiracy to defraud the United States), 26 U.S.C. § 7206(1) (false IRS return by a tax exempt organization) and 31 U.S.C. § 5316(a)(1)(A) (failure to file report of international transportation of currency or monetary instrument). The indictment charges that the individual defendants conspired with the U.S. branch of the AHIF to defraud the U.S. Government by obtaining \$150,000 in funds intended for distribution to mujahideen in Chechnya, later concealing their intent by filing a false tax return, and subsequently failing to acknowledge they were transporting the funds out of the United States. If convicted, the two individual defendants may be sentenced to up to 8 and 10 years in prison. The indictment also seeks a forfeiture of \$130,000 by the U.S. branch of the AHIF. This investigation was conducted jointly by criminal investigators in the Internal Revenue Service, ICE, and the FBI.

---

*These responses are current as of 4/29/05.*

**8. How has the FBI implemented a coordinated law enforcement strategy with other federal, state, and local law enforcement agencies to combat the illicit flow of cash leaving the U.S. and, ultimately, funding terrorist and criminal organizations?**

**Response:**

The JTTFs are the primary method by which the FBI coordinates the law enforcement strategy to identify and stop the financing of terrorism and other criminal enterprises, using the capabilities of the participating law enforcement and intelligence agencies to quickly focus critical assets in order to fully investigate illegal financing schemes.

In addition to the coordination capability afforded by the JTTFs, FBI officials participate in regular meetings with their counterparts in other federal agencies at various levels, fostering intra-governmental liaison relationships that facilitate the joint effort to detect and disrupt plans to finance terrorism and other criminal activities. With specific respect to terrorist financing, TFOS continues to expand its existing relationships in the financial sector and to develop new sources of information in financial and other business entities, both formal and informal, including traditional financial institutions, debit and credit card companies, and money services businesses. In order to maximize the contributions of the FBI's law enforcement partners, the FBI provides training on a variety of topics (including terrorism financing) to federal, state, and local law enforcement agencies through National Academy courses at Quantico and numerous other training and outreach programs.

**9. The Department of Justice released a report last year regarding the FBI's analysis of alternative financing mechanisms in money laundering and terrorist financing cases and established a Program Management and Coordination Unit to analyze field data on alternative financing mechanisms.**

**a. Thus far, what trends have been found regarding alternative financing mechanisms and how is this information being utilized to initiate other terrorist financing investigations?**

**Response:**

Among the goals of the FBI's TFOS are to identify terrorist financing trends and techniques and to disseminate this information and intelligence within the FBI and to the FBI's JTTF partners. Specifically, TFOS's Program Management Coordination Unit (PMCU) was tasked to record the statistical data regarding terrorist financing. To this end, PMCU surveyed all JTTFs for specific information regarding investigations having a connection to terrorism financing, including

---

*These responses are current as of 4/29/05.*

financing methods, underlying criminal activity, and other issues specifically related to financing trends. TFOS is in the process of evaluating the results of this extensive project.

Terrorism financing methods range from the highly sophisticated to the extremely rudimentary. They include the use of both the formal banking system (including correspondent and private bank accounts and offshore shell banks) and informal banking systems (including Hawalas and bulk cash smuggling). The sources of terrorist funding range from relatively unsophisticated criminal activities such as identity theft and credit card fraud to the misuse of charities and other non-governmental organizations. As trends and patterns are identified, TFOS disseminates the information to the JTTFs for use in identifying similar trends and patterns in their jurisdictions. When appropriate, intelligence assessments and intelligence bulletins are prepared and distributed to members of the United States Intelligence Community.

**b. When will this information be made available to Congress and in what form?**

**Response:**

As indicated in response to subpart a, above, the PMCU is currently reviewing investigations having a connection to terrorism financing with the objective of identifying alternative terrorist financing mechanisms. Given the large amount of information being examined, PMCU will document in CTD files the progress of the analysis as well as the methodology used and the scope of the overall project. When this analysis is complete, TFOS will provide the trends and patterns in the use of alternative terrorism financing mechanisms to Congress, as well as to the law enforcement and intelligence communities.

**c. How is this information being shared with other agencies that have jurisdiction over other aspects of money laundering to ensure coordination and collaboration of our efforts?**

**Response:**

The data analysis is provided to law enforcement and intelligence agencies through the JTTFs via Intelligence Information Reports and other forms of written notification. To facilitate the analysis and promote information sharing, the FBI converts financial and other records into electronic, text-searchable documents through either optical scanning or manual data entry.

This information is included in the FBI's IDW, to which every JTTF has access. TFOS's PDEU is working with IDW to acquire and integrate additional relevant terrorism and non-terrorism data, to increase the number of FBI users with IDW access, and to enhance the ability of IDW to support FBI data analysis. To further these goals, PDEU has begun a number

---

*These responses are current as of 4/29/05.*

of proactive projects and initiatives, which have been enhanced by the technological advances made by the FBI and by the greater access to existing data afforded by these new systems, such as the IDW. These projects involve exploitation of existing FBI and other agency data to identify previously unknown or unrecognized connections between suspicious financial activities and terrorism related matters. During this past year, PDEU's effort has increased the number of data sets on the IDW more than fortyfold, resulting in the availability of more than 340 million searchable records. Substantive hits found in a search are then examined and disseminated to the appropriate entity for investigative follow-up and action. Existing relationships, information sharing, and coordination with other agency partners, including the Central Intelligence Agency, the Treasury Department's FinCEN, the Department of State, and DHS have been strengthened through these efforts.

d. How often is this data collected and analyzed?

Response:

The data are collected and analyzed on a continuing basis.

10. In its January 2005 unclassified report on the Sibel Edmonds allegations against a co-worker in the FBI language program, the DOJ-IG found that, "Even now, the FBI has not carefully investigated the allegations about the co-worker to determine if the co-worker compromised any FBI information."

a. The DOJ-IG report notes that "[i]n light of the need for FBI vigilance about security issues, as demonstrated by the Hanssen case, we believe the FBI should have investigated these serious allegations more thoroughly." Do you agree with this assessment? Why or why not?

b. Since the DOJ-IG report, has the FBI made any further attempts to determine whether the co-worker compromised any FBI information? If not, why not?

c. If so, (1) what steps has the FBI taken to determine whether FBI information was compromised, (2) what determination has the FBI made about whether information was compromised, and (3) what is the basis for any such determination?

Response to a - c:

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

---

*These responses are current as of 4/29/05.*

11. In addition to Sibel Edmonds, others have made allegations that in its haste to quickly hire as many translators as possible, the FBI has cut corners on background checks and hired individuals with questionable associations. What steps have you taken to inquire into allegations that certain FBI translators had questionable or inappropriate associations?

Response:

While the FBI is placing great emphasis on recruiting qualified linguists on a very fast track, all potential FBI employees, including linguists, are subject to a pre-employment vetting process to ensure trustworthiness and suitability for FBI employment. This process, which complies with Executive Order 12968 (Access to Classified Information), eliminates many candidates from further consideration. This is particularly true of translators, over 90% of whom are eliminated during the background investigation (BI) process, which includes:

- A thorough personnel security interview conducted by appropriately trained FBI SAs or security personnel;
- A polygraph examination focused on the candidate's purpose in seeking FBI employment and involvement with foreign CI matters, the completeness of the application, and any prior involvement with the sale or use of illegal drugs;
- A Single-Scope BI covering the past 10 years or longer, and,
- A review of the BI package and risk analysis by FBI CI and/or CT personnel.

Only if the candidate successfully completes the BI process is access to national security information approved. The FBI has not, and will not, cut corners during the vetting process.

To avoid, monitor, and manage the risks associated with hiring for our language program, the FBI instituted a post-adjudication risk-management program in late 2002. Pursuant to this program, FBI linguists are subject to regular personnel security interviews, polygraph examinations, and database access audits. In the event this process discloses questionable or inappropriate associations, whether they are based on self-reporting or brought to our attention by a third party, a security assessment is immediately conducted by the appropriate Field Office in coordination with the Security Division. If an FBI linguist's trustworthiness is questionable, the linguist's access to FBI space and information is suspended pending resolution.

---

*These responses are current as of 4:29:05*

If the Committee is aware of allegations that the FBI has failed to comply with security measures in hiring linguists, we would appreciate any specifics available to the Committee so we can immediately initiate investigation.

12. According to last summer's DOJ-IG report, the FBI has been aware of problems regarding audio sessions that need to be translated being automatically deleted without the ability to identify or quantify the deleted audio. According to that report, "necessary system controls have not been established ... such as protecting sessions of the highest priority[.] ... The results of our tests showed that three of eight offices tested had Al Qaeda sessions that potentially were deleted by the system before linguists had reviewed them."

a. Since that DOJ-IG report was issued last July, what steps have you taken to ensure that un-reviewed audio material for critical cases is not automatically deleted?

Response:

Among the steps the FBI has taken to ensure that unreviewed audio material for critical FISA cases is not automatically deleted are the following.

- We have upgraded our digital collection systems to significantly augment storage capacity at each site. Our current systems provide a minimum of 30 days of on-line storage for all sessions and are configured to alert system administrators if the system is approaching the point at which sessions must be deleted.
- As a matter of standard procedure, data storage at all sites is monitored by the FBI's Investigative Technology Division on a weekly basis. Facilities identified as having high storage utilization and a high percentage of unreviewed or in-process sessions are evaluated and scheduled for storage capacity upgrades if necessary. Pursuant to this procedure, the San Francisco field office has been upgraded and the Los Angeles system is under evaluation. Additionally, we have upgraded the New York Division, the Criminal Justice Information Services facility in West Virginia, FBIHQ, the Washington Field Office, and the Los Angeles Division as part of an ongoing digital collection system and software conversion.
- To prevent the inadvertent deletion of electronic surveillance (ELSUR) data, system controls are set to alert system administrators before any session is deleted. In addition, all audio sessions are automatically written to a magneto-optical disk immediately upon receipt. No data is ever deleted beyond recovery. In addition, the FBI continues to develop its ELSUR Data Management System, which is designed so

---

*These responses are current as of 4/29/05.*

that no information will ever be automatically deleted. The current strategy is for all ELSUR sessions to be immediately available on-line for a period of approximately one year, after which time the information will be archived but available for upload upon request.

**b. What steps have you taken to ascertain the extent to which audio went un-reviewed as a result of this failure of the FBI's computer systems?**

**Response:**

In order to ascertain the extent to which FISA audio was unreviewed, we have communicated with each individual field office and documented why and to what extent audio was deleted before review. We learned, for example, that of the 5,792 hours of al Qaeda-related data the Inspector General identified as unreviewed, the FBI was able to account for all but 115 hours (1.9 percent). As noted in response to subpart a, above, the FBI has since taken a number of technical and procedural steps to prevent the deletion of unreviewed audio. All audio is now immediately archived onto magneto-optical disks upon receipt and can therefore be re-imported into the on-line system as required. No audio is ever deleted beyond recovery.

**c. What steps have you taken to implement the report's recommendation that the FBI improve the level of information provided to the foreign language program about the relative priority of counterterrorism and counterterrorist cases?**

**Response:**

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

**d. What steps have you taken to implement the report's recommendation that you strengthen quality control procedures to ensure the accuracy of translations and that all pertinent material is being translated?**

**Response:**

The FBI's Directorate of Intelligence (DI) has aggressively pursued the strengthening of its quality control (QC) procedures by instituting the Translation QC Policy and Guidelines. The DI's QC program requires that, after an initial week of training, all work performed by new linguists during their first 40 hours of service is subject to review by a senior linguist. Work performed during the second 80 hours of service will also be heavily spot-checked and later checked with decreasing frequency as appropriate. In all, it is estimated that each new linguist

---

*These responses are current as of 4/29/05.*



(both language analysts and contract linguists) will require an investment of at least 120 hours by a senior linguist dedicated to QC.

In addition, the DI has:

- Developed a Manual of Standards for Translation.
- Revised and enhanced its QC policy by providing specific instructions and clearly defined milestones to all field offices for implementing QC improvements, including quarterly reporting mechanisms to monitor compliance.
- Coordinated with the Inspection Division to ensure thorough reviews of field offices' foreign language programs (including compliance with QC policy) as part of the regular inspection schedule.

Funds provided in the Consolidated Appropriations Act of 2005 will permit the employment of additional program management staff to guide and monitor field QC compliance and will allow annual review of the work of all FBI linguists. A successful QC program will require the work of approximately 30 senior linguists.

**13. The Commission on the Intelligence Capabilities of the U.S. Regarding WMD released its report to the President on March 31<sup>st</sup>. In that report, the Commission expressed a fear it may be impossible for the Director of National Intelligence (DNI) to impose the level of accountability envisioned by the Intelligence Reform and Terrorism Prevention Act (IRTPA) because the FBI's budget is not configured to allow effective oversight.**

The Commission's report explains that although one-third of the FBI's budget is funded through the National Intelligence Program (NIP), none of the NIP budget goes through the Bureau's Directorate of Intelligence. So, the DNI will have no budget authority over the Directorate of Intelligence. While the DNI will have some personnel authority over the head of the Directorate of Intelligence, he will have no personnel authority over the two FBI components that do receive the bulk of NIP money (the Counterterrorism and Counterintelligence divisions). The report describes this arrangement as "peculiar" and argues that it diminishes the DNI's ability to ensure that the FBI is fully integrated into the Intelligence Community.

---

*These responses are current as of 4/29/05.*

a. Does this "peculiar" arrangement serve any legitimate purpose other than to prevent the DNI from asserting control over the FBI's intelligence functions?

**Response:**

The arrangement described in the Weapons of Mass Destruction (WMD) Commission's Report was constructed under an earlier budget structure before the DNI was even created. It does not reflect the system the FBI is currently creating to bring its budget into line with the new authority of the DNI.

For many years, a portion of the FBI's budget has been designated as National Foreign Intelligence Program (NFIP) funding (the appropriations community refers to this designation as "scoring"). The FBI's appropriated funds are provided by the Appropriations Subcommittees responsible for DOJ's budget and, while these funds have never included designated NFIP funding, a portion of the FBI's budget has been "scored" to the NFIP by the Community Management Staff so that oversight entities can quantify the federal government resources devoted to "foreign intelligence" activities.

As noted in the WMD Commission report, the programs "scored" to the NFIP generally have been the FBI's CT and CI programs, in addition to small pieces of other programs, since these programs are related to "foreign intelligence." The FBI's Office of Intelligence (later designated the DI) was established in FY 2004, and at that time the FBI decided not to score all the resources of the DI to the NFIP. This decision was made, in part, because the FBI's intelligence program, which is managed by the DI, spans all investigative functions, including criminal investigations, and is therefore not focused solely on foreign intelligence.

The system just described was created well before the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) renamed the NFIP the National Intelligence Program (NIP) and created the position of Director of National Intelligence (DNI). Since this renaming, the FBI has undertaken a review to determine which resources should be scored to the NIP, and the DI will likely be one of the primary NIP programs. Other probable inclusions are certain intelligence resources associated with the CT and CI Divisions.

The report goes on to state that "[i]n our view, the FBI's budget process should be organized in a way that unambiguously ensures the responsiveness of the FBI's national security elements to the DNI." In order to achieve this, the report makes two recommendations: (1) that the NIP budget should include the budgets of the Directorate of Intelligence and the Counterintelligence and Counterterrorism Divisions, and (2) that the DNI

---

*These responses are current as of 4/29/05.*

have personnel authority over the FBI official who is responsible for all NIP budget matters within the FBI.

b. Do you agree with these recommendations? Why or why not?

Response:

Once NIP guidance is issued, we will bring our Intelligence Budget Decision Unit and the NIP in line. We are open to all recommendations and await the completion of the President's 90-day review.

c. If the DNI does not know how NIP funds are allocated and spent by the FBI, and if the DNI does not have some personnel authority over the FBI official responsible for managing NIP funds, then how is he going to exercise the authority that IRTPA intended to confer upon him?

Response:

The FBI will work with the DNI to ensure that NIP funds are properly allocated.

IRTPA empowers the DNI to lead the Intelligence Community, which is defined as including the FBI's "intelligence elements."

d. What are the "intelligence elements" of the FBI?

Response:

The FBI, DOJ, and the DNI will work together to appropriately define the FBI's "intelligence elements." Those "elements" will include at least the FBI's Directorate of Intelligence.

e. Are the FBI's Counterintelligence and Counterterrorism Divisions among its intelligence elements? Why or why not?

Response:

As indicated in response to subpart d, above, the FBI, DOJ, and the DNI will work together to appropriately define the FBI's "intelligence elements."

---

*These responses are current as of 4/29/05.*

Questions Posed By Senator Kyl

14. If section 201 of the USA PATRIOT Act is allowed to expire, is it true that criminal investigators could obtain a court-ordered wiretap to investigate mail fraud and obscenity offenses but not offenses involving weapons of mass destruction?

Response:

This answer is provided in response to Question 118 of the Questions for the Record (QFRs) posed to the Attorney General (AG) based upon this hearing.

15. It is my understanding that, before the passage of the USA PATRIOT Act, answering-machine messages on a home machine and voice-mail messages stored with a communications provider were treated differently. Answering-machine messages could be obtained with a search warrant, while law enforcement was required to seek a wiretap order to access voice-mail messages. Am I correct in the distinction, and if so, do you think that this distinction made sense?

Response:

This answer is provided in response to Question 119 of the AG's QFRs.

16. Section 212 of the USA PATRIOT Act allows Internet service providers to voluntarily disclose customer communications and records in life-threatening emergencies. It is my understanding, however, that the Homeland Security Act repealed the portion of section 212 governing the disclosure of the content of communications in emergency situations, and placed a similar authority in a separate statutory provision. Therefore, would there be any significant change in the law if section 212 were allowed to expire?

Response:

This answer is provided in response to Question 120 of the AG's QFRs.

---

*These responses are current as of 4/29/05.*

17. Has section 212, which allows computer-service providers to disclose communications and customer records in life-threatening emergencies, proven to be useful? And if so, could you please provide some real-life examples of its use?

Response:

This answer is provided in response to Question 121 of the AG's QFRs.

18. Many people have expressed concern about section 215 of the USA PATRIOT Act, which allows investigators in national-security investigations to seek court orders to obtain business records and other items. In particular, they have expressed the fear that this provision could be used to obtain records from libraries. It is my understanding, however, that prosecutors currently may obtain business records and library records in ordinary criminal investigations through grand jury subpoenas. Furthermore, it is my understanding that while a federal judge must approve requests for business records under section 215 of the Patriot Act; grand jury subpoenas for business records are issued without judicial supervision. Is this correct?

Response:

This answer is provided in response to Question 122 of the AG's QFRs.

19. Before the passage of the USA PATRIOT Act, courts had interpreted FISA to mean that the surveillance could be conducted under the statute only when foreign intelligence was the "primary purpose" of an investigation. Section 218 of the PATRIOT Act replaced the "primary purpose" requirement with a "significant purpose" standard. Has this provision had any appreciable effect in the war against terrorism? If so, please provide examples.

Response:

This answer is provided in response to Question 123 of the AG's QFRs.

20. Critics have charged that section 220 of the PATRIOT Act, which provides that a federal judge may issue a search warrant for electronic evidence stored anywhere in the country, encourages prosecutors to forum-shop for a friendly judge. Is this an accurate criticism of this provision?

Response:

This answer is provided in response to Question 124 of the AG's QFRs.

---

*These responses are current as of 4/29/05.*

21. I have heard many people express opposition to the USA PATRIOT Act because of their concern about the status of detainees being held at Guantanamo Bay and enemy combatants, such as Jose Padilla, being held in the United States. Could you please clarify for me whether those being held at Guantanamo Bay or enemy combatants, such as Jose Padilla, are being detained pursuant to any authority contained in the USA PATRIOT Act? If the Act were to be repealed tomorrow, would it have any effect on the status of these detainees and enemy combatants?

Response:

This answer is provided in response to Question 125 of the AG's QFRs.

22. There has been some discussion that section 412 allows the Attorney General in his sole discretion to indefinitely detain immigrants. I have two questions about this provision. First, how frequently has the Attorney General used this provision? Second, is the Attorney General's decision to use this provision subject to any review?

Response:

This answer is provided in response to Question 126 of the AG's QFRs.

23. As you know, a National Security Letter ("NSL") is basically an FBI request for information in national security investigations. Several newspapers and critics of the USA PATRIOT Act suggested last fall that a federal court in New York had held section 505 of the Act, which amended existing NSL authorities, unconstitutional on First and Fourth Amendment grounds. However, isn't it the case that it was not section 505, but rather 18 U.S.C. § 2709, the pre-existing NSL authority established by the Electronic Communications Privacy Act of 1986, which the court invalidated? Moreover, isn't it true that the Department urged an interpretation of section 2709 which would have expanded NSL recipients' rights in order to save the statute's constitutionality, and has appealed the judge's decision?

Response:

This answer is provided in response to Question 127 of the AG's QFRs.

---

*These responses are current as of 4/29/05.*

Questions Posed By Senator Leahy

24. At the April 5 hearing, I asked about an e-mail released to the ACLU in response to its Freedom of Information Act (FOIA) litigation. The e-mail is dated May 10, 2004, addressed to T.J. Harrington at the FBI, and contains the subject line, "Instructions to GTMO interrogators" (copy enclosed). Over the past six months, the Department has released the same e-mail in three different redacted versions. When asked about the e-mails at the hearing, you stated that you would "have to go back and look at how the various iterations were developed" before answering any questions. As you know, there is a presumption of disclosure under the FOIA, but agencies may withhold information pursuant to exemptions and exclusions in the statute, such as information properly classified, or protected by the Privacy Act. The three versions of the e-mail described above were significantly different from one another in what was redacted and what was released. Much of the information that was eventually released does not fit squarely within a FOIA exemption, suggesting that it should have been released pursuant to the ACLU's original request.

a. Please explain the process followed by the Department of Justice and the Bureau in reviewing documents for release under FOIA.

Response:

Requests for records under the Freedom of Information Act (FOIA) are initially processed by the Department components that possess the records. If the component does not produce all of the responsive records or redacts information from those records pursuant to FOIA's statutory exemptions, then the requestor is advised of his or her administrative appeal rights. Administrative appeals are adjudicated by the Department's Office of Information and Privacy (OIP) and sometimes result in the release of additional text. A requestor may file suit in U.S. District Court if he or she is dissatisfied with the results of this process. Alternatively, requestors may file suit if the Department component does not respond to the request within the statutory time frame, as the ACLU chose to do in connection with the document request that included the FBI e-mail, dated 5/10/04, that was described in your question.

As of 12/31/04, the FBI has over 2,000 FOIA requests in various stages of processing and has received, on average, 790 new FOIA requests per month this year. As of 1/19/05, the FBI is working with DOJ's OIP to resolve 630 administrative appeals and is presently involved in over 150 pending FOIA lawsuits in various federal district and appellate courts throughout the United States. Through an ongoing re-engineering effort, the FBI has successfully reduced its backlog of FOIA requests by approximately 89%, and a continuation of this downward trend is anticipated.

---

*These responses are current as of 4/29/05.*

In order to respond to FOIA and Privacy Act requests, the FBI currently has 247 employees, most of whom are Legal Administrative Specialists (LASs). These employees are assigned to various FOIA units, the shared function of which is to intake, review, process, and release information, as well as to respond to administrative appeals and to support FBI and DOJ entities representing the United States in FOIA litigation. "Processing" involves a page-by-page, line-by-line review of responsive documents to determine which FOIA and/or Privacy Act exemptions may apply, if any. Pursuant to this review, exempt material is redacted and applicable exemptions are noted. During its review, the FBI consults with other government agencies regarding their determinations as to the releasability of their information contained within FBI records, or refers non-FBI documents to those originating agencies for processing and direct response.

**b. When documents that originated with the FBI are sought by a FOIA requestor, is it the FBI or DOJ that ultimately determines what information can be released?**

**Response:**

This answer is provided in response to Question 165 of the AG's QFRs.

**c. How could the FOIA process, with its well-defined exemptions, lead the Department or the FBI to release three different versions of the same document?**

**Response:**

As indicated in response to subpart a, above, the originating component may initially release a document in one redacted form and a subsequent review by OIP, as part of an administrative appeal process, may result in a partial reversal of the component's determination and a second release with reduced redactions.

In response to the ACLU's FOIA request and subsequent lawsuit, on 9/15/04 the FBI was ordered by the district court judge to either produce or identify and describe all documents responsive to plaintiffs' requests by 10/15/04. This order resulted in numerous employees being diverted from their ordinary duties to review and process thousands of potentially responsive pages and to draft the necessary declarations for the court. Five additional LASs were shifted internally to support this litigation effort.

Between 9/15/04 and 10/15/04, the FBI reviewed and processed 1,388 pages and provided the court with public and in-camera logs for the remaining documents (approximately 2,600

---

*These responses are current as of 4/29/05.*



pages) along with a supporting Declaration. Among these, the FBI processed and released the 5/10/04 document (Bates 1373) in this initial production. In November, without the time constraints imposed by the 9/15/04 court order, the FBI processed a non-identical duplicate of the 5/10/04 document (a non-identical duplicate is, in this instance, a later e-mail that contains an embedded version of the 5/10/04 email). The processing of the subsequent version of the 5/10/04 document (Bates 2709) was premised on a different judgment regarding the release of information and resulted in reduced redactions.

In March 2005, OIP was asked to review the non-identical duplicate (Bates 2709) as if it were the subject of an administrative appeal and, in that process, the FBI agreed to release text that had previously been withheld to protect privacy interests and deliberative process. This revised version was provided to Senators Levin and Lieberman, as well as to the ACLU, on 3/18/05. As the cover letter to the Senators noted, a small amount of text remained redacted because it implicated Department of Defense (DoD) interests and, in accordance with established third-agency practice, the FBI was obligated to consult with DoD before releasing that text. Following that consultation and DoD's review, a fourth version of the document, which restored the DoD text, was released to the Senators and the ACLU on or about 4/6/05.

**d. In discussing Defense Department interrogations that used coercive techniques, the document states that, "results obtained from these interrogations were suspect at best." The words "suspect at best" were redacted in the first two versions of the document that were released, but not redacted in the final version that was released to Senator Levin. Please explain why "suspect at best" was initially redacted.**

**Response:**

This answer is provided in response to Question 167 of the AG's QFRs.

**25. On October 29, 2004, I requested unredacted copies of the FBI documents released to the ACLU in response to the FOIA litigation. While the FBI referenced that request in a letter to me dated December 23, 2004, signed by Eleni Kalisch, Assistant Director, Office of Congressional Affairs, I still have not received these documents. Why?**

**Response:**

As indicated in the 12/23/04 letter from the FBI's Office of Congressional Affairs (OCA) to Senator Leahy, the FBI's OCA informed DOJ of the request for documents regarding the treatment of detainees. DOJ advised that they would review the matter and inform us as to what information could be provided. We have not received DOJ's input on this matter to date.

---

*These responses are current as of 4/29/05.*

26. Some of the FBI documents released in response to the FOIA litigation are almost completely redacted. I would like to ask about two specific documents. (Copies enclosed.) The first is a seven page document dated February 13, 2002, and titled "Assessment and Recommendations regarding Interviewing, Debriefing, Interrogation of Al-Qaeda/Taliban Detainees at Guantanamo Bay, Cuba (GITMO)." Other than the heading on the first page, the document is entirely redacted. The second document is a seven page email string, dated May 31, 2003, through June 4, 2003, that appears to be an exchange between an FBI employee and an Army sergeant. In seven pages, the only thing that is not redacted is the subject line for each email, which reads, "hello, fbi-guy" and the closing on some of the emails, such as "Later!" and "have a good day!"

a. Please provide unredacted copies of these documents to cleared Committee staff.

Response:

The Freedom of Information Act (5 U.S.C. § 552) requires the disclosure of agency information, but exempts certain information from this requirement. These exemptions are typically referred to by the subsection of 5 U.S.C. § 552 that provides for them. For example, the exemption of classified information from release is provided for by 5 U.S.C. § 552(b)(1), and is therefore called a "b1" exemption.

As indicated on the documents enclosed with this question, much of the content is not only classified (a b1 exemption), but is also redacted on one or more other bases, including redactions based on § 552(b)(7)(E) (information that would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions, if such disclosure could reasonably be expected to risk circumvention of the law) and (b)(7)(D) (information which, if disclosed, could reasonably be expected to disclose the identity of a confidential source).

The redacted portions of the email string running from 5/31/03 through 6/4/03 contain no information that is subject ONLY to exemption b1, so disclosure even to cleared personnel would contain redactions taken on other bases. We are, therefore, unable to provide, even to cleared staff, a version of this document that differs from that already in the Committee's possession.

This is also true for most of the 2/13/02 document; that is, all those portions redacted for b1 purposes are additionally redacted for other purposes and therefore cannot be provided, even to cleared staff. The redactions applied to the introductory paragraphs of that document have,

---

*These responses are current as of 4/29/05.*

however, been removed, and that document, with these more limited redactions, is provided as Enclosure 1.

b. In response to a request by Senator Levin, the e-mail cited in question 1 was submitted to the Justice Department Office of Information and Privacy for review as if it were the subject of a FOIA administrative appeal. Please submit the two documents discussed above to a similar review and make the results public.

Response:

DOJ's OIP has reviewed the two referenced documents. OIP has advised that all of the redacted content in the 2/13/02 "Assessment" provided at Enclosure 1 is exempt from disclosure under exemptions other than b1. OIP's review of the email string running from 5/31/03 through 6/4/03 resulted in the determination that all of the redacted content is exempt from disclosure under exemptions other than b1 except for one line consisting of 11 words from an email dated 6/2/03 at 4:12 p.m. (that particular line is not exempt from disclosure under FOIA). That document, including these 11 words, is provided at Enclosure 2.

Rendition

27. At the hearing, I asked if the FBI has transferred detainees to other countries and, if so, what countries. You replied, "I don't believe so," but said you would confirm that response, [c]an you now confirm that, other than as a part of legal extradition proceedings, the FBI has not participated in the transfer of a detainee to another country?

Response:

To the best of my knowledge, the FBI has not transferred any detainee out of the country other than as part of legal extradition proceedings.

---

*These responses are current as of 4/29/05.*

Detainee Abuse

28. At the hearing, Senator Cornyn asked the following question: "[T]he reason why the FBI did not believe it could use all of the DOD-approved interrogation techniques is because different rules apply in a criminal prosecution with regard to information that an interrogator obtains from a suspect. Is that right?" You replied, "That's one of the reasons, yes." What are some other reasons that the FBI did not believe it could use all of the DOD-approved interrogation techniques?

Response:

From the time they enter the FBI Academy, FBI SAs are taught that statements, including confessions, whether obtained in the United States or abroad, must be voluntary and must be obtained consistent with the Fifth and Sixth Amendments to the Constitution. While these basic principles have been taught for years because they are the foundation for ensuring that the results of an interview can be admitted into evidence in a criminal trial, in most respects they are just as important when the sole goal of the interview is to gain intelligence, rather than evidence for use at trial.

The FBI's policy decision not to participate in the use of DoD-approved interrogation techniques that were not consistent with FBI policy was based in part on the fact that such techniques might preclude the introduction of the fruits of the interrogation into evidence, and in part because FBI agents involved in the interrogation of detainees can also be expected to testify in cases unrelated to detainees in DoD custody. If FBI agents were to participate in DoD-approved, aggressive interrogation techniques, such participation might be used to impeach their testimony concerning the treatment of other individuals in the United States. Finally, the FBI declined to participate in the use of such techniques because our experience is that rapport-building interrogation techniques are more likely to generate valuable information than aggressive techniques.

Access to Library Records

29. On April 4, 2005, the PEN American Center issued a press release announcing that a librarian who fought the FBI's search of patron records would receive the 2005 PEN/Newman's Own First Amendment Award. The press release states as follows:

*"On June 8, 2004, an FBI agent visited the Deming branch of the Whatcom County Library System in rural Washington State ... (and) demanded the names of all library patrons who had borrowed the book Bin Laden: The Man Who Declared War On*

---

*These responses are current as of 4/29/05.*

*America. The FBI made the request after a reader contacted the agency to report that someone had left a handwritten note in the margin of the book that said, 'If the things I'm doing is considered a crime then let history be a witness that I am a criminal. Hostility toward America is a religious duty and we hope to be rewarded by God' - a nearly direct quote of a statement Osama Bin Laden made in a 1998 interview. ... The Deming branch refused to provide information to the visiting agent, and the library system informed the FBI that no information would be released without a subpoena or court order. The library Board then voted to fight any subsequent subpoena in court.*

*"On June 18, a grand jury's subpoena was served requesting the names and any other identifying information of patrons who had borrowed the Bin Laden biography since November 15, 2001. At a special meeting of the Board, the library resolved to go ahead with a motion to quash the subpoena on the grounds that the request infringed on the First Amendment rights of readers; that libraries have the right to disseminate information freely and confidentially, without the chilling effects of disclosure; and that Washington state's library confidentiality laws protected the records. ... On July 14, the library learned that the FBI had withdrawn the grand jury subpoena."*

a. Do you take issue with any of [the] facts set forth in the PEN American Center's press release and, if so, what is the FBI's version of the events described?

Response:

The issuance and withdrawal of grand jury subpoenas are matters protected by the grand jury secrecy rule, and proceedings relating to grand jury subpoenas are sealed. See Fed. R. Crim. P. 6(e)(2), (5), and (6). For that reason, we can neither confirm nor deny the accuracy of the PEN American Center's press release to the extent that it claims to describe the issuance and withdrawal of a grand jury subpoena relating to the book *Bin Laden: The Man Who Declared War On America*. We acknowledge, however, that a library patron contacted the FBI regarding the referenced marginalia. That FBI office, which is near the Canadian border where individuals associated with the Millennium bombing plot entered the United States, attempted to resolve this complaint. In order to do so, an FBI SA visited the library for the purpose of determining what records were maintained and how they might be accessed. The Agent was given the name of the public library system's attorney, which he provided to his supervisor. The FBI subsequently learned that although relevant records were not maintained by the Deming library, they were maintained electronically elsewhere, but those records were not readily retrievable.

---

*These responses are current as of 4/29/05.*

**b. Do you believe the FBI acted properly in its initial demand for names of library patrons?**

**Response:**

The FBI is responsible for protecting the American people from terrorist acts. In fulfilling that responsibility, we obtain information from many sources, including the public. When we receive information indicating a possible threat, we take reasonable measures to identify the nature and credibility of the threat. The patron who brought the book to the FBI's attention was pleased to identify himself to the FBI in the interest of protecting others from the threat he perceived, and this willingness is important to the FBI's ability to provide the level of protection the Congress and the public demand.

**c. Do you believe the FBI acted properly in seeking and serving a grand jury subpoena for patron records? If so, why did the FBI choose to withdraw the subpoena rather than litigate its validity?**

**Response:**

Please see the response to question 29a, above.

**d. What can you tell us about the grand jury investigation that gave rise to the issuance of this subpoena? What crime was it investigating? Is the investigation still open?**

**Response:**

Rule 6(e) of the Federal Rules of Criminal Procedure prohibits the government from discussing grand jury investigations. Therefore, we can neither confirm nor deny the existence of a grand jury subpoena.

**e. Please describe any other instances since September 11, 2001, in which the FBI has withdrawn a grand jury subpoena in a terrorism investigation after being challenged as to its scope or validity.**

**Response:**

Subpoenas may be withdrawn for a variety of reasons, including a determination that the information sought will not forward the investigation. Rule 6(e) of the Federal Rules of Criminal

---

*These responses are current as of 4/29/05.*

Procedure prohibits the government from discussing grand jury investigations. Therefore, we can neither confirm nor deny the existence of a grand jury subpoena.

Oklahoma City Bombing

**30. The press reported that FBI agents, acting on a tip, searched the former home of Terry Nichols, and found blasting caps and other explosive materials buried in a crawl space that may have been related to the Oklahoma City bombing.**

**a. Was the crawl space searched back in the spring of 1995?**

Response:

Yes, the crawl space was searched in the spring of 1995. However, the FBI recently received additional information relative to the specific location of new evidence. The new evidence, which was discovered on 04/01/2005, was found buried under approximately eighteen inches of dirt and rock.

**b. Is any of the newly discovered evidence linked to the 1995 bombing?**

Response:

This is not yet known because the investigation and laboratory analysis are still in progress.

**c. Was the tip anonymous? Was it shaken loose by the prosecution or investigation of an unrelated crime? Who could be in a position to provide this new information?**

Response:

An inmate in the Bureau of Prisons Administrative Maximum facility in Florence, Colorado, provided the information to a correctional staff member, who passed it to the FBI's Denver Division. This inmate also provided the information to a private investigative agency in Michigan. Members of the investigative agency forwarded the information to the FBI's Detroit Division, as well as to United States Congressmen Dana Rohrabacher and William Delahunt.

Follow-Up to May 20, 2004 Hearing Questions

**31. In the classified set of answers to questions submitted after your appearance before the Judiciary Committee on May 20, 2004, a document was attached as "Enclosure #5 to the**

---

*These responses are current as of 4/29/05.*

5/30/03 EC." Please review this document for declassification and release it to the public, in redacted form if necessary.

**Response:**

That particular attachment was not classified and is provided as Enclosure 3.

**Questions Posed By Senator Feingold**

32. Prior to September 11th, various federal agencies maintained their own criminal or terrorist watch lists, some of which were shared with other government agencies but many of which were not. After September 11th, the federal government has tried to consolidate those lists. In 2002 and 2003, the Administration moved this important responsibility from agency to agency and there were significant delays. Ultimately, the task ended up being assigned to the Terrorist Screening Center (TSC), which is housed at the FBI, and which has made progress but has not completed the project.

a. The Director of the Center, Donna Bucella, testified about a year ago that there were roughly 120,000 names on TSC's consolidated watch list.

1) Has that number changed?

**Response:**

As of 4/20/05, the Terrorist Screening Database (TSDB) contained records on approximately 175,000 individuals.

2) Roughly what portion of the people on the terrorist watch list are known, dangerous terrorists?

**Response:**

All of the entities in the TSDB represent known or suspected terrorists or individuals associated with known terrorists or terrorist organizations. Nominations for inclusion in the TSDB are provided by either the National Counterterrorism Center (formerly the Terrorist Threat Integration Center) or the FBI.

3) Roughly what portion are people who may have tangential ties to someone who is the subject of a counter-intelligence or international terrorism investigation?

---

*These responses are current as of 4/29/05.*



**Response:**

As indicated in response to subpart 2, above, all of the entities in the TSDB represent known or suspected terrorists or individuals associated with known terrorists or terrorist organizations.

**4) Roughly what portion are U.S. citizens or legal permanent residents?**

**Response:**

25,006 of the entities in the TSDB are U.S. Persons.

**b. I understand that Transportation Security Administration (TSA) is planning to compare the names on the terrorist watch list, or at least some significant portion of them, to passenger lists from domestic flights. Passengers who match the list would either undergo additional security screening or be denied boarding, depending on their level of risk. The GAO recently reviewed TSA's plans and expressed concerns about the accuracy of the watch lists at TSC. Under the intelligence reform bill that became law in December, TSA must provide passengers with a redress mechanism and appeal rights, as well as the ability to correct inaccurate information in the system. Do you agree these are important protections? Does the Terrorist Screening Center have any plans to implement a similar redress system for people who face other types of adverse consequences as a result of its lists?**

**Response:**

Allowing individuals the opportunity to challenge whether they have been misidentified during a screening process, and to prevent that misidentification from recurring, is critical to the public's trust in the U.S. Government and its CT programs. The TSC recently hired a Privacy Officer who is developing a redress process for individuals who are having terrorist watchlist-related difficulties during screening processes. The TSC coordinates redress issues closely with all partner agencies and helps them to resolve redress inquiries from the public related to the terrorist watchlist. Because of its limited role under Homeland Security Presidential Directive 6 and the accompanying MOU, the TSC does not receive and respond to redress inquiries from the public directly, but does so through its partner agencies (such as the Transportation Security Agency) that run the screening programs. This helps to ensure that only redress inquiries regarding terrorist watchlist-related screening problems – as opposed to other reasons for screening, like random selection – are referred to the TSC.

---

*These responses are current as of 4/29/05.*

One of the options the TSC is considering for its redress process is the development of a consolidated misidentified persons list, which will help individuals who are repeatedly misidentified during screening because their names or dates of birth are similar to those of known or suspected terrorists.

**33. Is it true that no criminal defendant or defense attorney has ever been given access to the underlying FISA application or order when the fruits of that surveillance have been introduced in a criminal proceeding?**

**Response:**

The use of FISA information in criminal cases is governed by section 106 of FISA, 50 U.S.C. § 1806. Pursuant to section 106(c), whenever the government intends to introduce evidence obtained pursuant to FISA, it must give the defendant and the court notice in advance of trial. If the defendant is an "aggrieved party" (i.e., either the target of the surveillance or an individual whose communications were intercepted), then he can make a motion to suppress on the ground that the evidence was not lawfully acquired or that the surveillance was not conducted in accordance with legal requirements. Pursuant to section 106(f) of FISA, if the AG files an affidavit that disclosure of the FISA application or order or an adversary hearing would harm the national security, then the trial court must review the application, order, and any other documents relevant to the surveillance *in camera* and *ex parte* to determine whether the surveillance of the defendant was lawfully authorized and conducted. Congress has provided that, in making that determination, the district court may disclose the FISA application or order to the defendant only if such disclosure is necessary to make an accurate determination of the legality of the surveillance. To date, no judge has determined that the defendant needs the underlying application in order for that determination to be made. (See, e.g., *United States v. Squillacote*, 221 F.3d 542, at 551-52 (4th Cir. 2000), and *United States v. Isa*, 923 F.2d 1300 (8th Cir. 1991).)

---

*These responses are current as of 4/29/05.*

**34. In your testimony, you called for broad administrative subpoena authority for terrorism investigations because National Security Letters (NSLs) and Section 215 orders are inadequate or take too long to implement.**

**a. Has the FBI had significant trouble with recipients of NSLs not promptly complying, or not complying at all? If so, what actions has the FBI taken in response?**

**Response:**

In the FBI's experience, recipients of National Security Letters (NSLs) sometimes respond quickly and completely, sometimes respond slowly and incompletely, and sometimes do not respond at all. We believe there are several reasons for this. First, an NSL is a letter; it does not look like and is not a subpoena or court order. That appearance of informality apparently leads some recipients to treat an NSL differently than they would an instrument that comes from a court or that has a clear enforcement mechanism, like a subpoena. Additionally, there is no statutorily created enforcement mechanism for NSLs. Historically, the absence of a statutory enforcement mechanism led the FBI to make efforts to obtain the cooperation of those who do not respond rather than bringing an enforcement action against a recalcitrant or tardy NSL recipient.

**b. I understand that in the usual case, it might take several weeks or even months to complete a FISA application, get the appropriate signatures, and have the court review it. But I also understand that there are several internal procedures, aside from the emergency provisions, for expediting an application in a case where it is critical that the FBI obtain a FISA order quickly. Why are those procedures inadequate? Shouldn't they address the problem that you have outlined?**

**Response:**

FISA business orders under section 215 of the USA PATRIOT Act cannot currently be obtained on an emergency basis. If such authority were granted, or if DOJ were to implement procedures under which section 215 orders could be expedited, the FBI would be able to obtain such orders more quickly than is currently possible. Neither solution, however, would be as desirable as obtaining administrative subpoena authority.

First, any process that requires case agents to submit requests for documents through FBIHQ and then through DOJ will necessarily be slower, more cumbersome, and more manpower intensive than the process for issuing administrative subpoenas. Second, in order to obtain a section 215 order, resources of DOJ's Office of Intelligence Policy and Review and the Foreign

---

*These responses are current as of 4/29/05.*

Intelligence Surveillance Court must be used. Those resources are limited and currently quite strained. It is our judgment that those limited resources are better used with respect to electronic surveillance, which implicates significant privacy interests, than with respect to orders to obtain documents, which will generally not implicate Constitutionally protected privacy interests. Third, orders obtained under section 215 are classified, whereas administrative subpoenas would not be. The fact that the 215 order is classified means that it is subject to special handling requirements by both the agent who serves it and the recipient. Frequently, recipients are not cleared to handle classified documents, necessitating the use of a "trust receipt," further slowing the process. In short, for a variety of reasons, however efficient the process to obtain an order under section 215, an administrative subpoena would be superior.

**35. There has been a lot of news coverage lately about security breaches at information brokers like Choicepoint and Lexis-Nexis. Based on some FOIA requests, we know that the FBI has had contracts with Choicepoint to subscribe to some of its products.**

**a. From what companies does the FBI currently subscribe?**

**Response:**

Currently, the FBI contracts for services from the following vendors: Axciom, ChoicePoint, Dun and Bradstreet, iMAPdata, LexisNexis, Seisint, and Westlaw. Following is the type of data accessed from each vendor.

**Axciom** provides address history, occupancy data, phone number, Social Security number, age, gender, date of birth, and the year the individual graduated from high school.

**ChoicePoint** provides the numerical rank of the match, name, alias names, current and previous addresses, telephone numbers, Social Security number, driver's license number, date of birth, links to possible relatives, real property, bankruptcies, tax liens and judgments, corporation information, death indicator (yes/no), evictions, and geographic codes for each address found.

**Dun and Bradstreet** provides business name, address, phone and fax numbers, limited employee information, trade and assumed business names, special events (such as indictments, fraud charges, fires, and floods), officers and directors and their backgrounds, bankruptcies, lawsuits, liens, judgments, financial information, corporate affiliations, and linkages across companies worldwide.

---

*These responses are current as of 4/29/05.*

iMAPdata provides an interactive web-based tool that displays data via map layers covering the United States, including information regarding critical infrastructure, demography, political party affiliations, Emergency Management Services, geography, transportation, and telecommunications.

LexisNexis provides data on persons, organization names, license and registration numbers, addresses, zip codes, phone numbers, and related information to provide access to other public records where such data are also mentioned. The data returns usually include full address, name, date of birth, phone number, and Social Security number.

Seisint (Accurint Product) provides current address and phone number, historical addresses and phone numbers, dates associated with each address, date of birth, date of death, aliases, relatives, associated information, bankruptcies, property assessments, property deeds, neighbor information, neighborhood census information, corporate filings, national Uniform Commercial Code filings, internet domains, merchant vessels, Federal Aviation Administration (FAA) aircraft, professional licenses, FAA pilot licenses, voter registration, federal firearms and explosives, bankruptcies, criminal records, civil court records, and motor vehicle driving records.

Westlaw provides daily and archived news dating back 15 years. Westlaw also provides statutes and legal case information and captures public records, including criminal records, voter registration records, and public utility reports.

**b. How often do investigators use these databases?**

**Response:**

FBI agents and IAs access these databases on a daily basis. The following table reflects the number of searches conducted by the FBI using several of the above databases in FY 2004.

Vendor	FY 2004 Searches
ChoicePoint	1,280,244
Dun and Bradstreet	77,472
LexisNexis	712,137
Westlaw	14,042

*These responses are current as of 4/29/05.*

c. Does the FBI have accuracy and security benchmarks that it uses to evaluate whether to enter a contract with an information broker? What safeguards are in place in case information provided by these companies turns out to be inaccurate?

**Response:**

Maximizing the quality and accuracy of the data obtained from information sources is critical to FBI investigations. Before contracting with a data provider, the FBI conducts assessments to determine whether the data will add value to existing analytical processes, and only does business with companies with acceptable standards for quality and security. The company's customer list is one measure of quality and security. In addition, because many public source databases contain addresses, business records, travel information, phone numbers, and state drivers' licenses, the FBI uses a variety of sources of partially overlapping data to cross-check data accuracy. Because these measures cannot guarantee the accuracy of a given item of information, investigators are instructed to treat public and proprietary data as unverified; investigative decisions are rarely based on a singular source of information, and intrusive investigative techniques, such as searches and seizures, must be based on "probable cause" rather than on isolated pieces of information.

To enhance security, FBI contracts include a provision prohibiting public source providers from monitoring or tracking the searches conducted by the FBI. Vendors are permitted to record only who made the query, when it occurred, the location from which it was made, the type of query (e.g., a motor vehicle search or a personal identity search), and whether the search revealed any responsive records.

d. Are FBI agents using these databases for subject-based searches to track down information on people who are already suspects, or are they using them to run more open-ended, data mining searches to look for people who might fit a certain pattern of criminal or terrorist activity?

**Response:**

The FBI does not use the public source providers to data mine or run "open-ended" searches for people who might fit a certain pattern. Public and proprietary databases are accessed only after a specific request is received through official government channels predicated by an intelligence or criminal investigation. These predicated requests allow the FBI to access public and proprietary databases that it has a license and/or legal authority to access.

---

*These responses are current as of 4/29/05.*

# **ENCLOSURE 1**

## **QUESTION 26a**

**REDACTED DOCUMENT DATED  
2/13/02**

~~SECRET~~

DATE: 11-14-2004  
CLASSIFIED BY 61579 DMH/PLB/JAC 04-CY-4151  
REASON: 1.4 (C)  
DECLASSIFY ON: 11-14-2029

Date: 13 February 2002  
From: Behavioral/Operational Consultation Team  
To: Criminal Investigations Task Force  
Subj: Assessment and Recommendations regarding Interviewing, Debriefing, Interrogation of Al-Qaeda/Taliban Detainees at Guantanamo Bay, Cuba (GITMO).

This report is based on the observations and opinions of the Behavioral Component of the Debriefing Training Team made while conducting the Debriefing Training session at GITMO on 6 February 2002. The authors have expertise in the DOD, Federal Law Enforcement and Intelligence Communities and a wide range of experience dealing with investigations, operations and conducting behavioral forensic assessments. It is hoped that the observations and recommendations provided, may prove useful for planning tactics and strategies to deal with detainees held at GITMO. This report does not contain the observations or the opinions of the Operational Component of the Debriefing Training Team, but is the product only of the Behavioral Component of the Team.

This report is in response to the CITC request to offer recommendations regarding the method and style in which interviews, debriefings and interrogations of the detainees currently housed in Guantanamo Bay should be conducted. The assessment was completed in conjunction with a mobile training evolution conducted on February 6 2002, for military personnel and federal law enforcement agents, tasked with conducting interviews, debriefings and interrogations of Al-Qaeda/Taliban detainees. As part of the assessment, the team visited Camp X Ray, conducted meetings with senior leadership responsible for security, intelligence and interrogation/debriefings.

Purpose

The purpose of this assessment is to provide useful suggestions and options for commanders and task force leaders. These recommendations will hopefully add additional perspective regarding elicitation methods for interviewing Al-Qaeda and Taliban detainees. We believe the recommendations can enhance and optimize the potential for successful elicitation of information regarding Al-Qaeda and Taliban recruitment, training, activity and plans for future operations. This report will provide a variety of recommendations that may prove useful in eliciting information that can interrupt forward motion of current and future attacks. These approaches may also aid in the elicitation of confessions of crimes committed against the US and the world.



(S)

b1  
b2 -3  
b5 -1  
b7E

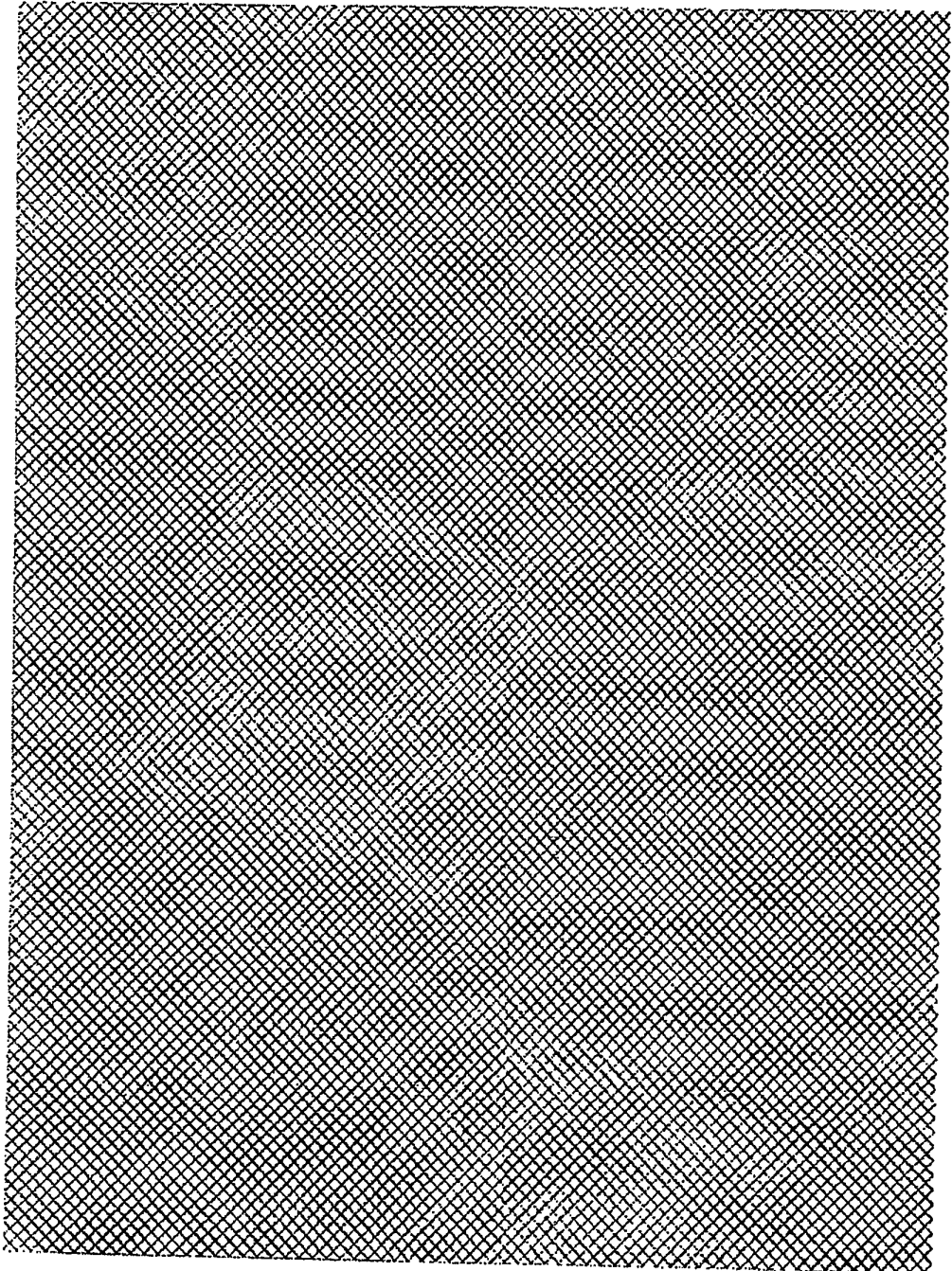
ALL INFORMATION CONTAINED  
HEREIN IS UNCLASSIFIED EXCEPT  
WHERE SHOWN OTHERWISE

~~SECRET~~

DETAINEES-3226



~~SECRET~~



(S)

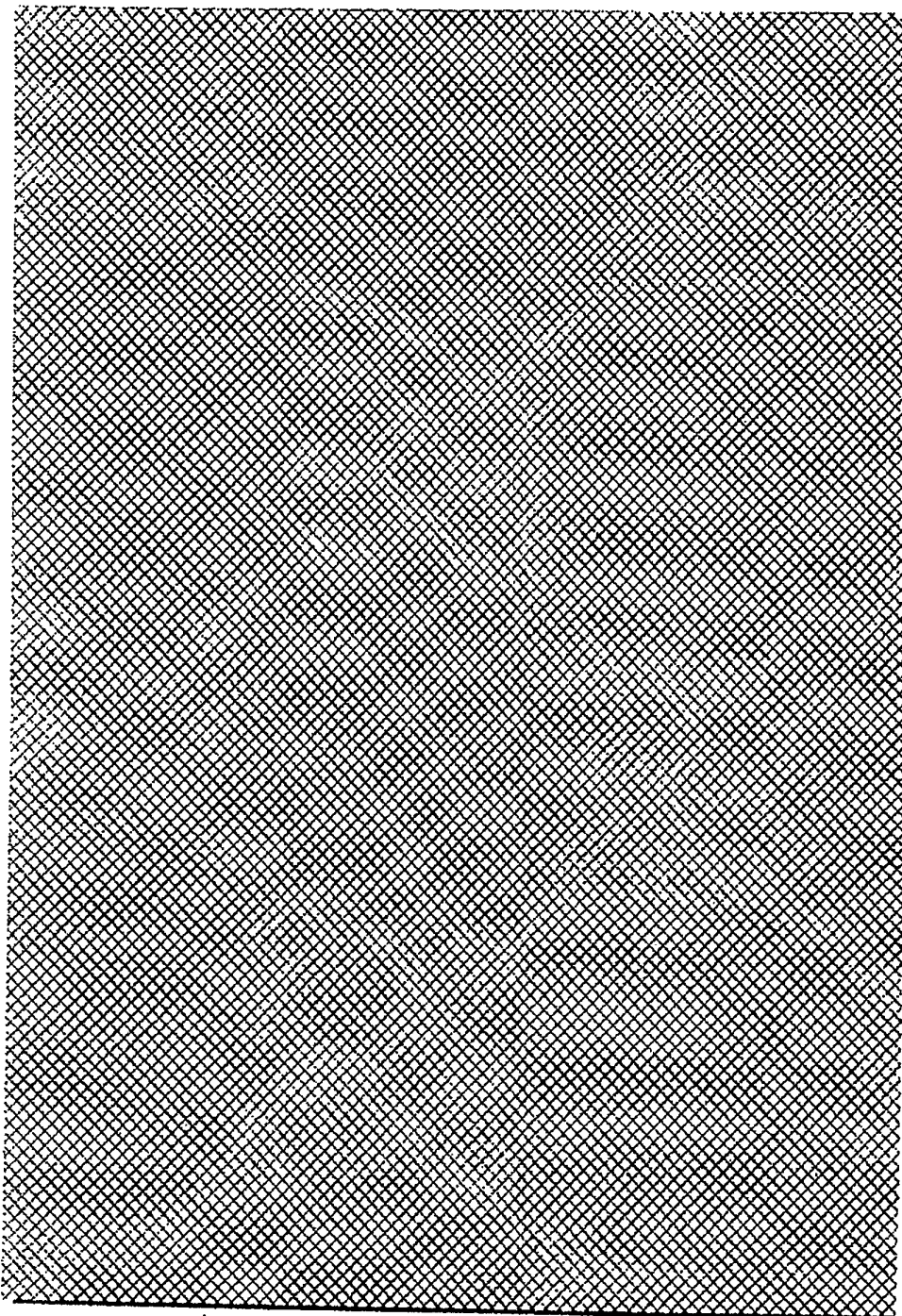
b1  
b2 -3  
b5 -1  
b7E -1

~~SECRET~~

DETAINEES-3227

~~SECRET~~

(S)

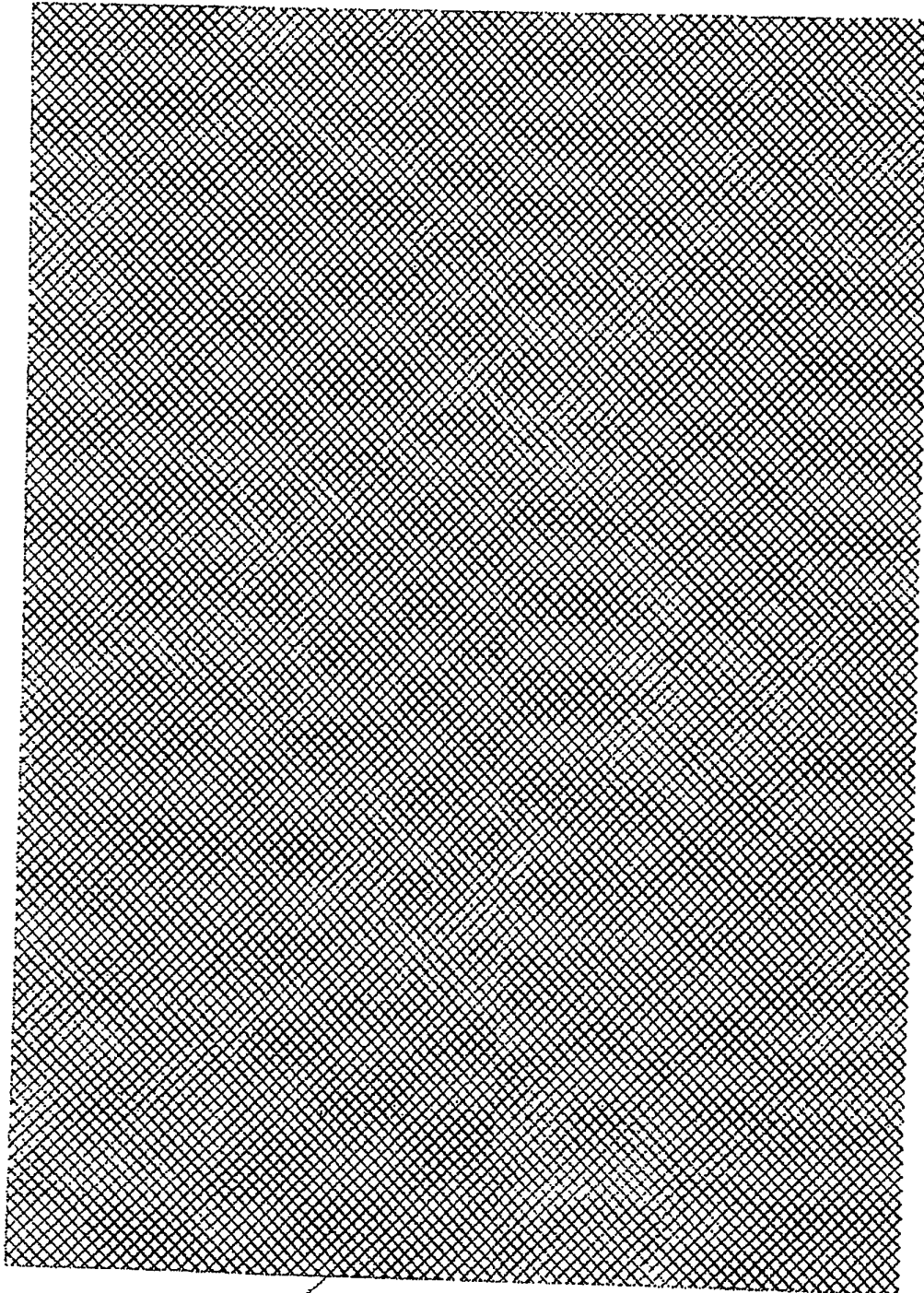


b1  
b2 -3  
b5 -1  
b7E -1

~~SECRET~~

DETAINÉES-3228 3

~~SECRET~~



(S)

b1  
b2 -3  
b5 -1  
b7E -1

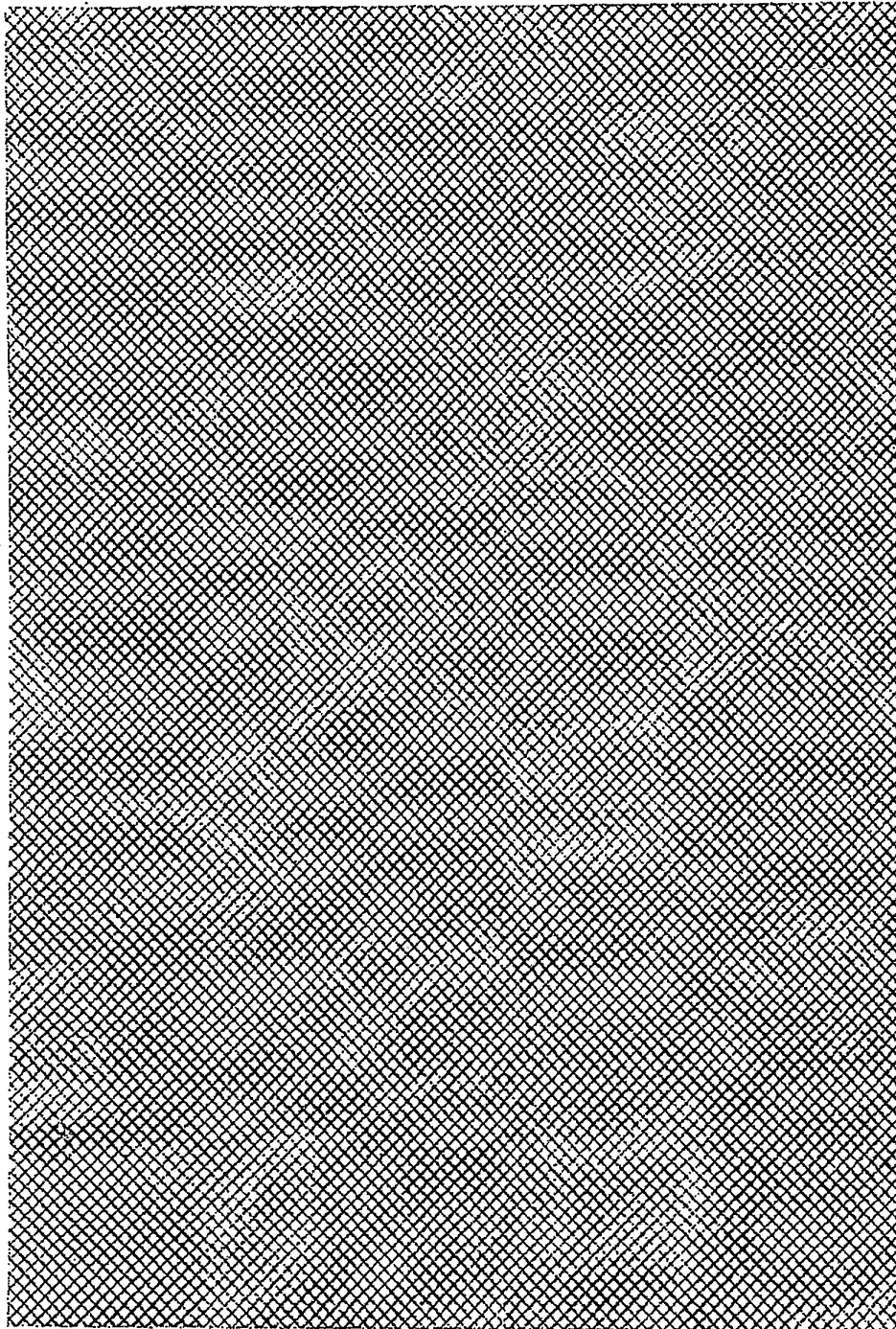
~~SECRET~~

DETAINees-3229

~~SECRET~~

(S)

b1  
E2 -3  
b5 -1  
b7E -1

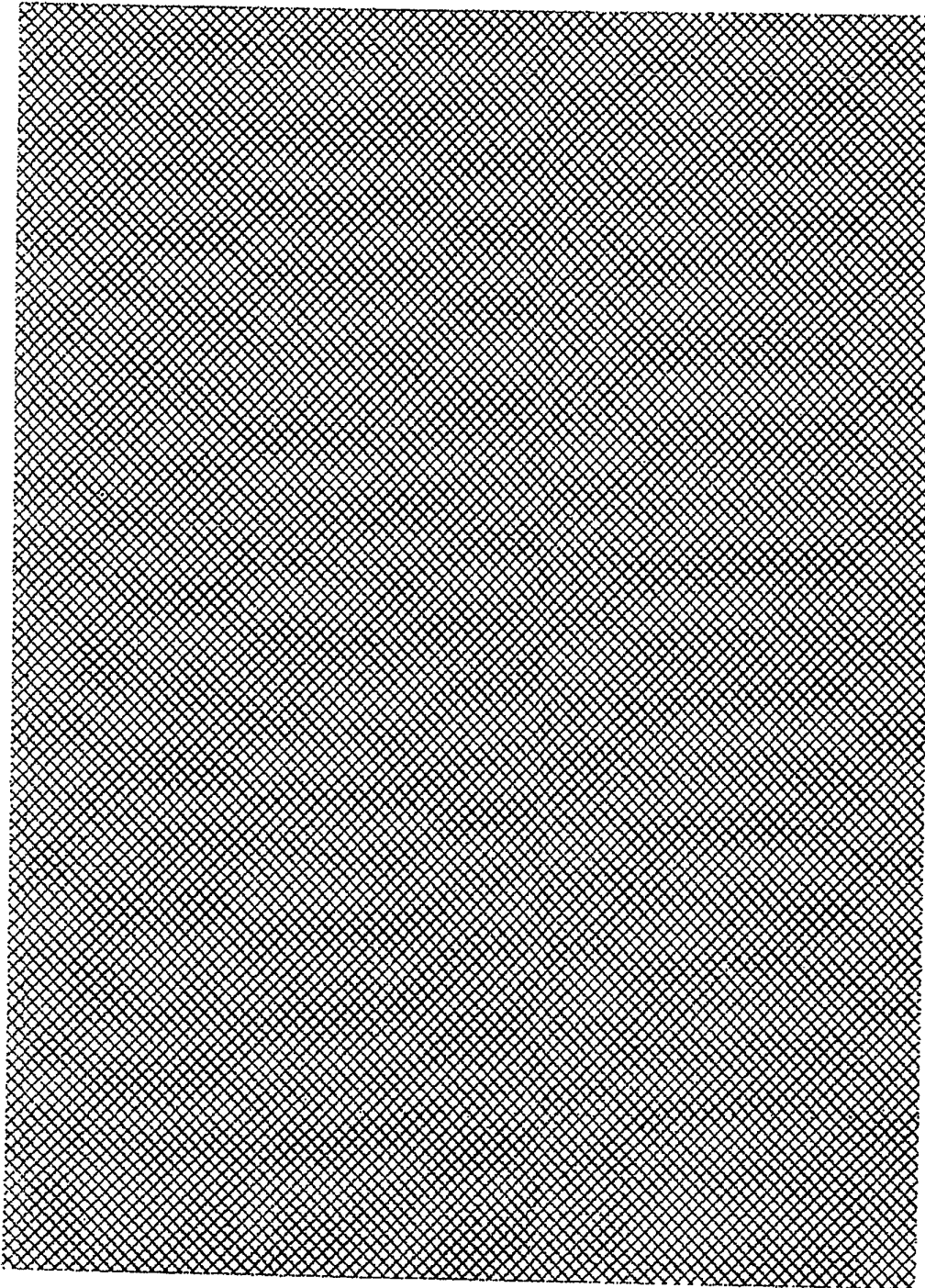


DETAINES-3230

~~SECRET~~

5

~~SECRET~~



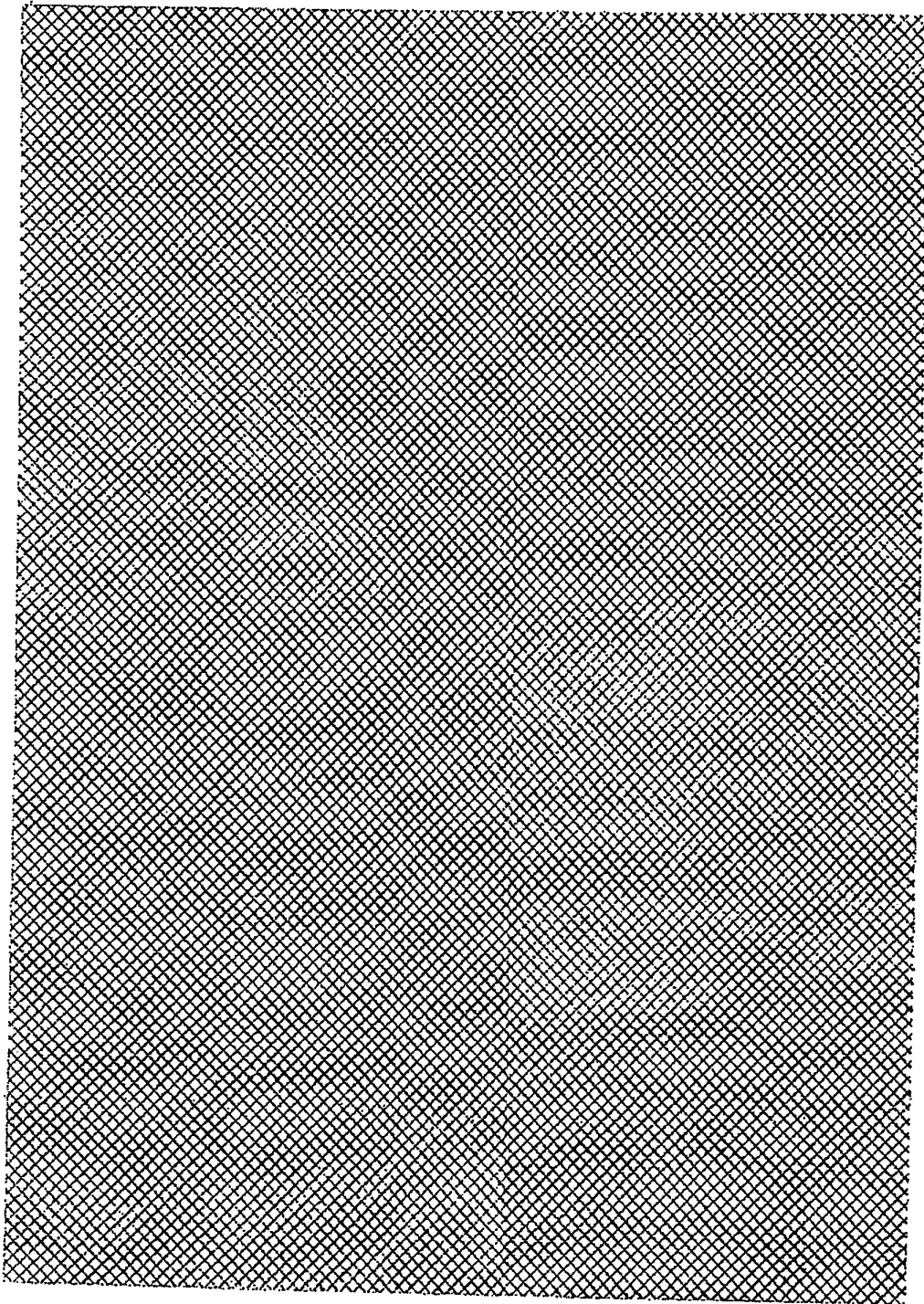
(S)

b1 }  
b2 -3  
b5 -1  
b7E -1

~~SECRET~~

DETAINEES-3231

~~SECRET~~



(S)

b1  
b2 -3  
b5 -1  
b7E -1

~~SECRET~~

DETAINEES-3232

7

ALL INFORMATION CONTAINED  
HEREIN IS UNCLASSIFIED  
DATE 04-13-2012 BY 65179 DMH/STP/MJS

## **ENCLOSURE 2**

### **QUESTION 26b**

**REDACTED E-MAIL STRING FROM  
5/31/03 THROUGH 6/4/03**

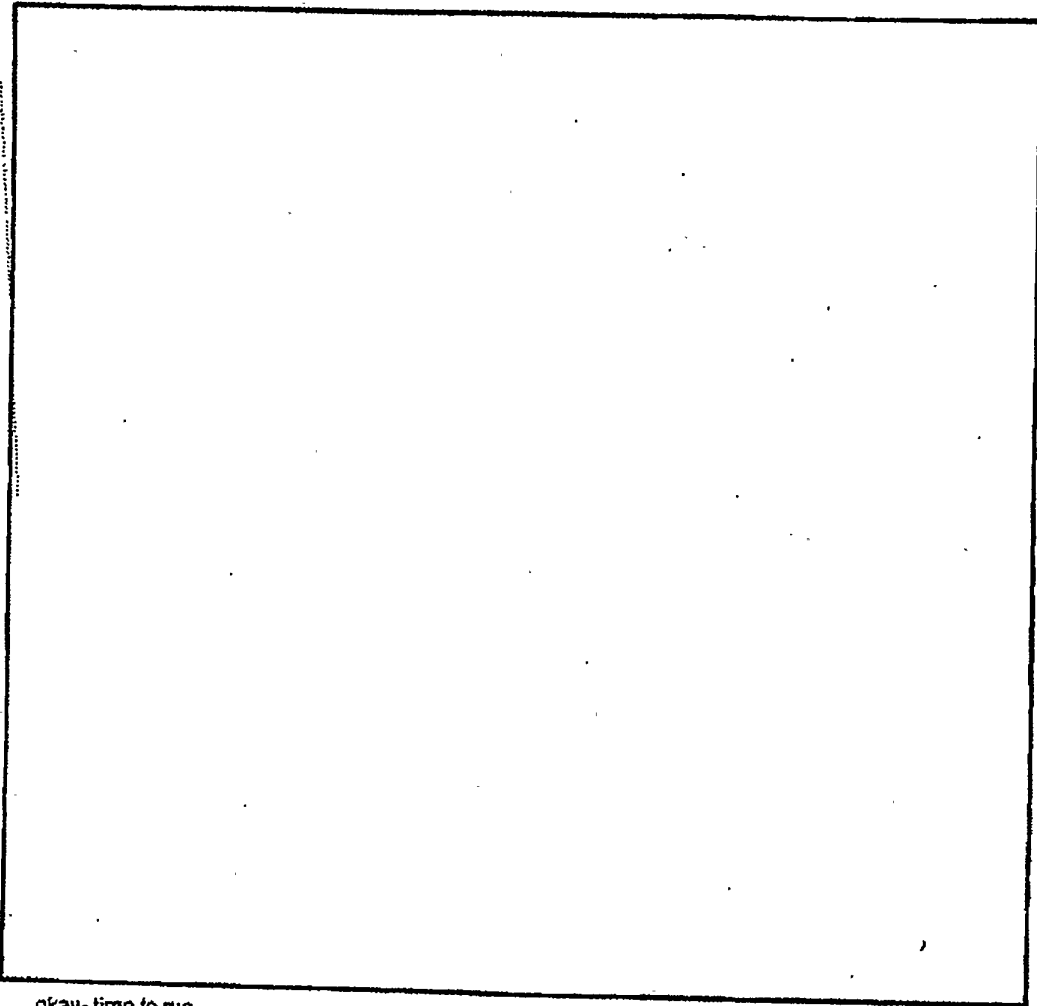
~~SECRET~~

b6 -1,2  
b7c -1,2

From: [redacted] (H)  
Sent: Wednesday, June 04, 2003 4:21 PM  
To: [redacted] FBI (H)  
Cc: [redacted]  
Subject: RE: hello, fbi-guy  
Classification: ~~SECRET~~  
Caveats: NONE

[redacted]

(S)



b1 |  
b2 -3  
b5 -1  
b6 -3,4  
b7c -3,4  
b7d -1  
b7e -1  
b7f -1

okay- time to run ...

[redacted]

DETAINees-3206

~~SECRET~~

EFF Section 215-227



~~SECRET~~

b6 -1  
b7C -1  
b6 -2  
b7C -2

-----Original Message-----  
From: [redacted] (FBI (H))  
Sent: Tuesday, June 03, 2003 12:43 PM  
To: [redacted] (H)  
Subject: RE: hello, fbi-guy

b1  
b5 -1  
b6 -2,3,4  
b7C -2,3,4  
b7D -1  
b7F -1

[redacted]

(S)

Later!

b6 -2  
b7C -2  
b6 -1  
b7C -1

-----Original Message-----  
From: [redacted] (H)  
Sent: Monday, June 02, 2003 4:12 PM  
To: [redacted] (H)  
Subject: RE: hello, fbi-guy

b1  
b5 -1  
b6 -3,4  
b7C -3,4  
b7D -1  
b7F -1

j-  
[redacted]

(S)

gotta run. today's a paperwork day, so you're welcome to call!

s :)  
dgs2

b7C -2

-----Original Message-----  
From: [redacted] (FBI (H))  
Sent: Monday, June 02, 2003  
To: [redacted] (H)  
Subject: RE: hello, fbi-guy

b6 -2  
b7C -2  
b6 -1  
b7C -1

b6 -2  
b7C -2

[redacted]

(S)

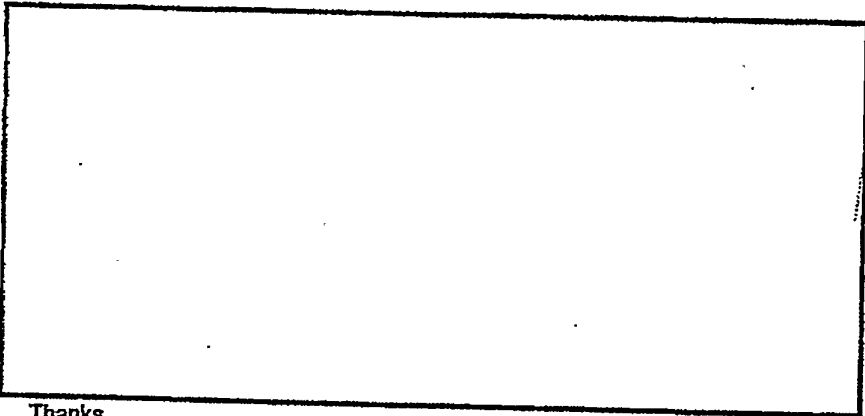
b1  
b2 -3  
b5 -1  
b6 -3,4  
b7C -3,4  
b7D -1  
b7E -1  
b7F -1

~~SECRET~~

DETAINEES-3207

EFF Section 215-228

~~SECRET~~

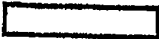


(S)

b1  
b2 -3  
b5 -1  
b6 -3,4  
b7C -3,4  
b7D -1  
b7E -1  
b7F -1

Thanks,

b6 -1  
b7C -1

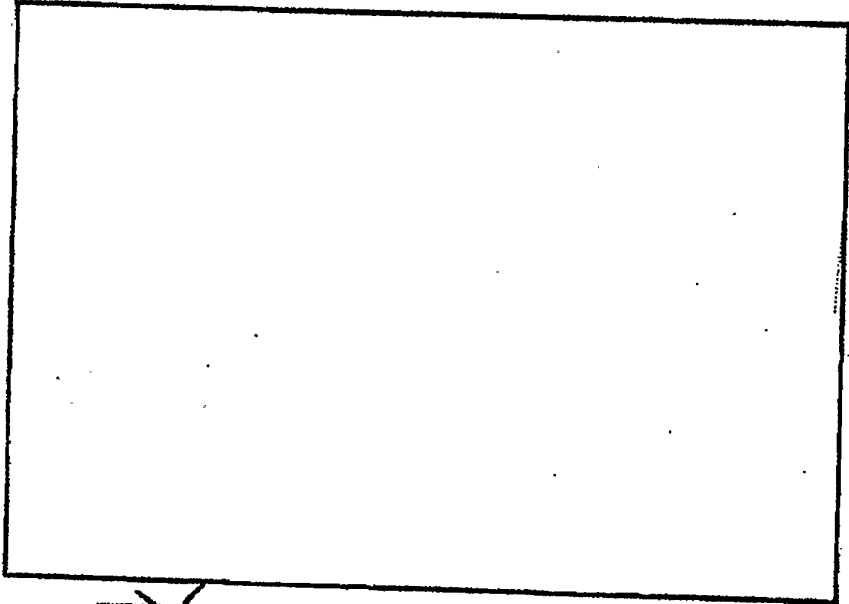


b6 -1,2  
b7C -1,2

From: [redacted] E SGT(H)  
Sent: Saturday, May 31, 2003 12:04 PM  
To: [redacted] EMT (H)  
Cc: [redacted]  
Subject: RE: hello, fbi-guy

Classification: ~~SECRET~~  
Caveats: NONE

b6 -1  
b7C -1



(S)

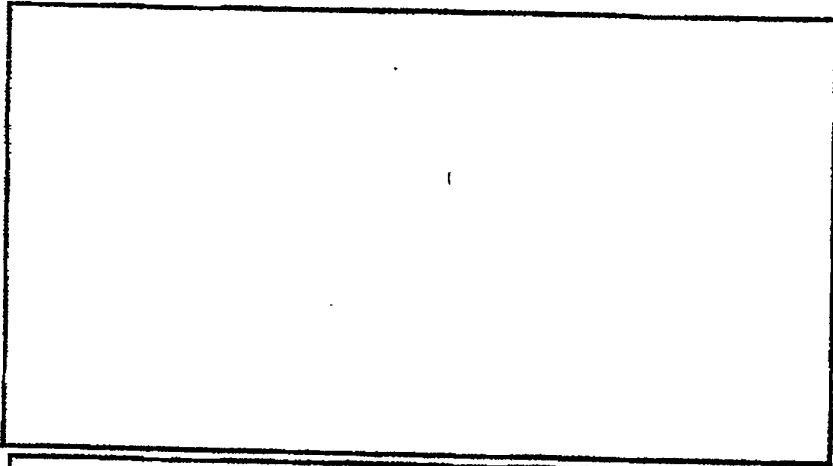
b1  
b2 -3  
b5 -1  
b6 -3,4  
b7C -3,4  
b7D -1  
b7E -1  
b7F -1

~~SECRET~~

DETAINEES-3208

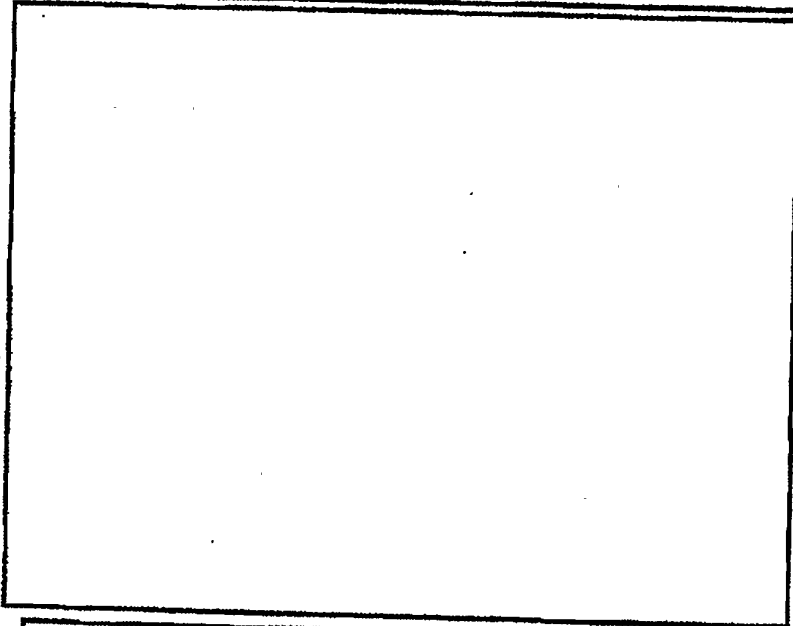
EFF Section 215-229

~~SECRET~~



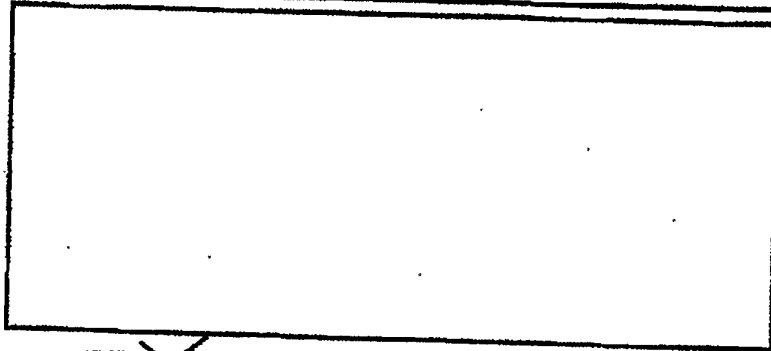
(S)

b1  
b2 -3  
b5 -1  
b6 -3,4  
b7C -3,4  
b7D -1  
b7E -1  
b7F -1



(S)

b1  
b2 -3  
b5 -1  
b6 -1,3,4  
b7C -1,3,4  
b7D -1  
b7E -1  
b7F -1



(S)

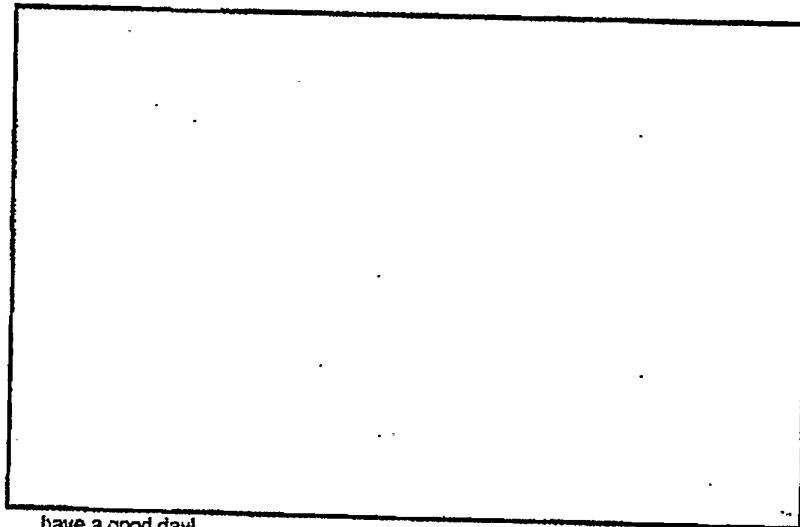
b1  
b2 -3  
b5 -1  
b6 -3,4  
b7C -3,4  
b7D -1  
b7E -1  
b7F -1

~~SECRET~~

DETAINEES-3209

EFF Section 215-230

~~SECRET~~



(S)

b1  
b2 -3  
b5 -1  
b6 -3,4  
b7C -3,4  
b7D -1  
b7E -1  
b7F -1

have a good day!

b6 -2

[redacted] das2

b7C -2

[redacted]

b6 -1

-----Original Message-----

b7C -1

From: [redacted] FBI (H)  
Sent: Saturday, May 31, 2003 10:44 AM  
To: [redacted] E SGT(H)  
Subject: RE: hello, fbi-guy

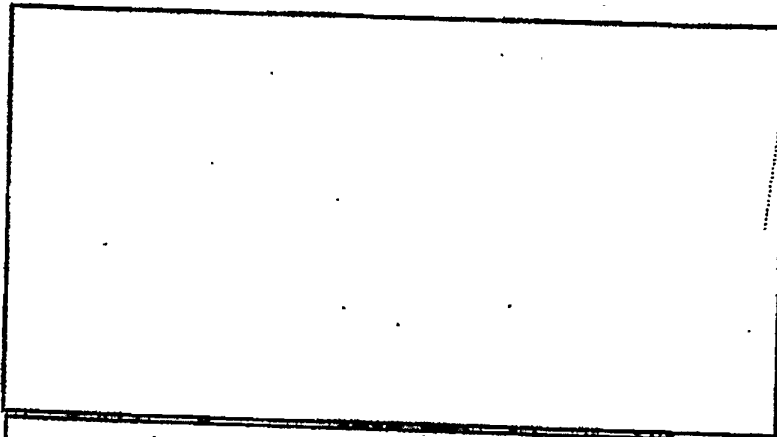
b6 -2

b7C -2

b6 -2

Hey [redacted]

b7C -2



(S)

b1  
b2 -3  
b5 -1  
b6 -3,4  
b7C -3,4  
b7D -1  
b7E -1  
b7F -1

b1

b5 -1

~~SECRET~~

DETAINEES-3210

(S)

EFF Section 215-231

~~SECRET~~

b1  
b6 -3,4  
b7C -3,4  
b7D -1  
b7F -1

[Redacted]

(S)

-----Original Message-----  
From: [Redacted] (H)  
Sent: Saturday, May 31, 2003 9:03 AM  
To: [Redacted] (H)  
Subject: helo, fbi-guy

Classification: ~~SECRET~~  
Caveats: NONE

b6 -1  
b7C -1

[Redacted]

b1  
b6 -3,4  
b7C -3,4  
b7D -1  
b7F -1

[Redacted]

(S)

b6 -2  
b7C -2

[Redacted]

Classification: ~~SECRET~~  
Caveats: NONE

Classification: ~~SECRET~~  
Caveats: NONE

Classification: ~~SECRET~~  
Caveats: NONE

DETAINEES-3211

~~SECRET~~

ALL INFORMATION CONTAINED  
HEREIN IS UNCLASSIFIED  
DATE 04-13-2012 BY 65179 DMH/STP/MJS

## **ENCLOSURE 3**

### **QUESTION 31**

**Enclosure #5 to the 5/30/03 EC**

## LEGAL ANALYSIS OF INTERROGATION TECHNIQUES:

### Interrogation Techniques

#### Category I -

1. Gagging with gauze.
2. Yelling at detainee.
3. Deception
  - a. Multiple Interrogators
  - b. Interrogator posing as an interrogator from a foreign nation with a reputation of harsh treatment of detainees.

#### Category II -

1. Use of stress positions (such as standing) for a maximum of 4 hrs.
2. Use of falsified documents or reports.
3. Isolation facility for 30 day increments.
4. Non-standard interrogation environment/booth.
5. Hooding detainee.
6. Use of 20-hour interrogation segments.
7. Removal of all comfort items (including religious items).
8. Switching detainee from hot rations to MRE's.
9. Removal of all clothing.
10. Forced grooming (shaving of facial hair etc...)
11. Use of individual phobias (such as fear of dogs) to induce stress.

#### Category III -

1. Use of scenarios designed to convince detainee that death or severe pain is imminent for him or his family.
2. Exposure to cold weather or water (with medical monitoring).
3. Use of wet towel and dripping water to induce the misperception of drowning.
4. Use of mild physical contact such as grabbing, light pushing and poking with finger.

#### Category IV -

1. Detainee will be sent off GTMO, either temporarily or permanently, to Jordan, Egypt, or another third country to allow those countries to employ interrogation techniques that will enable them to obtain the requisite information.

ALL INFORMATION CONTAINED  
HEREIN IS UNCLASSIFIED  
DATE 10/20/2003 BY 60324

## Legal Analysis

The following techniques are examples of coercive interrogation techniques which are not permitted by the U.S. Constitution:

### Category I -

3. b. Interrogator posing as an interrogator from a foreign nation with a reputation of harsh treatment of detainees.

### Category II-

1. Use of stress positions (such as standing) for a maximum of 4 hrs.
2. Use of falsified documents or reports.
5. Hooding detainee.
6. Use of 20-hour interrogation segments.
9. Removal of all clothing.
11. Use of individual phobias (such as fear of dogs) to induce stress.

### Category III-

1. Use of scenarios designed to convince detainee that death or severe pain is imminent for him or his family.
2. Exposure to cold weather or water (with medical monitoring).
3. Use of wet towel and dripping water to induce the misperception of drowning.

Information obtained through these methods will not be admissible in any Criminal Trial in the U.S. Although, information obtained through these methods might be admissible in Military Commission cases, the Judge and or Panel may determine that little or no weight should be given to information that is obtained under duress.

The following techniques are examples of coercive interrogation techniques which may violate 18 U.S.C. s. 2340, (Torture Statute):

### Category II-

5. Hooding detainee.
11. Use of individual phobias (such as fear of dogs) to induce stress.

### Category III-

1. Use of scenarios designed to convince detainee that death or severe pain is imminent for him or his family.
2. Exposure to cold weather or water (with medical monitoring).
4. Use of wet towel and dripping water to induce the misperception of drowning.



In 18 U.S.C. s. 2340, (Torture Statute), torture is defined as "an act committed by a person acting under color of law specifically intended to inflict severe physical or mental pain or suffering upon another person within his custody or control." The torture statute defines "severe mental pain or suffering" as "the prolonged mental harm caused by or resulting from the intentional infliction or threatened infliction of severe physical pain or suffering; or the administration or application, or threatened administration or application, of mind-altering substances or other procedures calculated to disrupt profoundly the senses of the personality; or the threat of imminent death; or the threat that another person will imminently be subject to death, severe physical pain or suffering, or the administration or application, of mind-altering substances or other procedures calculated to disrupt profoundly the senses of the personality."

Although the above interrogation techniques may not be per se violations of the United States Torture Statute, the determination of whether any particular use of these techniques is a violation of this statute will hinge on the intent of the user. The intent of the user will be a question of fact for the Judge or Jury to decide. Therefore, it is possible that those who employ these techniques may be indicted, prosecuted, and possibly convicted if the trier of fact determines that the user had the requisite intent. Under these circumstances it is recommended that these techniques not be utilized.

The following technique is an example of a coercive interrogation technique which appears to violate 18 U.S.C. s. 2340, (Torture Statute):

**Category IV-**

1. Detainee will be sent off GTMO, either temporarily or permanently, to Jordan, Egypt, or another third country to allow those countries to employ interrogation techniques that will enable them to obtain the requisite information.

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. s. 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. s. 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.



**U. S. Department of Justice**

Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

April 1, 2005

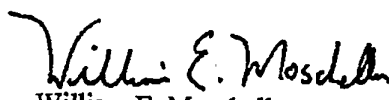
The Honorable Arlen Specter  
Chairman  
Committee on the Judiciary  
United States Senate  
Washington, D.C. 20510

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 May 20, 2004. The subject of the Committee's hearing was "FBI Oversight: Terrorism and Other Topics."

We hope that this information is helpful to you. 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,

  
William E. Moschella  
Assistant Attorney General

Enclosure

cc: The Honorable Patrick J. Leahy  
Ranking Minority Member

EFF Section 215-237

**Responses of the Federal Bureau of Investigation  
Based Upon the May 20, 2004 Hearing Before the  
Senate Committee on the Judiciary  
Regarding "FBI Oversight: Terrorism and Other Topics"**

**Questions Posed by Senator Hatch**

**1. In order to more fully understand this issue, please provide a chronology of events leading up to the misidentification of Mr. Mayfield. Include in this chronology an explanation of the events leading up to the initial identification of Brandon Mayfield as well as the circumstances that led to acknowledgement that Mayfield had been misidentified. Specifically, what efforts were made to secure the original or best fingerprint evidence? How many requests were made? Was there any attempt to utilize the actual prints held by the authorities in Spain? How many visits to Spain were made regarding the fingerprints in question? When was Mr. Mayfield officially identified? At what point did the FBI become aware of the doubts of the Spaniards as to Mr. Mayfield being the owner of the prints in question? When did the FBI discover the misidentification? What actions were taken immediately following the misidentification?**

**Response:**

The FBI provided two briefings to Committee staff concerning this issue; first on 5/25/04 and again on 6/9/04. Since that time, both the Department of Justice (DOJ) Office of the Inspector General (OIG) and the DOJ Office of Professional Responsibility (OPR) have initiated separate reviews of the Mayfield matter. The FBI will cooperate fully with these reviews and looks forward to the forthcoming reports from OIG and OPR. In addition, Brandon Mayfield has filed a lawsuit against the FBI, DOJ, and certain individuals arising out of this matter. In light of the pendency of the OIG and OPR reviews and the Mayfield lawsuit, it would be inappropriate to provide additional comment at this time.

**2. a. Please describe the standard protocols and methodologies that FBI fingerprint examiners use to determine whether a particular latent fingerprint is of value for identification purposes and whether such protocols and methodologies were utilized in the case of Brandon Mayfield.**

**b. What is standard procedure regarding the use of direct evidence versus secondary evidence?**

**c. In addition, what changes, in policy and procedure, do you anticipate making in order to assure the American public that such misidentification and wrongful incarceration does not happen again?**

**Response to a through c:**

As indicated above, the FBI will defer response during the pendency of the OIG and OPR reviews and the Mayfield lawsuit.

### Questions Posed by Senator Grassley

3. The Department of Justice recently released a report regarding the FBI's analysis of alternative financing mechanisms in money laundering and terrorist financing cases. The report, which is a 3 page document, states that TFOS has established a Program Management and Coordination Unit to analyze data on alternative financing mechanisms.

a. Thus far, what trends have been found regarding alternative financing mechanisms?

Response:

The response to this question is provided For Official Use Only (FOUO), and is included with the classified response.

b. How is the information being utilized to initiate other terrorist financing investigations?

Response:

The data from the field survey discussed above will be used to develop and enhance an analytic framework based upon identifiable patterns and trends. The analytic framework will enable Joint Terrorism Task Forces (JTTFs) to identify potential terrorism connections in investigations and facilitate the identification of previously unknown or "sleeper" terrorist suspects. In the interim, all pertinent information and data will be disseminated to the JTTFs and other agencies and entities as appropriate.

c. When will this information be made available to Congress and in what form?

Response:

The FBI has pursued more than 400 investigations concerning terrorism financing since 9/11/01. Unfortunately, because the vast majority of these investigations are ongoing, the FBI is unable to provide this information to the Committee at this time. (The very small number of cases that have been closed typically are offshoots of more significant ongoing investigations or involve very narrow facts, and do not reflect the nature, complexity, or value of the ongoing investigations.) The FBI would be pleased to provide this information to the Committee through classified briefings or other appropriate vehicles once the investigations have been closed.

**d. How will this information be shared with other agencies that have jurisdiction over other aspects of money laundering to ensure coordination and collaboration of our efforts?**

**Response:**

Information sharing is critical to the efforts of the United States Government (USG) against terrorism and criminal activities. The United States Intelligence Community (IC), including the FBI, produces and obtains tremendous amounts of classified intelligence information. While much of the information can be of significant value in terrorist finance investigations, this value may not be realized or maximized without the ability to filter, analyze, and disseminate the information to those who can make the best use of it.

The data analysis will be available to appropriate investigative, regulatory, and intelligence agencies through the JTTFs. TFOS also participates in joint endeavors with the Treasury Department, others in DOJ, and the Department of Homeland Security (DHS) with respect to potential terrorist-related financial transactions and money laundering.

In addition, the National Security Council (NSC) established the Policy Coordinating Committee (PCC) on Terrorist Financing at the end of 2001. The NSC chairs the PCC, which generally meets at least monthly to coordinate the USG's campaign against terrorist financing. The FBI presents all pertinent information at the PCC meetings, which focus on ensuring that all relevant components of the federal government are acting in a coordinated and effective manner to combat terrorist financing.

**4. Recently, the National Research Council, at the FBI's request, reviewed the Trilogy program and found the system inadequate for counter-terrorism analysis and significantly over budget. The Council recommended that the FBI scrap the whole thing and start over.**

**a. Are you following the Council's recommendations regarding testing and implementation?**

**Response:**

Yes. A 5/10/04 report by the National Research Council identified five areas of focus, and a 6/7/04 letter by the National Academies Chair of the Committee on the FBI's Trilogy modernization program advises that the FBI is addressing all five areas consistent with the Council's recommendations by: 1) converting from the Automated Case Support (ACS) system to a more powerful, user-friendly system, 2) creating an Enterprise Architecture (EA), 3) developing linked enterprise subarchitectures, 4) restructuring the Trilogy management plan, and 5) increasing internal FBI expertise in information technology (IT) and contract management.

**b. How will the additional funding you requested address the basic concerns that the system does not work?**

**Response:**

The FBI has completed two of the three components that comprise the Trilogy program. The Transportation Network Component and the Information Presentation Component were completed, providing the FBI with the Trilogy infrastructure, including the installation of the LAN, WAN, workstations, printers, and scanners in all Field Offices, resident agencies, offsites, and FBI Headquarters. Trilogy has also provided the FBI with Full Site Capability, which included the installation of new servers, upgrading of the FBI's office automation and learning management systems, and the provision of Microsoft Outlook email for all FBI users. The User Application Component is the only piece of Trilogy that has not yet been completed.

Although the FBI received funding in FY 2004 for Trilogy Operations and Maintenance and technical refreshment, it has not received any additional funding for Trilogy development since the Trilogy reprogramming in FY 2003. As indicated in response to Question 4a, above, the FBI's IT modernization program is ongoing. Included in the modernization program is the completion of a software application that will improve the FBI's efficiency, workflow, and records management functions.

**c. What solution do you recommend for ensuring that the FBI has an adequate computer system to support its intelligence and analytical needs?**

**Response:**

An Office of Intelligence (OI) Executive Working Group, chaired by OI and facilitated by the Office of the Chief Information Officer (OCIO), was created to identify the enterprise IT requirements needed to support OI operations. Participants in the working group include representatives from operational and support Divisions at FBI Headquarters (FBIHQ) as well as FBI Field Offices. The initial focus of the working group is the identification of immediate and near-term IT requirements; "requirements" are defined as the high-level, end-goal business and mission operational needs to support FBI intelligence activities.

Initial analysis of the immediate and near-term OI IT needs, which are those that can be addressed within 6 to 12 months, resulted in the identification of 53 "requirements." The 53 requirements have been validated and provided to the OCIO for systems/solution development.

Collection of the mid-term IT requirements, which are those that can be completed within 1-3 years, has been initiated.

**5. Drug trafficking is one of the main industrial and financial bases for the funding [of] terrorism and terrorist organizations. In Afghanistan, for example, the explosion of opium production poses a significant threat to our ability to halt terrorist financing in that region. What action is the FBI currently taking to address the direct connection between terrorism and drug trafficking in that country, as well as other countries such as Colombia that have a significant drug/terror nexus?**

**Response:**

Through the JTTFs, TFOS has partnered with investigative, regulatory, and intelligence agencies to determine the genesis of funding to terrorist groups. The FBI continues to gather intelligence and actively investigate all leads with respect to drug trafficking as a source of such terrorism funding.

Historically, Afghanistan has been a major source of heroin throughout the world. While conventional wisdom and some press accounts support the premise of the question, exhaustive investigation has not revealed direct evidence that drug trafficking proceeds support extremist groups. This does not mean there is no basis for inferring a likely link. For example, a joint FBI/DEA investigation in 2003 resulted in the arrests of 16 Afghan and Pakistani subjects for involvement in an extensive drug ring. The investigation revealed that heroin, grown and processed in Afghanistan and Pakistan, was being shipped to the United States. Profits from the sale of the heroin were laundered through Afghan and Pakistani-owned businesses and then sent back to suspected associates of terrorist organizations. A direct link between the drug trafficking profits and terrorist organizations was, however, not proven.

With respect to Colombia, the FBI is aware that the region continues to produce and distribute cocaine and is a significant supplier of heroin to the United States. In addition to supporting independent drug traffickers and cartels, the drug trade serves as a major source of funding for the Revolutionary Armed Forces of Colombia (FARC) and the United Self Defense Forces of Colombia (AUC). The AUC and FARC each control areas within Colombia that support coca and poppy cultivation. FBI investigations have led to the prosecution of both members and leaders of these organizations.

**6. It is my understanding that the FBI is implementing the National Security Support Capability (NSSC) program. The NSSC will be an important tool in the FBI's arsenal in the war on terrorism, because it brings a highly valuable new mix of methods and approach to this highest priority problem. There is considerable support for this unique effort on both sides of the Capitol and both sides of the aisle. I am pleased that you have included it in your FY06 budget and your program plans. But 2006 is too far off.**

**a. Could you tell me what efforts you are taking to implement the program now?**

**Response:**

The FBI's CTD has recently held a series of meetings with DHS and the Department of Energy (DOE) concerning the National Security Support Capability (NSSC). Based on these meetings, CTD developed a plan to incorporate the NSSC into its training mission and to work with private industry beginning in 2005. In August 2004, CTD and DOE worked out an arrangement to detail a DOE employee to the FBI for one year to assist in initiating this program. Later that same month, the DOE detailee unexpectedly withdrew from the detail assignment and is no longer supporting the NSSC initiative.

CTD and DHS have discussed alternative solutions that will deliver results that are the same as or similar to those expected from the NSSC. These discussions are ongoing but are too formative to permit comment on specific programs or dates of delivery.

**b. Using this program first on threats and vulnerabilities to the U.S. food supply is a great beginning and will bring an enthusiastic response from those of us who know how important it is to protect this critical resource. What other priorities will the program be extended to?**

**Response:**

Discussions regarding the NSSC's scope have indicated that it can be applied not only to the food and agriculture industries, but to a range of industries, including telecommunications and the oil and gas industry. Current discussions with DHS include focus on the possible uses of this or similar methodologies to produce valuable security-related information.



**Questions Posed by Senator Leahy**

**Prisoner Abuse**

7. I asked you at the hearing how many FBI agents were currently stationed in Iraq, Afghanistan, and Guantanamo Bay. You offered to submit that information for the classified record. Please do so now. In addition, please state how long these agents have been stationed in these countries, and describe their mission(s).

**Response:**

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

8. At the hearing on May 20, you stated that the Department of Defense had not, to date, referred any prisoner abuse cases involving military contractors to DOJ. The next day, DOJ announced that it had received such a referral the day before and that it had "opened an investigation into the matter."

a. At what time on May 20 did DOJ receive the referral from DOD?

**Response:**

The referral described was initially directed to an attorney in the Department's Criminal Division who had been previously identified to the Department of Defense as a point-of-contact for matters of this sort. The attorney learned of the referral in the middle of the day on May 20. At the time of the hearing, the FBI had not yet been informed of the referral.

b. When did you first learn about that referral?

**Response:**

The FBI learned about the referral close in time to when the information was publicly released, approximately May 21.

body is?

c. Is the FBI conducting this investigation and, if not, what investigating

**Response:**

It is the FBI's understanding that the investigations into prisoner abuse by civilians were referred to the U.S. Attorney for the Eastern District of Virginia. Investigative materials have been provided to the FBI and the FBI is currently evaluating them.

**9. At the hearing, you noted that the CIA had referred a prisoner abuse case to DOJ, but that the investigation was being conducted by the CIA Inspector General and not the FBI. Has the FBI become involved in that investigation since the hearing? If not, what investigating body or bodies are involved?**

**Response:**

One case involving prisoner abuse was referred to the FBI by the CIA Inspector General and the FBI has opened an investigation into that allegation.

**10. At the hearing, I asked you whether any of your agents have encountered any objectionable practices involving the treatment of prisoners in Iraq, Afghanistan or Guantanamo Bay. You limited your answer to Abu Ghraib, stating that none of your agents had witnessed abuses in that facility. Subsequently, in response to a similar question by Senator Feinstein, you stated, "We have, upon occasion, seen an area where we may disagree with the handling of a particular interview. And where we have ... seen that, we have brought it to the attention of the authorities who were responsible for that particular individual."**

**a. Upon how many occasions since September 11, 2001, have FBI agents "disagreed with" the handling of a prisoner interview in Iraq, Afghanistan, or Guantanamo Bay?**

**b. In how many of these cases was such disagreement "brought to the attention of" the responsible authorities?**

**c. What authorities were notified of the FBI's "disagreement" with particular interviews, and what, if anything, did they do in response? Did the FBI ever follow up with these authorities to determine if its concerns had been addressed?**

**d. What was the FBI's role in these interviews? Were agents actively involved and asking questions, or were they merely observing?**

**e. What sorts of practices did FBI agents "disagree with"? Please provide specific examples.**

**f. What guidance have field agents received from HQ about how to proceed in the event of a "disagreement" with another agency's handling of prisoner interviews?**

**g. Please provide copies of any written reports generated since September 11, 2001, that note an FBI agent's "disagreement" with, or objection to, the handling of a prisoner by the CIA, DOD, or any other American entity, in Iraq, Afghanistan, or Guantanamo Bay.**

**Response to a through g:**

From the time they enter the FBI Academy, FBI Agents are taught that statements, including confessions, whether obtained in the United States or abroad, must be voluntary and must be obtained consistent with the Fifth and Sixth Amendments to the Constitution. While these basic principles have been taught for years because they are the foundation for insuring that the results of an interview can be admitted into evidence in a criminal trial, in most respects they are just as important when the sole goal of the interview is to gain intelligence, rather than evidence for use at trial.

There are, however, other schools of thought regarding the best means of obtaining information from recalcitrant individuals. These varying schools of thought were at the heart of the disagreement over which interrogation methods should be used against individuals captured and suspected of involvement in terrorism against the United States.

In 2002, as a matter of policy, the Director of the FBI determined that, regardless of the legality of more aggressive interrogation techniques, FBI personnel would not participate in interrogation techniques that would not be appropriate for use within the United States. Rather, they would at all times conduct interrogation in accordance with FBI policies. A 5/19/04 electronic communication reiterating this policy, and directing FBI employees to report known or suspected abuse or mistreatment of detainees, follows this response.

Prior to the Committee's 5/20/04 hearing, the FBI surveyed its employees who were at Abu Ghraib prison during the time period of abuse as identified in General Taguba's report. That survey revealed no knowledge by FBI employees of the sort of abuses that were publicized around the time of the hearing. FBI employees were aware, however, of detainees being subjected to sleep deprivation and environmentally harsh conditions. The results of that survey were provided to the Department of Defense (DOD) for such follow-up as it deemed appropriate.

During 2002, there were disagreements in Guantanamo between the FBI and DOD concerning the interrogation plan that would be used for a particular detainee, and more general disagreements regarding the efficacy of rapport building techniques as opposed to more aggressive interrogation techniques. A classified electronic communication dated 5/30/03 documents these discussions and is provided under separate cover.

Subsequent to the Director's testimony before the Judiciary Committee, the FBI surveyed its personnel who had been in Guantanamo to determine whether any witnessed mistreatment of detainees. Prior to that survey, three incidents in which FBI personnel witnessed questionable treatment of detainees had been orally discussed with members of the DOD Office of General Counsel, in early 2003. Follow-up correspondence to Major General Donald J. Ryder, Department

of Army Criminal Investigation Command, dated 7/14/04, is provided separately.

The Guantanamo survey revealed other instances of treatment of detainees by non-FBI employees that would not have been in accord with FBI policy. All responses to the survey that included any knowledge of such treatment of detainees have been communicated to DOD for such follow-up as it deemed appropriate.

The FBI has not surveyed all Agents who have served in Afghanistan as to their knowledge of aggressive techniques. Some Agents have expressed concerns as to techniques being utilized in Afghanistan by non-FBI personnel. That information is being provided to DOD officials. In addition, the DOJ OIG has initiated an investigation into alleged abuse of detainees at Abu Ghraib, Guantanamo, Afghanistan, and any other venue controlled by the U.S. military. We are cooperating and providing relevant information in conjunction with the OIG inquiry as well.

(Rev. 01-31-2003)

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 Miranda 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.

To: All Field Offices From: General Counsel  
Re: (U) 66F-HQ-A1258990, 05/19/2004

**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.

To: All Field Offices From: General Counsel  
Re: (U) 66F-HQ-A1258990, 05/19/2004

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.

◆◆

**11. Do you think it is appropriate for the U.S. to use interrogation methods that are prohibited under U.S. law, as well as by the Geneva Conventions, to gain information in terrorism investigations? Has the FBI used any information produced by such methods in any terrorism case it is investigating or prosecuting?**

**Response:**

I do not believe it is appropriate for the United States to use interrogation methods that are unlawful under applicable law. It is FBI policy that all interrogations, regardless of the status of the person being interrogated, shall be conducted using methods that would be lawful if used within the United States (except that Miranda warnings are not required prior to extraterritorial questioning conducted for intelligence purposes). Among the techniques that FBI employees may not use, therefore, regardless of whether the interviewee is a U.S. citizen or an unlawful combatant taken into custody on the battlefield of Afghanistan, are physical abuse, the threat of such abuse to the person being interrogated or to any third party, or the imposition of severe physical or environmental conditions.

**Nicholas Berg**

**12. There is continuing confusion as to who held Nicholas Berg in custody and for how long. The Iraqi police deny ever holding Mr. Berg, and Mr. Berg's father has asserted that he was held illegally by the U.S. for two weeks. You testified, in response to a question from Senator Durbin, that Mr. Berg was detained by Iraqi police officers under circumstances that "I am not sure are totally clear"; Mr. Berg then "came to our [the FBI's] attention"; the FBI did some follow-up interviews with Mr. Berg and found that he had no association with terrorism, whereupon Mr. Berg was released and urged to leave Iraq.**

**a. Did the U.S. Government ever hold Mr. Berg in U.S. custody for any period of time?**

**Response:**

The FBI did not have Mr. Berg in custody. Mr. Berg was interviewed by FBI personnel at the One West Iraqi Police Station in Mosul, Iraq, on 3/25/04, 3/26/04, and 4/3/04.

**b. Did the U.S. Government ever ask or encourage the Iraqi police to arrest or detain Mr. Berg?**



**Response:**

Mr. Berg was detained by the Iraqi Police on 3/25/04 without the knowledge of the FBI. The FBI was notified of Mr. Berg's detention later that day.

Following his detention by Iraqi police, FBI personnel were asked to evaluate Mr. Berg for security purposes. After interviewing Mr. Berg and conducting preliminary background checks, FBI personnel expressed an investigative interest in Mr. Berg. It was understood that Mr. Berg would not be released until a more thorough investigation was completed and any security issues involving him were resolved.

**c. Did the U.S. Government ever make any efforts on behalf of this citizen, to secure his release from custody?**

**Response:**

Yes. The FBI interviewed Mr. Berg several times, conducted background checks, and followed up on leads in the U.S. relating to Mr. Berg. Once these steps were completed, the FBI advised the U.S. military and the Coalition Provisional Authority (CPA) that the FBI had no investigative interest in Mr. Berg.

**d. Has the U.S. Government ever inquired into the circumstances under which Mr. Berg was arrested and detained? If so, please describe those circumstances with specificity. If not, why not?**

**Response:**

The FBI was informed by the CPA that Mr. Berg had been detained by Iraqi Police while riding in a taxi in Mosul, Iraq. Because of the high level of violence in that area, the Iraqi Police were on the lookout for suspicious activity and for any individuals who did not appear to be from the area. In an interview, Mr. Berg disclosed that he had been arrested previously by Iraqi Police in January 2004 in Diwaniya, Iraq, because he looked suspicious.

**Brandon Mayfield**

**13. On Monday, May 24, a federal court dismissed the material witness proceeding against Oregon lawyer and former army officer Brandon Mayfield, and the FBI expressed regret for the erroneous fingerprint match that led to his arrest. The FBI has said that it made the initial match by running a latent fingerprint from the Madrid train bombing investigation through the Integrated Automated Fingerprint Identification System (IAFIS).**

- a. Did the FBI run the latent print against the entire IAFIS database, or against some sub-database of IAFIS that has been created for terrorism investigations? If the latter, please explain how Mr. Mayfield's print came to be included in the terrorism database.
- b. The FBI has said that IAFIS produced 20 possible "hits" with the latent print from the bombing, the fourth of which belonged to Mayfield. To whom did the other 19 prints belong? As to each of these 19 individuals, how did his or her fingerprints come to be included in IAFIS?
- c. What, if any, additional information was provided to the investigators and/or the lab technicians by IAFIS and/or the Criminal Justice Information Services (CJIS) Division at the time the 20 fingerprint cards (the "hits") were sent to the laboratory for a side by side comparison?
- d. The FBI has maintained that its lab technicians had no idea who Mayfield was when they matched his fingerprint to the latent print from the bombing investigation. It does seem improbable that the match happened to be with a Muslim lawyer who once represented the chief defendant in the "Portland Seven" terror case. What steps have been taken by the OIG or the FBI to review the actions of those responsible for this mismatch?
- e. I understand that the FBI was able, ultimately, to review the best evidence of the questioned latent print in order to eliminate Mr. Mayfield as the suspect, but did not review that evidence to determine whether the "points of identification" that had been made were, in fact, erroneous as well. Does the FBI intend to conduct such a review to determine what, if any, errors were made in that portion of the original analysis? If not, why not?
- f. What statements were made to the court by any government representative, at any time, orally or in writing, about the fingerprint "match"?
- g. Please provide a copy of the original fingerprint report prepared by the examiner.
- h. Following the erroneous fingerprint match, was Mayfield the subject or target of any secret surveillance under FISA or any other national security authority? Please explain your answer.
- i. Was the fingerprint that was originally identified as Mayfield's the very same fingerprint that was ultimately identified by the Spanish authorities as belonging to a suspect from Algeria? If it was a different fingerprint, were the two fingerprints (the one misidentified as Mayfield's; the others belonging to the Algerian man) on the same, or a different, piece of evidence? Please describe the pieces of evidence on which the fingerprints were identified. How many fingerprints have the Spanish authorities identified as belonging to the Algerian and on what pieces of evidence?

**Response to a through i:**

As indicated above, the FBI will defer response during the pendency of the OIG and OPR reviews and the Mayfield lawsuit.

**Fingerprint System**

14. Earlier this year, Inspector General Fine issued a report on the slow pace of the integration of IDENT and IAFIS, the fingerprint identification databases of the former INS and the FBI. The report examined the case of Victor Manuel Batres, a Mexican national with a criminal history who was twice simply returned to Mexico by Border Patrol agents whose database did not identify him as a wanted man. Batres eventually entered the country illegally, and then raped two nuns in Oregon, killing one. The Inspector General reported that the integration that would give Border Patrol agents access to the FBI database was two years behind schedule, and was not expected to be completed until 2008. This report is the third OIG report in the last four years to highlight various aspects of this problem.

a. Why has progress on this issue been so slow?

**Response:**

During 1990 and 1991, the FBI and the Immigration and Naturalization Service (INS) met to discuss possible coordination of their planned automated fingerprint identification systems. Memoranda summarizing some of these meetings indicate that the INS and FBI were attempting to determine if an integrated fingerprint system could satisfy INS's needs. The memoranda also include preliminary diagrams and narratives as to how the FBI's Integrated Automated Fingerprint Identification System (IAFIS) and the INS's proposed system (which evolved to become the Automated Biometric Identification System (IDENT) system) could be linked in an overall automated fingerprint identification system network. There was also discussion of how to ensure common high-quality fingerprint image and electronic transmission standards for fingerprints and identification data so that they could be transmitted among different fingerprint identification systems.

The INS and FBI recognized that integration of their separate automated fingerprint identification systems would benefit both agencies. An integrated system would reduce the likelihood that INS would release an alien who had a serious criminal record and prior deportations. It also would enable federal, state, and local law enforcement authorities to search fingerprints from a crime scene against an immigration database of those who have crossed borders illegally.

The two identification systems are, however, not yet interoperable. This is in part because each system was designed to meet different mission requirements: IAFIS was designed to match ten-print submissions against a ten-print database because this is the best means by which law enforcement can identify criminal subjects (since crime scenes may offer latent prints from any of a subject's ten fingers), and IDENT was developed with a two-print standard in order to meet the need to quickly and accurately verify an individual's identity.

DOJ and DHS have undertaken an effort to integrate the FBI's IAFIS with DHS's IDENT. This multi-year effort is designed to give DHS the ability to determine quickly whether an individual, such as a person encountered at a border crossing, has a record in the criminal master file of the FBI's IAFIS. Full integration would also enable other law enforcement agencies to obtain an individual's DHS apprehension history through the IAFIS infrastructure and communications network. DOJ and DHS continue to research possible solutions. The FBI will continue to provide support to DOJ by providing relevant information concerning operational impacts on the FBI.

**b. When can we expect that the databases will be integrated?**

**Response:**

An initial phase of integration has occurred with the deployment of integrated IDENT/IAFIS workstations at ports of entry across the United States. Completion of the integration process depends on the development of appropriate interoperability standards. DHS and DOJ are working together to resolve these issues as expeditiously as possible in the pursuit of full integration.

**Trilogy**

**15. The Trilogy project is now more than \$200 million over budget and still incomplete.**

**a. Is the FBI cooperating fully with the OIG's audit of the cost and contractual issues involved?**

**Response:**

The FBI cooperated fully with DOJ's OIG, providing that office with extensive documentation relative to the Trilogy audit.

**b. Can you assure me that the FBI will cooperate fully with a subsequent review that Senators Hatch, Grassley, Durbin and I asked the GAO to complete regarding fraud, waste and abuse?**

**Response:**

The FBI has cooperated, and will continue to cooperate, fully with GAO reviews requested by Congress.

**c. Has the FBI done any investigation of its own into whether there has been any fraud, waste or abuse involved in this government contract?**

**Response:**

A financial review of the Trilogy funding was conducted by the FBI Inspection Division's Audit Unit during January and February 2004. The objectives of the review were to determine: 1) the overall funding used in support of Trilogy; 2) what funds remain available to support the Trilogy roll out; 3) whether transactions were recorded accurately within the financial management system; and 4) whether the program had adequate financial management oversight.

The financial review identified some compliance deficiencies and internal control weaknesses, the most prominent of which was the inability to obtain a global financial profile. The FBI has taken action to resolve the deficiencies and internal control weakness identified through this review.

**16. Please provide me a detailed chronology of the key contractual events for all parts of Trilogy.**

**Response:**

The enclosed memorandum dated 1/26/05 contains an historical account of the FBI Trilogy effort.

The Trilogy contract with Dyncorp/CSC for the hardware and software components was completed in April 2004.

**17. You testified that "the reason we have spent far more funds" on Trilogy is that the contracts for the program were entered into in the summer of 2001, and the program had to be "changed and adapted" in the wake of the 9/11 attacks. Please specify what changes/adaptations were made to Trilogy as a result of the 9/11 attacks that account for the more than \$200 million difference between the original budget for the program and the currently estimated cost.**

**Response:**

The modifications to Trilogy required as a consequence of the 9/11/01 attacks are articulated in response to Question 16, above.

18. You testified that the FBI had already implemented or begun to implement many of the recommendations contained in the May 2004 report of the National Academies on the Trilogy program. Please identify[:]

a. The specific recommendations that you have implemented;

Response:

Enterprise Architecture

Recommendation: The FBI's top leadership, including the Director, must make the creation and communication of a complete enterprise architecture a top priority. Status: The FBI Director briefed Congress regarding his commitment on 3/23/04.

Recommendation: The FBI should seek independent and regular review of its EA, as it develops, by an external panel of experts with experience in both operations and technology/architecture. Status: The FBI regularly seeks independent review of its EA by experts outside the FBI, including the Director's Science and Technology Advisory Board. For example, based on an October 2004 meeting with that Board, the FBI is expanding: (1) the Performance Reference Model, including validated outcomes; and (2) the development of an Interim Architecture, which will be used to assess current projects and to direct funding so as to ensure that the Bureau moves strategically toward a successful target architecture.

Recommendation: Given that the CT mission requires extensive information sharing, the FBI should seek input on and comment from other intelligence agencies regarding its enterprise architecture effort. Status: The FBI coordinates with the National Reconnaissance Office, National Geospatial-Intelligence Agency, Army Architecture Integration Cell, and others, and has requested review by the Intelligence Community System for Information-Sharing Implementation Board.

Recommendation: The FBI should build on the early efforts under way in the intelligence area in defining a sub-architecture for the intelligence process, rather than beginning with the VCF architecture. Status: The OI published its "Immediate/Near-Term Requirements" report on 6/30/04 and is developing its architecture in collaboration with the FBI's EA Program.

System Design

Recommendation: The FBI should plan to rework the next version of the VCF to include a workflow engine as a high priority. Status: This plan has been

completed and both VCF and any successor software will include a robust workflow management capability.

**Recommendation:** The FBI should adopt a risk management approach to security so that it can understand the operational penalties it pays for risk avoidance.  
**Status:** An IT Continuity of Operations Plan was initiated in January 2004.

**Recommendation:** The FBI should encourage creative experimentation with exploitation of IT in the field, such as the PDA experiment mentioned in section 2.2.4 of the report. **Status:** Research and Development with respect to the Blackberry Wireless has been completed, and the RAND Corporation is assisting with analysis of this effort.

#### Program and Contract Management

**Recommendation:** Because testing is such a critical dimension of system development and deployment, the FBI must allow adequate time for testing before any IT application (including VCF) is deployed, even if the dates of initial operational capability are delayed. **Status:** This has been approved under the Lifecycle Management Directive (LCMD) and transition for existing projects has been initiated.

**Recommendation:** Evolution is an essential component of any large system's life cycle. Future development contracts for user applications should be premised on the use of small-scale prototypes that can be built rapidly and tested with user feedback before committing to large-scale development. **Status:** The FBI concurs and has revised the VCF development consistent with this recommendation.

**Recommendation:** For IT applications beyond VCF, the FBI should exploit proven methodologies of contracting and contract management, including the use of detailed functional specifications, specific milestones, frequent contract reviews, and earned-value metrics. **Status:** The FBI's LCMD, which governs how IT projects are managed from "cradle to grave," is consistent with industry and other government agency best practices. All IT projects and programs will be required to pass through rigorous project and executive level control "gate" reviews for each state, from inception through disposal. The FBI is in the process of establishing an IT metrics program that identifies and measures IT performance according to industry standards, government regulations, and earned-value management system principles.

**Recommendation:** The FBI's contracting strategy should be tied to features of its EA; e.g., it should identify opportunities for multiple, smaller contracts with

well-defined deliverables and major progress checkpoints. This strategy should also highlight areas in which the FBI requires in-house or trusted technical expertise to define and manage key concepts that govern contracts and relationships between contractors. Status: This recommendation is implemented in the LCMD. Acquisition reform efforts will include consolidation of numerous existing contracts to leverage economies of scale and avoid duplication of effort. Strategies will be tied to EA, as appropriate.

#### Human Resources

Recommendation: Because of their importance to the short- and long-term success of the FBI's IT modernization efforts, the FBI must permanently fill the positions of Chief Information Officer (CIO) and Chief Enterprise Architect, and the committee concurs with the Director's judgment that filling these positions with appropriately qualified individuals should have the highest priority. Status: The position of CIO was filled in May 2004, and the positions of Chief Technology Officer (CTO) and Program Management Executive (PME) were filled in August 2004.

Recommendation: The FBI should develop an improved system for internally reviewing the state of progress in key IT programs and for communicating relevant findings to key stakeholders, thus preempting the perceived need for and distraction of constant external investigations. Status: The LCMD implements such a system.

**b. The specific recommendations that you plan to implement, and when you plan to implement them;**

#### Response:

##### Enterprise Architecture

Recommendation: The FBI should give high priority to reducing the management complexity of its IT systems, even at the expense of increased costs for hardware that may appear duplicative or redundant. Status: The LCMD establishes a structure by which new and existing IT proposals and systems will be evaluated to ensure they are being managed appropriately. Reducing management complexity is a priority in the development of the FBI's "To Be" or "target" architecture, scheduled for the late spring or summer of 2005.

Recommendation: The FBI should make heavy use of scenario-based analysis in its development of an enterprise architecture. Status: Phase II of the EA development includes scenario-based analysis, which will be included in the target architecture scheduled for the late spring or summer of 2005.



### System Design

**Recommendation:** The FBI should develop a process map for information sharing that clearly defines the current state and a desired end state for the information-sharing process so that the numerous information-sharing initiatives can be coordinated and properly monitored and managed. **Status:** The FBI defers to DOJ, who is taking the lead on this recommendation.

**Recommendation:** The FBI should develop a future release plan for VCF that specifies what capabilities will be added to it, in what order, and in what time frame. **Status:** The FBI is employing a two-track plan designed to move us forward. Track One, also known as Initial Operating Capability (IOC), will test the Virtual Case File (VCF) prototype that has already been developed. Beginning in mid-January 2005 and for the following three months, personnel in the New Orleans field office, the Baton Rouge Resident Agency, and the Criminal Investigative Division's Drug Unit at FBI Headquarters will use the prototype VCF as their document routing system. This will assist the FBI in determining at least three things: 1) how easy the graphic interface is to use and how the electronic workflow process works from a business perspective; 2) what impact the prototype system has on the performance of the new Trilogy network; and 3) how training can be improved so that we can deliver the most helpful and user-friendly training possible Bureau-wide. Armed with these lessons and the new ACS interface, the FBI will move forward with Track Two - the development and delivery of a computer-based investigative case management system that will help the FBI meet its responsibilities to our country more efficiently. As part of the Track Two activities, the FBI has asked a new contractor to examine the latest version of the VCF as well as available off-the-shelf software applications and those designed for other agencies, to determine the best combination to meet the FBI's needs. In many ways, the pace of technological innovation has overtaken the original vision for VCF, and there are now existing products to suit the FBI's purposes that did not exist when Trilogy was initiated. The FBI has also asked a different contractor to review and verify users' requirements, because the mission of the FBI has evolved and there are new requirements for information and intelligence sharing.

### Human Resources

**Recommendation:** For Trilogy and subsequent IT projects to have access to the human talent they need to succeed, the FBI must dramatically grow its own internal expertise in IT and IT contract management as quickly as possible. **Status:** 25 IT managers have taken the EA Program Management Program review course, and 20 are currently enrolled in the program. A training curriculum for all IT employees is scheduled for implementation by the fall of 2005.

Recommendation: The FBI should seek relief from excessively tight constraints on reprogramming allocated funds, or at least seek to streamline the approval process. Status: The FBI hopes to accomplish this during FY 2005.

**c. The specific recommendations that you do not plan to implement, and why you do not plan to implement them.**

**Response:**

**System Design**

Recommendation: The FBI should refrain from initiating, developing, or deploying any IT application other than VCF until a complete EA is in place. Status: FY 2004 efforts include development of the "As Is" baseline and the EA Board. FY 2005 efforts will include initiation of the "To Be" architecture. Applications will include EA compliance and review as appropriate.

Recommendation: The FBI should immediately develop plans that address recovery of data and functionality in the event that essential technology services are subject to denial-of-service attacks (e.g., from viruses and pervasively replicated software bugs). Status: Some plans have been developed with respect to classified, mission-critical systems to provide system redundancy and fail-over capabilities. Broader, system-wide plans would require additional funding.

**19. The National Academies report concluded that the Virtual Case File is not now and is unlikely to be an adequate tool for counterterrorism analysis, and that the FBI needs to start "more or less from scratch" to develop the operational requirements for its intelligence functions. Do you agree with the National Academies' assessment?**

**Response:**

Following the 5/20/04 National Academies' report, the Committee on the FBI's Trilogy Information Technology Modernization Program issued a letter to Director Mueller, dated 6/7/04, highlighting the FBI's progress in addressing the report's findings. This letter acknowledged that VCF was designed primarily to enhance workflow automation, serving as the vehicle for various data feeds into analytical applications. One such application is the Investigative Data Warehouse (IDW) project, which encompasses CT activities as well as the deployment of criminal investigative capabilities. These capabilities will be extended Bureau-wide and to joint activities (including the JTTFs). IDW is a concept describing the preparation and organization of a variety of databases so they can be searched in a coordinated fashion along with other databases. This coordinated searching across several databases is known as advanced data analysis. IDW provides FBI investigators and analysts, particularly those

investigating terrorism and criminal conspiracies, with a new capability to easily and rapidly search and share information across all FBI investigative files, including text, photographs, video, and audio materials. It appears from the 6/7/04 letter that the Committee's understanding of the purpose and scope of VCF was assisted by a meeting at which FBI CIO Azmi explained this technology in more detail, including its role as one of the data feeds into IDW. Based on this preliminary information, the Committee indicated that "IDW appears to provide some of the key capabilities necessary for intelligence use."

**20. Is it true that the FBI still does not have in place an automated system that will allow the FBI to share top secret and sensitive compartmentalized information internally and throughout the intelligence community or an automated system to allow FBI employees to readily access and share information throughout the FBI? Please explain your answer.**

**Response:**

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

**21. The OIG's December 2003 Report on the FBI's efforts to improve the sharing of intelligence and other information reinforced the need for the Virtual Case File and the problems with the Automated Case Support (ACS) system: "Under ACS, all documents, including ECs, require handwritten signatures; therefore, all documents are physically passed from person to person as they move through the review chain." Given the continuing delays in implementing VCF, are the procedures and paper-intensive approach of ACS still being used? Is there any plan in place to make the eventual transition to VCF easier? Are files, new and archived, being scanned and maintained on-line?**

**Response:**

The current ACS file system utilized within the FBI does present limitations. ACS works adequately as a retrieval device to aid in the analysis and evaluation of information for investigative purposes. The system does not, however, support the sharing of important unclassified and classified materials with outside agencies. When ACS was developed, FBI investigations were primarily criminal in nature. Consequently, most investigations were not classified and those that were classified were classified at the secret level. ACS was developed to run on the FBI's internal network, which has been certified and accredited for secret-level information only and, therefore, cannot be used to transmit top secret or sensitive compartmented information. To rectify these shortcomings, the FBI initiated several methods of information sharing that afford the ability to electronically share and analyze both classified and unclassified information.

The FBI is increasing desktop access to the Internet by those with a need to share sensitive but unclassified information with law enforcement and IC partners. This

capability would also facilitate access to both the LEO and RISS networks. LEO is a national interactive computer communications system and information service; an intranet system exclusively for the law enforcement community. The RISS program is composed of six regional centers that share intelligence and coordinate efforts against terrorist and criminal networks operating in many locations across jurisdictional lines.

VCF was originally envisioned as a case management tool to replace the ACS system. In many ways, though, the pace of technological innovation has overtaken the original vision for VCF. Because the mission of the FBI has evolved and there are new requirements for information and intelligence sharing, the FBI has asked Aerospace Corporation, a not-for-profit federally funded contractor, to review and verify FBI users' requirements. It is likely that VCF or its successor software will be deployed in phases, which will ease the transition for FBI employees.

**22. If VCF is the system needed for the FBI to greatly improve the FBI's ability to share intelligence and other information, and if the current system was the critical weakness in the FBI's intelligence analysis and dissemination, what, if any, "stop gap" measures are currently in place to close the holes caused by the faulty and antiquated system the FBI is still working under?**

**Response:**

The FBI is working on several IT improvements outside of Trilogy, including IDW, which permits sophisticated analysis of information from multiple data sources. The FBI has also changed its approach to IT to facilitate centralized management and to permit better coordination. The FBI now has a full-time CIO, who is responsible for the FBI's overall IT efforts, including: 1) developing an IT strategic plan and operating budget; 2) developing and maintaining the FBI's technology assets; and 3) providing technical direction for the re-engineering of FBI business processes. The CIO is in the process of formulating a strategic IT plan which takes into account the needs of the Intelligence Program, outside customers, and field and FBIHQ division needs. The FBI's Chief Technology Officer is responsible for guiding the IT research and development functions of the FBI. An EA Board, made up of 14 representatives from eight FBI divisions, meets regularly to review technical proposals for new FBI IT systems.

**Translators**

**23. It has been nearly 3 years since Congress directed the Attorney General to prepare a comprehensive report on the FBI's translator program. I authored that reporting requirement – and it was a requirement, not a request. It was included in the USA**

**PATRIOT Act so that Congress could better assess the needs of the FBI for specific translation services, and make sure that those needs were met. The Foreign Translation Program is vital to our understanding of virtually every piece of intelligence information from the Middle East.**

**a. When will the report issue?**

**Response:**

Section 205(c) of the Act required the Attorney General to provide a report to Congress on the employment of translators by the FBI and other components of the Department, but the Act did not specify the form or a timeline for submission of this information. The report called for by section 205(c) was transmitted to Congress on 12/22/04.

**b. What are the current needs of the FBI for specific translation services? Is the FBI where it wants to be, right now, today, as of this moment?**

**Response:**

Since the beginning of FY 2001, FBI audio and text translation requirements have increased by 51%. In several Middle Eastern languages, such as Arabic, collection has increased by more than 100%. Because of this increased demand, and despite an addition of several hundred translators during this period, unaddressed work remains in certain languages. Simply put, the growth in demand for FBI translation services has outpaced the increased translator supply.

The President's FY 2006 budget includes a \$27 million enhancement to the FBI's language analysis program, supporting an additional 274 language analyst positions above the FY 2005 funded staffing level of 490 language analyst positions. This funding would greatly enhance the FBI's capacity to address intelligence collected in foreign languages in support of critical counterterrorism and counterintelligence investigations, to provide the National Virtual Translation Center with a permanent staff of linguists, and to address an expected FY 2006 deficit in the FBI's contract linguist program.

**c. Are there any legal or practical impediments to using translators employed by other Federal, State, or local agencies, on a full, part-time, or shared basis? Have such options been explored? If not, why not.**

**Response:**

The scarcity of qualified translators available to federal agencies, particularly among Middle Eastern and Asian languages, has been documented through

several studies (these studies include the 1/31/02 GAO report referenced above and a 2001 report by the National Commission on Terrorism entitled, "Countering the Changing Threat of International Terrorism"). Since most agencies' demands for translator resources exceed the supply, the concept of sharing translators is not practical, because each agency's natural tendency is to preserve limited resources for its own use. Such sharing is further impeded by non-uniform proficiency testing and clearance requirements.

Intermediate and long-range benefits of pooling federal translator resources are possible, but only if each federal agency is equally committed to the aggressive recruitment of translators and/or to the internal development of translator resources through language training. Otherwise, scarcity issues will continue to pose barriers to translator sharing.

There would likely be immediate, though limited, benefits from the pooling of IC and federal law enforcement translator resources in languages where demand is diminishing or shifting across agencies or where needs are sporadic. This is especially true when the lending agency has higher vetting and clearance standards than the receiving agency. For example, the FBI's current excess supply of Spanish CL resources could be immediately absorbed by DEA, Customs, or ATF because of the rigorous vetting and clearance requirements of the FBI. However, it would often be difficult for the FBI to absorb the resources of those agencies because most DEA, Customs, and ATF translators are cleared only for access to law enforcement sensitive information and not to national security information.

At the state and local law enforcement level, translation services are typically provided by police officers whose language proficiencies are uncertified or by CLs. While the FBI reviews any opportunities for resource sharing carefully, in most cases the law enforcement officer or translator does not possess the requisite security clearance to provide services to the FBI. For example, when the FBI's Chief of Language Services recently met with the Deputy Commissioner of the New York Police Department (NYPD) regarding the feasibility of such resource sharing, the NYPD indicated that they did not want their officers to undergo polygraph examinations, thus precluding them from receiving Top Secret clearances.

**24. How is the monitoring of an unprecedented 1,727 new FISA wiretaps impacting on critical FBI resources? How do these numbers "translate" to the Bureau's ability to obtain, understand, assess, analyze and, if necessary, act upon threat information obtained in a foreign language and from a foreign culture?**

**Response:**

While the number of wiretaps pursuant to the Foreign Intelligence Surveillance Act (FISA) has increased dramatically, the number of linguists to monitor these intercepts has also grown, from 883 linguists in 2001 to over 1200 linguists today. The FBI is continuing to process thousands of applicants to further enhance capabilities in the most critical languages. Although in the past the FBI's collection capabilities have outpaced its ability to process the materials acquired in several languages, successful hiring has eliminated the performance gaps in some languages and is steadily eroding the gaps between collection and review in other languages. The Language Services Translation Center at FBIHQ manages the FBI's translation resources, which are located throughout the country. The Center works closely with the FBI's operational program managers to prioritize the review of FISA materials, and will review previously untranslated material whenever the investigative value of the material becomes apparent.

**25. When can we expect implementation of a statistical reporting system that will be able to track the status of translations so that the FBI can know what items are not being timely translated and provide insight as to why?**

**Response:**

While the FBI has statistical reporting systems and other automated mechanisms in place to ensure the efficient use of translation resources, these systems are antiquated and mostly exist in a decentralized environment. To improve capabilities in this vital area, a Bureau-wide statistical reporting system known as Workflow Manager (WFM) has been developed for FISA electronic surveillance collections. WFM will measure review frequencies and production rates for trend analysis and command and control purposes. WFM is undergoing a test and evaluation process and is expected to become fully operational by the end of CY 2004.

**26. Will data from translated material obtained through FISA wiretaps be included in the Virtual Case File system? If not, why not? How do agents and analysts currently do searches of FISA wiretap data to try to "connect the dots?"**

**Response:**

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

**27. Did the resources that the FBI requested DOJ to include in its 2005 budget request to fill performance gaps in the FBI's translator program differ in any way from the resources that DOJ ultimately sought in its 2005 budget request? If so, in what way? What other resources will assist the FBI in filling performance gaps.**

**Response:**

Executive Branch agencies are not permitted to release pre-decisional data regarding budget requests. The President's FY 2005 budget requests an increase of 86 positions and \$12.838 million for the FBI's Language Program.

**28. During the hearing, Senator Grassley asked you about the retroactive classification of information provided by the FBI to Committee staff related to a whistleblower who previously worked for the FBI translation program. I share Senator Grassley's concern that this order is unrealistic. A great deal of information regarding the whistleblower's claims, including the FBI's corroboration of many of the problems she raised, has been in the public record for more than two years. I appreciated your statement that the retroactive classification order was not intended to place a gag on Congress. However, the notice received by staff members of the Judiciary Committee was very vague, referring only to "some" information conveyed in the briefings. If state secrets are truly implicated by something that was said in an unclassified briefing two years ago, the FBI should provide very specific instructions to current and former staff on what information must be kept secret. Will you instruct your staff to provide more specific information to relevant staff about what, exactly, from the 2002 briefings is classified and what is not?**

**Response:**

There was no reclassification of any information at any time with respect to matters regarding Ms. Edmonds. Some information regarding this matter has always been classified. Other information was classified as of October 18, 2002, when the Attorney General asserted the state secrets privilege and DOJ moved to dismiss Ms. Edmonds' employment case. No further original classification occurred after October 18, 2002, and there was never any reclassification. We could provide a classified briefing for staffers who possess the necessary clearances.

**Arrest Statistics**

**29. The GAO issued a March 2004 Report on Federal Law Enforcement on Use of Investigation and Arrest Statistics that appears to validate double or triple-counted investigation and arrest data to measure individual work load and performance. I think there is a need to distinguish among law enforcement agencies by valid statistics that can measure when an agency is actually working or simply piggy-backing on a multi-jurisdiction investigation to which they added little by way of resources or manpower. Congress often relies on the same data in determining FBI productivity and resource allocation. As GAO points out, if law enforcement agencies were to distinguish between unilateral and joint arrests and investigations within their databases, this distinction could help guide Congress when making budget decisions about these agencies. The agencies could modify those databases to reflect even more refined data. GAO also suggested that a**



**federal repository of joint investigations and arrests conducted by federal law enforcement is a good starting point.**

**a. Do you support the need for such a repository?**

**Response:**

In light of the inherent complexities in the creation and maintenance of a centralized repository, we would need to determine whether the intended benefits would justify the added burdens and costs associated with the activity. For example, a single repository would require the integration of all federal agency information systems to efficiently report arrest-related data. Because numerous federal agencies (including numerous Inspectors General) have federal law enforcement authority, the creation of a single, integrated repository would be labor intensive. In addition to the need to assimilate potentially incompatible data, software, and hardware, such an effort would need to accommodate the fact that some information systems, including the FBI's, permit limited access for security reasons, so that integration with non-secure systems may not be supportable. Any process other than an automated integration would add manual reporting responsibilities, burdening personnel already overburdened with administrative responsibilities. Creation of a "federal repository of joint investigations and arrests" would also require the development of definitions that do not currently exist. For example, if the FBI conducts a multi-year, complex investigation and the U.S. Marshals Service assists only by effecting the arrests, would this constitute a "joint investigation"? If other organizations were not afforded appropriate "credit," would they be as willing to assist? If these organizations do receive a "joint investigation" credit, does this fairly represent the organizations' roles? Which organization would maintain and support the repository?

It is also critical to the FBI that the creation of a single repository not jeopardize interagency cooperation and coordination. As discussed below, there is a risk that changes to data reporting may appear to diminish the benefits participating agencies currently derive from assisting one another. The FBI would not perceive as advantageous anything that may jeopardize the growing inter-agency cooperation we have worked so hard to achieve.

**b. What are the pros and cons of establishing such a repository?**

**Response:**

A single repository would make it easier for GAO to track contributions to the federal government's law enforcement effort. The greatest disadvantages in establishing such a repository are the resources required to gather and report

information and the possible damage such reporting would inflict on critical joint working relationships.

Over the years, the FBI has forged partnerships with many state, local, and federal agencies in an effort to: (1) improve interagency cooperation and coordination; (2) maximize the development of intelligence in furtherance of inter-agency interests; (3) improve the effectiveness of operations; (4) take advantage of inter-agency talents, experience, and abilities; and (5) augment personnel resources to ensure mission accomplishment even when resources are limited.

If distinctions between unilateral and joint investigations are made, it will be important to ensure that these distinctions do not harm inter-agency cooperation. Joint investigations are often more successful when all parties share equally in accomplishments. This is particularly important in long-term, complex investigations in which smaller agencies offer the assistance of their limited personnel with the understanding that they will share equally in the investigative results and accomplishments even though the resources they commit are not as great as those contributed by larger organizations.

The FBI has always worked to afford appropriate credit to all participating organizations, regardless of the level of resource commitment. Sometimes the commitments of other organizations, while minor compared to those of the FBI, are particularly significant because they are based on that organization's expertise in a specialized area or unique ability to make a critical contribution, or are relatively more burdensome to that organization due to its very limited resources. Attempts to rate or categorize the relative contributions of various organizations is, however, quite difficult. If the FBI allocates five Agents to a highly complex white collar crime investigation, while the IRS commits one Agent, who would claim the "unilateral" indictment, arrest, and conviction accomplishments, and who would claim the "piggy-back" accomplishments? If the result of this investigation is the arrest of a prominent CEO of a major corporation and there is only one reportable accomplishment, how is credit assessed? Will organizations seek the credit most likely to be valued during congressional allocations of resources? If sufficient value is not attached, will the level of cooperation and coordination presently enjoyed be significantly impaired as agencies seek the credit most beneficial to their own interests in the congressional budget process?

**c. Do you agree that the FBI should distinguish between unilateral and joint arrests and investigations? If not, why not?**

**Response:**

The FBI believes it is important to distinguish between single, or "unilateral," agency arrests and multi-agency, or "piggy back," arrests, and that it is important

to apply uniform standards in reporting these accomplishments, provided this can be done without harming the joint working relationships that are often critical to investigative success, as indicated above.

Arrests are but one statistical accomplishment measured by the FBI. Generally, productivity in criminal matters is measured more by the numbers of high quality indictments and convictions because they are more indicative of the quality of investigative results and support for the affiliated U.S. Attorney's Office than arrest statistics alone. There are exceptions to this general guideline, such as when the arrest is the result of: an incident in which an Agent took direct action to save lives or property; or a fugitive investigation conducted in support of state, local, or international law enforcement authorities and the fugitive is believed to have been involved in serious violent crimes.

As noted in the GAO Report, the FBI credits each arrest only once, though an Agent who participates in an arrest can be credited with an "assist." If the arrest occurs in the context of an inter-agency investigation, this is reported in the FBI's Integrated Statistical Reporting and Analysis Application database. Although it is the FBI's understanding that, in multi-agency operations resulting in arrest, each participating agency claims an "arrest," the FBI is not aware whether other agencies report the multi-agency nature of the operation or whether they distinguish between arrests and assists.

### **First Responders**

**30. The Associated Press reported on May 26 that police in Vermont and New York will be able to check suspects instantly against the U.S. Government's terrorist watch lists under a "first-of-its-kind, FBI-coordinated program."**

**a. What is the name of the database system being used for this program?**

### **Response:**

The Upstate New York Regional Intelligence Center (UNYRIC) has an established Memorandum of Understanding (MOU) with CT Watch pursuant to which they submit a name check request for subjects who are stopped in circumstances consistent with possible terrorism activity. Under this agreement, CT Watch checks submitted names against the FBI's ACS system, the TIPOFF database, the FBI Watchlist, and the DHS Interagency Border Inspection System (IBIS) for possible terrorism watchlisting. The agreement provides for response within 20 minutes for "immediate" requests and within a reasonable amount of time for "routine" requests. The CT Watch has been performing these checks for UNYRIC since 2003 and sends facsimiles to requesters indicating search results.

The UNYRIC has always serviced the State of New York and recently entered into an agreement to provide these same services to the State of Vermont.

With the creation of the Terrorist Screening Center (TSC), the watchlist subjects in these databases are now uploaded into both ACS and DOJ's Violent Gang and Terrorist Organization File (VGTOF). The UNYRIC now receives hits from all of these databases by directly querying NCIC/VGTOF, and continues to send facsimile requests directly to CT Watch for subjects who are stopped in circumstances consistent with possible terrorism activity but on whom there is no NCIC/VGTOF hit. When these facsimile requests are received, they are checked against ACS (which now includes TIPOFF, IBIS, and VGTOF records) for any references to FBI-related matters.

**b. When was it first available for implementation?**

**Response:**

ACS has been used in UNYRIC requests since 2003, but the capability to search the uploaded TIPOFF, IBIS, and VGTOF records through ACS became available after the TSC began operations on 12/1/03.

**c. What 12 databases will the Vermont police be able to check?**

**Response:**

The database searched when the UNYRIC faxes a request to the FBI's CT Watch is ACS, which includes the TIPOFF, IBIS, and VGTOF databases.

**d. Are the Vermont police being provided direct access to the databases or are they being provided a number to call at the FBI? Please provide more information on the "direct line" being provided to Vermont police to report suspicious activities to Federal law enforcement. Is the "direct line" a two-way line -- that is, will Federal law enforcement have a direct line to Vermont police about suspicious activities in Vermont?**

**Response:**

The only direct access the Vermont Police have is through running routine NCIC/VGTOF queries (all U.S. law enforcement officials have the same capability). The Vermont Police send database check requests to the UNYRIC, which forwards the requests to CT Watch. There is no direct contact between the Vermont State Police and CT Watch (unless the State Police receive a VGTOF hit and go through the established process with the TSC). The UNYRIC may contact CT Watch through a direct telephone number to advise that a fax inquiry is being sent or to confirm that a fax was received. If the inquiry results in a hit, the

UNYRIC is notified and CT Watch puts an FBI Agent in touch with the UNYRIC directly.

The UNYRIC-CT Watch MOU provides a process for name check requests only, and it is not a mechanism for reporting "suspicious activity." The UNYRIC has a system in place by which suspicious activity deemed to be related to terrorism is reported directly to the appropriate FBI JTTF for immediate action. While the UNYRIC does not routinely report these matters to CT Watch, CT Watch notifies the affected JTTFs when this occurs.

**e. What safeguards and/or technology protocols are in place to protect data security and privacy and to ensure that searches are pertinent to individualized investigations?**

**Response:**

There is no transfer to the UNYRIC of information containing the specifics of FBI cases or TIPOFF records. The UNYRIC is simply made aware of FBI investigative interest and provided with an FBI case Agent or Field Division point of contact for further coordination. The CT Watch name check request form requests the justification for the name search, and this justification is reviewed by CT Watch personnel. If the justification does not relate to terrorist activities, the UNYRIC will be contacted to determine whether additional justification exists.

**Ricin**

**31. Following the February 2004 ricin scare that shut down some congressional offices for as much as four business days, some of us learned for the first time there had been an earlier ricin attack directed at the White House. *USA Today* and other newspapers reported that ricin was first detected and investigated by the Secret Service on November 7, 2003, at an off-site mail processing center for the White House, although the FBI, the White House, and other agencies were not notified until November 12.**

**a. Is it correct that the FBI was not notified until November 12?**

**Response:**

Yes. The FBI was notified by the Secret Service at approximately 10:30 p.m. on 11/12/03.

**b. If the FBI learned about the attack in November, why was no information provided to the Congress or to other relevant high-priority targets of al Qaeda?**

**Response:**

The texts of the two letters containing ricin, one of which was sent to the Secretary of Transportation and the other to the President, indicated that the ricin attacks were intended to cause the Department of Transportation (DOT) to make changes in the implementation of DOT trucking regulations. These threats were not related to al Qaeda or to international terrorism, and did not convey a threat to Congress or other high-priority al Qaeda targets.

**c. Did the FBI ever notify State and local law enforcement officers? When and through what mechanism?**

**Response:**

State and local law enforcement officers were notified on 11/13/03 through the National Joint Terrorism Task Force (NJTTF) and the JTTFs located in Washington, D.C., and Columbia, South Carolina.

**d. Have there been any changes or policies implemented at the FBI based on the federal government's law enforcement response to the ricin attacks? If so, please describe in detail.**

**Response:**

Yes. The FBI Laboratory and the Edgewood Chemical and Biological Center have begun efforts to develop more sensitive and dependable ricin detection methods. The FBI Laboratory has also begun closer collaboration with the Secret Service Laboratory in order to facilitate improved communication in these cases.

**USA PATRIOT Act/FISA**

**32. You testified that many of the FBI's counter-terrorism successes are the direct result of PATRIOT Act provisions. Please provide more specific information on how particular PATRIOT Act provisions have helped in particular counter-terrorism investigations.**

**Response:**

On 7/15/04, the Attorney General released "Reports from the Field: The USA PATRIOT Act at Work," which contains unclassified examples of cases in which the USA PATRIOT Act has been instrumental in counterterrorism investigations.

**33. You testified that, prior to the PATRIOT Act, "if a court-ordered criminal wiretap turned up intelligence information, FBI agents working on the criminal case could not share that information with agents working on the intelligence case." Please state**

**specifically what law or laws prevented such information-sharing prior to PATRIOT, and whether a court could authorize such information-sharing, regardless of any such law or laws?**

**Response:**

Prior to the changes effected by the USA PATRIOT Act, 18 U.S.C. 2517 was interpreted as authorizing the sharing of intercepted wire, oral, and electronic communications solely for criminal law enforcement purposes in the absence of a court order. Sharing intercepted information for foreign intelligence purposes required a court order, but the statutory language was unclear as to who would sign the order. The changes to the USA PATRIOT Act clearly allow the sharing of foreign intelligence information developed during a court-ordered criminal wiretap with the Agents working intelligence cases.

**34. You further testified that, prior to the PATRIOT Act, "information could not be shared from an intelligence investigation to a criminal investigation." Please state specifically what law or laws prevented such information-sharing prior to PATRIOT?**

**Response:**

Prior to the USA PATRIOT Act, there were procedures for sharing information between intelligence investigators and criminal Agents and prosecutors, but they were burdensome and usually resulted in less than complete information sharing. For example, the FISA statute was understood to require that, in order to secure a FISA Court order, the "primary purpose" of the activity had to be the acquisition of intelligence. Because of this interpretation, DOJ and the FISA Court placed procedural prerequisites on the sharing of intelligence with criminal investigators and prosecutors. Additional information is provided below in response to Question 35.

**35. In his statement to the 9/11 Commission, the Attorney General blamed the creation of the so-called "wall" between criminal investigators and intelligence agents on a 1995 memorandum authored by a senior official in the Reno Justice Department, now a member of the 9/11 Commission.**

**a. Do you agree that the architecture of the wall was in place long before 1995, having its genesis in established legal doctrine dating from 1980? If not, how do you explain the extensive discussion of this issue in the one and only reported opinion of the FISA Court of Review, decided on November 18, 2002? How did the FBI handle information-sharing between criminal investigators and intelligence agents before 1995?**

**Response:**

A distinction between the criminal investigation and intelligence functions existed before 1995, but the relationship between criminal and intelligence investigators became more distant as the "wall" developed and became more entrenched. In the years before FISA, and, indeed, in the early years of FISA, the relationship between criminal and intelligence investigators was closer than it was in 1995. In the 1980s, for example, criminal agents and intelligence agents were relatively free to talk to each other just as they had pre-FISA. Perhaps more significantly, prosecutors were free to give advice to both criminal and intelligence investigators because criminal process is always one option for the disruption of activities potentially harmful to the national security. By 1995, however, the wall precluded the sharing of all classified information – not just that which derived from FISA. Within a year thereafter, prosecutors were barred altogether from giving advice, and could only receive information about the progress of an intelligence case, unable to comment or make suggestions of any kind. Similarly, the intelligence agent and the criminal agent working related cases were by this time barred from discussing the intelligence aspects of the case, although criminal agents could disclose information to intelligence agents.

**b. Do you agree that the Gorelick memo established proactive guidelines amidst a critically important terrorism prosecution to *facilitate* information sharing?**

**Response:**

According to those who were directly involved in the case to which this memo refers, DOJ was trying to ensure that there were no artificial barriers to the flow of information. For those who were not involved in the specific case covered by the memo, the memo served to confirm that walls were necessary and that criminal investigators and prosecutors should not have access to classified information – even if that information was not obtained through FISA.

**Inspector General Audit Report on FBI Information-Sharing**

**36. Please provide me a copy of the information-sharing process map recommended by the OIG in its Audit Report dated December 2003. If not yet completed, when do you expect the map to be completed and will you ensure that I receive a copy promptly?**

**Response:**

The FBI's 12/5/03 Information Sharing Strategy was provided to the OIG pursuant to its recommendation that the FBI develop an FBI-wide enterprise architecture and process map. Because that report is **For Official Use Only**, and



therefore not appropriate for public dissemination, it is provided as an attachment to the Classified responses.

**37. The Inspector General recommended in the December 2003 Report that certain domestic terrorism cases involving “lower-threat activities by social protestors or crimes committed by environmental, animal rights and other domestic radical groups or individuals (unless explosives or weapons of mass destruction are involved)” should be transferred to the responsibility of the Criminal Division as opposed to the Counterterrorism Division. The FBI rejected this recommendation, believing that the transfer would “dilute the intelligence base” directed to other international and domestic terrorism matters.**

**a. Has the investigation of these types of social protestors in fact led to useful leads in international terrorism cases involving, for example, al Qaeda?**

**Response:**

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

**b. Are criminal prosecutions of “lower-threat activities by social protestors” part of the “terrorism” arrest statistics reported by the FBI?**

**Response:**

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

#### **Domestic Intelligence Agency**

**38. The 9/11 Commission completed a critical report on the performance of the intelligence community with the statement: “A question remains: Who is in charge of intelligence?” The report described a “loose collection” of intelligence agencies that often operated independently of one another with little communication or cooperation, and concluded that the goal of central coordination has still not been realized. You told the 9-11 Commission it would be a “grave mistake” to have a separate domestic intelligence agency. Why? Another option would be a statutorily-created “domestic intelligence unit” within the FBI. What is your position on such a unit?**

**Response:**

#### **Creating a Separate Domestic Intelligence Agency**

Creating a separate domestic intelligence agency would present numerous difficulties. While we cannot foresee every problem that would arise, we predict that the following challenges would impair the effectiveness of such an agency.

### Operational Disruption

The logistics of transferring intelligence elements out of the FBI and establishing them within a new agency would disrupt the FBI's ongoing efforts to prevent terrorist attacks. The new agency would be required to develop the infrastructure the FBI has been building for the past 96 years. During this building process, the FBI's domestic intelligence efforts would be less organized and structured, and many of the FBI's leaders and decision-makers, who would otherwise be focusing on CT operations, would instead be devoting their time and attention on agency building. The result would be a lower level of preparedness and protection against terrorist attack.

In weighing this option, it is important to consider that al Qaeda has demonstrated its ability to adapt its plans based on an assessment of the United States' level of preparation, avoiding the strengths of U.S. defenses and exploiting vulnerabilities. In light of that intelligence, it is reasonable to assume that al Qaeda might attempt to exploit the disruption caused by the creation of this agency, particularly in the period before it is functioning fully.

### Stove-piping

The creation of the new agency would likely recreate many of the obstacles to information sharing and operational coordination the FBI has worked hard to eliminate since the 9/11 attacks, building an operational wall between intelligence and law enforcement operations after the FBI succeeded in eliminating this impediment. The FBI and CIA have developed an effective process for coordinating the domestic and overseas dimensions of international terrorism investigations; movement of this responsibility to a new agency would complicate both the FBI's investigation of transnational terrorist threats and its inter-agency information sharing efforts. Finally, it would create the conditions for likely jurisdictional disputes, as the FBI and the new agency struggle to determine when a particular terrorist investigation is an "intelligence investigation" and when it is a "law enforcement investigation."

### Diminished Ability to Cultivate Cooperators

There are two basic means by which an investigating Agent induces an individual to divulge information he or she is otherwise unwilling to provide. One is to promise the individual a benefit, such as money, if the information is provided. The other is to threaten to harm his interests, typically through arrest, prosecution, or deportation, if he refuses to do so. The FBI uses both approaches to develop and sustain its network of informants, sources, and cooperators.

An Agent in a separate intelligence agency without arrest powers would be handicapped in this process. While cooperation could be induced through the promise of benefits, the specter of imminent legal action would be unavailable. To gain cooperation in this manner, the new agency would instead have to obtain the assistance of a law enforcement officer, which would entail briefing the officer about the individual and waiting for that officer to receive authorization to initiate a criminal or immigration proceeding against the individual. This awkward and time-consuming process would complicate the recruitment process and render this new agency less effective in developing human intelligence.

This would be a serious handicap, especially given the general recognition that the lack of human intelligence relating to al Qaeda was the IC's most glaring operational weakness prior to the 9/11 attacks. The FBI has increased the number of its CT sources by 91% since 9/11/01, but it could not have done so without the full use of both recruitment methods.

#### Lack of Established Relationships with Law Enforcement

As the JTTFs have demonstrated, state and local police departments play critical roles in the war on terrorism. The FBI has seen in cases from Portland to Lackawanna that the 750,000 local police officers who know the communities around this country are often in the best position to learn about terrorist suspects in those communities. Without close collaboration with these officers, a federal agency coordinating an international terrorism investigation cannot expect to obtain the human intelligence it needs. While the FBI enjoys an excellent working relationship with state and local law enforcement that is borne of decades of collaboration, a new agency would be starting operations with no established relationship with the nation's 17,000 different police departments. That relationship could be developed over the years, but our nation's defenses against terrorism would be weakened in that interim.

#### Fragmented Accountability

Currently, the Attorney General and the FBI Director are jointly accountable to the President for both the law enforcement and intelligence components of CT and CI operations within the United States. Separating and assigning the intelligence component to a new agency will simply fragment accountability and make it more difficult to assign responsibility.

#### Cost

Proponents of the M15 proposal have largely ignored the fiscal implications of creating a new agency. It would, in fact, be very expensive to build this new agency, the cost of which would not be covered by transferring the intelligence

funding that was previously allocated to the FBI for several reasons. First, the Bureau would still need a significant portion of those funds to develop and sustain the intelligence program needed to support its remaining areas of responsibility. Second, the new agency would require a substantial front-end investment, significantly greater than the cost of strengthening the FBI's intelligence capacity, to build the basic elements of its infrastructure, such as the facilities, information technology, and administrative operations necessary to support such an agency. The new agency would be competing for these resources with the existing members of the federal law enforcement and intelligence communities.

### Conclusion

These considerations make it clear that creating a separate agency to collect intelligence in the United States would be a grave mistake. Splitting the law enforcement and intelligence functions would leave both the FBI and the new agency fighting the war on terrorism with one hand tied behind their backs. The distinct advantage gained by having intelligence and law enforcement together would be lost in more layers and greater stovepiping of information, even after completion of the difficult transition to the new agency, which terrorists may well see as an opportunity for attack. The FBI's strength has always been, and still is, in the collection of information. While there have been weaknesses in the integration, analysis, and dissemination of that information, the FBI has made great strides in addressing these weaknesses. The United States has a tremendous resource in the FBI. It would be both more efficient and more effective to improve that resource than to replace one of its primary functions with a new agency.

### **Statutory Creation of a "Domestic Intelligence Unit" in the FBI**

The FBI supports the concept of an intelligence service within the FBI. This concept consists of two basic components: (1) creation of a new Directorate of Intelligence, and (2) more effective use of resources. These components can be addressed by applying the following principles.

First, any reform proposal must recognize that intelligence is fundamental to successful FBI operations. Intelligence functions are woven throughout the fabric of the FBI, and any changes to this integrated approach would be counter-productive. Intelligence capability is embedded in every aspect of the FBI workforce and organization - in the Agent and analyst populations, and in the Laboratory, Cyber, Investigative Technologies, and Training Divisions. Because of this integration, the FBI can analyze the devices and techniques of our adversaries, making information acquired from them available to our partners in the IC and in state and local law enforcement.

Second, the FBI must continue to integrate intelligence and law enforcement operations, employing both intelligence and criminal investigation tools as parts of an integrated CT strategy that affords the flexibility to move seamlessly from intelligence gathering to disruption at a moment's notice.

Third, analysis should be fully integrated into intelligence collection and other operations so that intelligence can drive the investigative mission.

Fourth, the FBI should have centralized management with distributed execution. Central management should support national collection efforts, information sharing, and dedicated strategic analysis that pulls intelligence from all FBI offices and across all programs, and ultimately drives planning and the allocation of resources.

And fifth, the FBI should limit stovepiping of intelligence collection and analysis, and encourage synergy in its operations and in collaboration with partners.

With these guiding principles in mind, the FBI supports the creation of a strong intelligence service within the FBI that leverages its formidable collection capabilities and fully integrates its efforts with its law enforcement and IC partners.

The first step toward this "service within a service" is to build upon the FBI's existing Office of Intelligence to create a Directorate of Intelligence with broad and clear authority over intelligence-related functions. The authority of the FBI's Executive Assistant Director for Intelligence (EAD-I), who now provides policy and oversight, would be extended to cover all intelligence-related budgeting and resources.

This structure would support each critical intelligence-related function, beginning with the critical function of management of the FBI's intelligence requirements process - the ongoing cycle of identifying intelligence gaps and directing collection to fill those gaps.

#### Management of Intelligence Requirements and Collection

The FBI currently has an Intelligence Requirements and Collection Unit that provides independent and centralized management of its intelligence requirements and collection functions. The efforts of this Unit would be strengthened by: (1) working with target experts to develop collection strategies to fill gaps in knowledge; (2) developing, implementing, and overseeing FBI standards for the validation of assets and sources; and (3) making intelligence from human sources available across program lines.

### Information Sharing

The EAD-I is responsible for information-sharing policy, and the FBI expects demands in this area to increase. In particular, the FBI must participate fully in the Justice Intelligence Coordinating Council (JICC), DOJ's Law Enforcement Sharing Initiative, the Director of Central Intelligence (DCI) Advisory Group, and other entities.

The FBI's contingent at the Terrorist Threat Integration Center (TTIC) would be part of the FBI's Intelligence Directorate and would be fully incorporated into the FBI's information-sharing efforts.

### Customer Support

To enhance the FBI's support of outside customers in state and local law enforcement, the Directorate would evaluate customer satisfaction, tailor the FBI's support to each major customer, and ensure that these partners are receiving the information they need from the FBI.

### Strategic Analysis

To boost the FBI's strategic analysis efforts, the new Directorate would be responsible for the organization and implementation of strategic intelligence campaigns to support major cases, crisis response, and significant threats. The Directorate would work with operational counterparts to design, organize, implement, and manage an FBI intelligence system support structure.

The proposal also envisions promoting enterprise-wide strategic analysis through the development of analytic products that cross traditional programmatic lines and identify intelligence gaps to facilitate the development of collection and dissemination requirements. This analysis would help the FBI forecast future threats, and would drive the allocation of resources and the development of investigative and intelligence strategies in support of the FBI's mission. This is analogous to the DCI's National Intelligence Council (NIC), which ensures a full-time focus on strategic issues.

### Intelligence Production and Use

To support intelligence production and use, the FBI would build upon existing units to improve its 24-hour intelligence production capability, FBI daily reports, and the FBI's Presidential Intelligence Assessments.

### Field Operations

To support intelligence activities in the field, the FBI would integrate intelligence received from Legal Attachés into the FBI's overall intelligence capability. The Field Intelligence Groups (FIGs) would be thoroughly integrated into the larger IC. The FBI would also focus on the new regional intelligence centers, such as the recently announced CT Unit at the Upstate New York Regional Intelligence Center.

#### Human Talent

To support vital functions related to human talent, the FBI would create a new Intelligence Career Management group to manage the intelligence career track for Agents, intelligence analysts, linguists, and others, including the development of intelligence training across the FBI. An FBI Intelligence Officer certification program would be developed, and would include IC Officer Training. These efforts would enable the FBI to build on its efforts to create career paths for analysts and intelligence Agents.

#### Language Analysis

The FBI's linguists are responsible for more than straight translation. To be effective, they must be familiar with those involved and understand the context in which they are translating. This is fundamentally an analytical function and, accordingly, the FBI's language analysts should be fully integrated into the Intelligence Program as well as into operations. To support this integration, the Language Services Section and the National Virtual Translation Center would be moved to the Directorate of Intelligence.

#### Program Management and Support

Last, but important to the success of this proposal, would be the strengthening of program management support to the EAD-I and across the elements of the Intelligence Program. Emphasis would be placed on: ensuring that FBI Intelligence Program priorities are consistent with those of the DCI, DOJ, and other critical parties; developing the annual Future Threat Forecast; and providing security planning and guidance. Budgeting, evaluations to measure progress, communications and administrative functions, and support for the EAD-I's role as Chair of the JICC would also be emphasized.

#### Budgeting

Formalizing and strengthening centralized management of all intelligence-related resources would be among the key responsibilities of the new Directorate. The OI's initial effort has been the development of the Concept of Operations for Intelligence Budgeting, but it can and should move further. The President's Fiscal

Year 2005 Budget proposes restructuring the FBI's budget decision units from the current ten to four, one of which would be an Intelligence Decision Unit. Similar recommendations have been made by members of the legislative branch and the National Association of Public Administrators. This change would allow the FBI to more effectively and efficiently manage its resources based on national priorities and threat assessments, providing the flexibility needed to internally shift resources to higher priorities and to respond to rapidly developing national security threats. If this change is effected, the Intelligence Decision Unit would be comprised of operational elements, including the existing OI, the FBI's TTIC contingent, programmatic elements representing analysts across the FBI, and administrative elements, such as training, recruitment, information technology, and security. Creation of this Decision Unit would provide internal safeguards for intelligence resources by requiring Congressional notification if funds are reprogrammed, and would permit easier assessment of the level of resources supporting the FBI's intelligence program.

#### Indonesia

**39. In August of 2002, two Americans and one Indonesian were murdered near the Freeport gold mine in Indonesia. Patsy Spier, the wife of one of the Americans killed, has done an extraordinary job of raising awareness of this crime, and has pressed the United States Government to determine who was responsible. The FBI has gone to Indonesia a number of times to investigate this crime, and until recently, has encountered resistance from the Indonesian Military (which is probably responsible for the crimes). Patsy Spier met with you earlier this year and you pledged to see the investigation through to its conclusion. Can you share the status of this case with me? I have worked to condition some military assistance for Indonesia on the government's cooperation with the FBI. Has there been cooperation? Can I have your personal assurance to see that justice is done in this case and that it does not fall through the cracks?**

#### Response:

During the first 14 months of this investigation, cooperation by the Indonesian military (TNI) was assessed as "poor" by the FBI. Since the FBI team traveled to Indonesia in December of 2003, cooperation has dramatically improved, and is currently assessed by the FBI as "good." This is in large part because of the pressure applied by Congress and the Administration, both of which have directly engaged Indonesian officials.

The FBI independently developed sufficient evidence to obtain a 6/16/04 indictment in U.S. Federal Court. The subject charged with the 8/31/02 murders is Anthonius Wamang, a member of the military branch of the Free Papua Movement, commonly known as OPM. The FBI has devoted significant effort to determining if the TNI was responsible for or involved in this attack. To date, the



FBI's investigation indicates that the TNI was not responsible for these murders. You have our assurance that the FBI will continue to pursue this matter to ensure that justice is done.

#### Data Mining

40. Data mining is a potentially critical information technology tool for investigating terrorism and other criminal activity, but it also poses significant challenges for privacy, data accuracy and security, and civil liberties. Well over a year ago, I began writing letters to the Department about its data mining projects and related safeguards, but the Department has failed to answer the questions. For example, on January 10, 2003, I wrote the Department seeking information on private sector databases obtained for data mining or pattern-recognition activities. On March 22, 2004, I questioned the Department about the DOJ-funded MATRIX program, its privacy and security protections, as well as its use of data mining techniques like the "terrorism factor information query capability" to search billions of records -- many of which belong to individuals with no criminal history. I still have not received answers to these letters. Even more disappointing is that in many cases, my colleagues and I have had to rely on information released by press accounts, often addressing the same issues that the Department has failed to answer. It is inexcusable that the Department has failed to answer these letters. When can I expect answers?

#### Response:

DOJ responded to your letter of 1/10/03 by letter dated 6/8/04, and to your letter of 3/22/04 by letter dated 6/18/04.

41. It was recently reported that following the 9/11 attacks, the nation's largest airlines responded to a sweeping request from the FBI for as much as a year's worth of passenger records, including names, addresses, travel destinations and credit card numbers. The FBI's request was different from its typical requests to airlines, which usually concern passengers on single flights, or the travel patterns of individual passengers. At least one airline went so far as to set up extensive facilities for FBI agents in its headquarters. Reportedly, the FBI developed "a model of what these hijackers were doing" and then searched the passenger data for patterns, an activity which largely resembles a data-mining operation. But as an FBI official stated in the *New York Times*, "[t]here is no indication that the passenger data produced any significant evidence about the plot or the hijackers."

a. What privacy and security protections were employed in this search of individual airline data?

**Response:**

The purpose of this FBI project was to construct a time line reflecting the travel of the 19 9/11/01 hijackers leading up to the attacks. Subpoenas or official letters requesting records related to these hijackers were used as necessary, and some information was provided voluntarily by airlines (because the focus of the FBI's inquiry was on international flights, FBI investigators worked with both U.S. and non-U.S. airlines; non-U.S. airlines were less likely to require U.S. subpoenas). In some cases the FBI identified those sitting next to or in close proximity to one of the 19 hijackers to try to identify potential associates, but information concerning these passengers was not the focus of the initial request to the airlines.

The information obtained by the FBI was maintained in a secure area. When FBI personnel were not physically present, the information was maintained in a locked safe to which only FBI personnel had access.

**b. What type of models or criteria were used to search the records?**

**Response:**

Initially, available lists of passengers on Middle Eastern flights were collected and reviewed. This was done only to identify passengers who appeared on more than one flight with a hijacker. To expedite analysis, commonalities with the 9/11 hijackers were established, such as Middle Eastern males having dates of birth (when available) near those of the 9/11 hijackers. Seat assignments were also used as a guide because the hijackers mainly flew first class. No further review was conducted with respect to passengers who shared only one flight with a hijacker, since the project focused on identifying individuals who traveled more than once on the same flight as one of the 19 hijackers.

**c. Was this data ever merged with any other government database?**

**Response:**

The flight manifests were scanned into Intelplus and passenger names were entered into ACS. In addition, the Foreign Terrorist Tracking Task Force (FTTTF) was given a copy of the passenger/travel database.

**d. Did these searches lead to any investigations, arrests or prosecutions, and if so, where these actions based solely on the search results, and what were the results of those efforts?**

**Response:**

Out of a pool of over 6,000 passengers, the project identified 44 individuals believed to require further review, and several FBI Field Offices opened investigations on one or more of these individuals. However, as most of the travel records did not contain identifiers for these passengers, the Field Offices typically view these identifications as valuable only for name match purposes, with additional investigation being needed to match a subject with a passenger on a hijacker's flight. These investigations are ongoing. The names of these 44 individuals were forwarded to the CIA.

**e. Does the Department still have possession of this airline passenger data, and if so, for what purposes is it being used and what are the plans for the data?**

**Response:**

The passenger data is currently boxed, sealed, and ready to be inventoried as evidence. These boxes will be delivered to the FBI warehouse facility so that they will be available for possible use at the upcoming Moussaoui trial.

**42. Recent reports indicated that "a key selling point" for the Department in awarding funds to Seisint, Inc. for the MATRIX program was the company's data-mining technique -- the "high terrorism factor" scoring system, which incorporated factors like age, gender, ethnicity, credit history and information about pilot and driver licenses. Reportedly, this scoring system identified 120,000 terrorism suspects and led to investigations and arrests. In addition to answering my March 22 questions about MATRIX, its terrorism scoring system and use by DOJ in investigations, please also answer the following:**

**a. Reports indicate that the scoring factor is no longer in use in the MATRIX program. Please confirm whether the scoring factor or any other data mining technique is currently a part of the MATRIX program. If so, please describe those techniques (e.g. whether identification, link-analysis, or pattern analysis), the success of use, and any privacy, accuracy or security protections. If not, please indicate whether there are any plans to include the scoring factor or any other data mining technique in future uses of the MATRIX program.**

**Response:**

While the MATRIX program was not developed or managed by the FBI, those in DOJ who are knowledgeable regarding this program have advised as follows.

The Factual Analysis Criminal Threat Solution (FACTS) application used by MATRIX is not able to conduct pattern recognition or predictive analysis. Queries, which may be posed by law enforcement investigators or analysts, will

elicit only records matching the specific request. While a scoring factor called a "High Terrorism Factor" (HTF) was used for a limited time with respect to the 9/11/01 attacks, and proved successful in developing investigative leads in conjunction with the 9/11 investigation, this is the only investigation in which the HTF factor has been used and there are no plans to use it in MATRIX applications.

The HTF, or "terrorist quotient," was developed in the aftermath of the 9/11 attacks, when commonalities among the 19 hijackers were developed by Seisint's technicians, along with representatives from the FBI Miami Field Office, INS Miami Region, Secret Service Miami Office, Florida Department of Law Enforcement (FDLE) Miami Office, and U.S. Customs Miami Office. The HTF combined patterns and anomalies to identify individuals who shared characteristics and commonalities with these 19 hijackers. Once these individuals were identified, human investigative and analytical efforts were applied to determine whether any of them did, in fact, have any involvement in the 9/11 attacks or other terrorist activities. Without this human analytical intervention, application of the HTF would have had no investigative value.

The HTF capability was subsequently enhanced by combining commercially available data and state-contributed public information, resulting in an application called "Florida Crime Information Center - Plus" (FCIC+), so called because it was a single-query interface between the criminal history records maintained by the FCIC "plus" the Accurant public data maintained by Siesint, Inc. Access to the HTF tool within FCIC+ was "locked" by security software and strictly limited to four senior FDLE investigators/analysts, as well as a few Seisint technicians (whose access was to permit application development and testing).

The individuals identified through application of the HTF were not terrorist "suspects," but instead were individuals who had characteristics similar to the 19 hijackers. Only through further investigation of these individuals could any possible suspects be identified. Upon conclusion of this investigation, the investigative team disbanded and returned to their respective agencies, though the FDLE's representative remained on-site to work with Seisint technicians to develop an investigative tool that would combine and apply commercially available data, public information, and law enforcement data subject to limited dissemination (such as drivers' licenses and photos, vehicle registrations, criminal and corrections histories, and sexual offender data).

During this same time period, at least 15 states were involved in significant discussions on how better to share information and intelligence to prevent future terrorist attacks. Many of these states later became the originating participants in the MATRIX Pilot Project. The success of the FCIC+ application, including the HTF, was demonstrated to these states as an effective means of sharing data and

performing factual data analysis. The FCIC+ application was further enhanced, and evolved into the present FACTS application. After careful consideration by project participants, including consideration of security and privacy concerns, it was decided that the FACTS application, which was to be included in the MATRIX Pilot Project, would not contain the HTF functionality. This decision was made in the course of discussions as the project progressed and was not memorialized in the form of a memorandum or meeting minutes.

**b. 120,000 is a very large number of suspected terrorists, and if accurate, would suggest a substantial threat. How many of the 120,000 suspects were subject to further investigation, arrest or prosecution, and what were the results of those efforts? Were any of the 120,000 successfully prosecuted for terrorist activity?**

**Response:**

The list of 120,000 names was compiled and delivered to law enforcement before the MATRIX Pilot Project was initiated. As indicated in response to subpart a, above, Seisint created and provided a list of individuals (not "suspects") to an investigative team following 9/11/01. This team was not associated with the MATRIX project. Upon conclusion of the team's efforts, the members assigned to the team disbanded and returned to their respective agencies. Because investigations could have been conducted by any of the agencies participating on this team, it is unknown how many of these individuals were investigated.

**c. Was there a process for determining whether any of the 120,000 individuals should be removed from the list or cleared of any association with terrorism activity, and if so, what was that process and how many individuals were cleared?**

**Response:**

As indicated in response to subpart a, above, the purpose of compiling a list of individuals who shared commonalities with the 19 hijackers was as to determine whether any of these individuals were, in fact, associated with terrorism. The list was not considered or used as a list of "suspects."

**d. Were any of the 120,000 individuals included in the terrorist watch list compiled by the Terrorist Screening Center, and if so, how many?**

**Response:**

Mere inclusion on the list of 120,000 individuals, without the development of additional information through investigation, would be an inadequate basis for inclusion on the Terrorist Screen Center (TSC) watch list. Nominations for the inclusion of international terrorists are provided to the National Counterterrorism

Center (NCTC), which determines whether to forward the nomination request to the TSC. Records forwarded to the TSC by the NCTC are adjudicated by the TSC to determine whether they are appropriate for inclusion in the TSC database.

**43. Recently, the Technology and Privacy Advisory Committee, which was appointed by Secretary Rumsfeld, issued a report on data mining. That report stated "[W]e believe that there is a critical need for Congress to exercise appropriate oversight, especially given the fact that many of these data mining programs may involve classified information which would prevent their being disclosed in full publicly. At a minimum, we believe that each agency's privacy officer and agency head should report jointly to appropriate congressional committees at least annually on the agency's compliance with applicable privacy laws; the number and nature of data mining systems within the agency, the purposes for which they are use[d], and whether they are likely to contain individually identifiable information about U.S. persons; the number and general scope of agency findings authorizing data mining." Do you agree with this statement? If not, please explain to what extent you disagree and your reasons.**

**Response:**

This question refers to the March 2004 report of the Technology and Privacy Advisory Committee (TAPAC), entitled "Safeguarding Privacy in the Fight Against Terrorism."

While the FBI agrees that information on FBI privacy law compliance should be made available to Congress and the public, present reporting requirements ensure appropriate disclosure. DOJ's Management and Planning Staff (MPS) maintains DOJ's official Privacy Act inventory and manages the administrative processing of notices and rules, and the FBI periodically advises DOJ of the status of FBI compliance with privacy laws. Reporting requirements include biennial matching activity reports, reports on the establishment of new "systems of records," and reports with respect to the modification of a "system of records" when a new routine use or exemption is added or a system of records is otherwise altered. These reports are submitted to OMB and both houses of Congress. In addition, the E-Government Act of 2002 requires agencies to report annually to OMB on agency compliance with that Act.

The second and third recommendations (regarding reports on the number and nature of data mining systems within the agency and the purposes for which they are used) both concern data mining. The FBI is concerned that there is a lack of consensus regarding the definition of "data mining." The TAPAC report defines "data mining" as searches of one or more electronic databases of information concerning U.S. persons, by or on behalf of an agency or employee of the government. Under this definition, the second and third recommendations become nearly impossible to implement. If data mining is any search of an

electronic database, then "the number and nature of data mining systems," would include every system on a computer within the FBI, and encompass all searches of all databases. As a criminal investigative agency, the FBI conducts thousands of records searches a day, all of which are fully in compliance with the Privacy Act and other applicable privacy laws. Under these circumstances, providing a report on "the number and general scope of agency findings authorizing data mining" pursuant to this definition would be extremely burdensome, inhibiting the FBI's investigative functions in the absence of additional resources and staffing.<sup>1</sup> Even if such reporting could be accomplished, it appears that these reports may be so broad that they would not provide information helpful to Congress in exercising effective oversight.

In assessing the need for additional reports in this area, it is important to recognize that the development of any new system affording the FBI access to data in ways that were previously technologically unavailable requires a Privacy Impact Assessment (PIA) to ensure that the new system complies with all privacy laws. The FBI had established such a process well before the E-Government Act required it, and both that process and the subsequent PIA process assure compliance with applicable laws, regulations, and policies governing individual privacy and provide FBI officials with an assessment of a proposed system's impact on privacy. The PIA process includes a review of new or modified systems by FBI legal staff and the FBI Senior Privacy Official. If warranted, proposals are submitted to the FBI Privacy Council for review and comment. Through this process, both Privacy Act compliance and privacy policy issues are addressed. DOJ is currently developing standardized PIA procedures.

*The following 26 questions from Senator Leahy request additional information with respect to questions posed following the 7/23/03 oversight hearing, to which the FBI has previously responded.*

44. (Follow-up to Leahy 2) Have you completed the review of the manuscript submitted by SA Robert Wright for publication? If so, when, and has SA Wright been notified? Were portions of the manuscript determined to be "objectionable" and why?

**Response:**

As indicated in the FBI's earlier response, Mr. Wright submitted an amended "Fatal Betrayals" manuscript in February 2002, and this manuscript was provided

---

<sup>1</sup>The GAO Report entitled "Data Mining: Federal Efforts Cover a Wide Range of Uses," GAO-04-058, defines "data mining" as the application of database technology and techniques, such as statistical analysis and modeling, to uncover hidden patterns and subtle relationships in data and to infer rules that allow for the prediction of future results. This definition, while narrower, is still not specific enough to provide the necessary guidance as to which systems should be reported.

to the FBI's Chicago and Milwaukee Divisions and to the U.S. Attorneys' Offices for the Northern District of Illinois and the Eastern District for Wisconsin for review. In May 2002, the FBI advised Mr. Wright that the manuscript contained information regarding open investigations, matters occurring before a federal grand jury, sensitive law enforcement techniques, intelligence, and information otherwise prohibited from release, and that the manuscript, as drafted, could not be published.

In June 2002, Mr. Wright appealed the prepublication review decision to the Director of the FBI; that appeal was denied in July 2002. A November 2002 appeal by Mr. Wright to the Associate Deputy Attorney General was denied on procedural grounds (appeal to that level is available only based on the inclusion of classified information in the submission, and the amended transcript did not include such information). In October 2003, Mr. Wright was advised that a recent re-review of the manuscript had resulted in the determination that Chapters 1-4 and pages 103-16 and 119-22 of Chapter 7 could be published, but that the remainder of the transcript remained unapproved for publication.

**45. (Follow-up to Leahy 3B) Has FINCEN finished preparing rules regarding precious gems as required by the USA PATRIOT Act? What is the status of the rules? What is the reason for the delay in promulgating the rules?**

**Response:**

FinCEN, which is part of the Department of the Treasury, is in the best position to provide an update on the status of this matter.

**46. (Follow-up to Leahy 4) Based on your response, I understand that individuals who were not named recipients of the Phoenix EC could not query ACS using search terms and locate the document. Given that "two Agents on international terrorism squads in the New York Office" were "recipients," in that they were on the addressee line of the Phoenix EC, would they have been able to query ACS prior to September 11, 2001, using search terms and locate the EC? If so, how? Under the ACS system being used today, can all agents and analysts query ACS using search terms and locate any ECs containing that search term within the FBI? Will this capability be different under the Virtual Case File and if so, how?**

**Response:**

The search capabilities of the ACS system were explained to this Committee by letter dated 6/14/02. This issue was again addressed in response to your Question 3 posed to Director Mueller following the 6/2/02 Committee hearing. That response was transmitted to the Committee by letter from Assistant Attorney General Moschella dated 7/22/03. In addition, we reiterate our request that



members of the Committee visit FBI Headquarters for an online demonstration of our current search capabilities.

The Trilogy program will eliminate the need for complex ACS searches, permitting the use of simpler and more intuitive search functions, similar to those used with Internet search engines.

**47. (Follow-up to Leahy 6) Under 50 USC § 2655, the FBI and the Department of Energy are required to consult on regulations necessary to carry out the Counterintelligence Polygraph Program. By statute, those regulations shall include procedures for (1) identifying and addressing "false positive" results of polygraph examinations; and (2) ensuring that adverse personnel actions not be taken against an individual solely by reason of that individual's physiological reaction to a question in a polygraph examination, unless reasonable efforts are first made to independently determine through alternative means the veracity of that individual's response to that question. Have such regulations been drafted, promulgated or implemented?**

**Response:**

The Department of Energy regulations are published at 10 C.F.R. Part 709.

**48. (Follow-up to Leahy 6) You note two differences in the Grassley-Leahy FBI Reform Act and the FBI's current polygraph program. The first involves the class of persons subject to a polygraph; the second involves the need to administer random, five-year periodic and compelled polygraphs where appropriate. Can you propose specific language to address these differences, such that you could support this provision of the FBI Reform Act?**

**Response:**

As the FBI indicated in response to questions following the Director's 7/23/03 hearing, the population subject to polygraph is comprised of those with access to sensitive FBI information, and these polygraphs are administered, pursuant to established criteria and procedures, on a periodic basis, on an aperiodic (random) basis, and when necessary to resolve particular security concerns. The FBI has designed its polygraph program to protect both FBI information and those who have access to it, using the polygraph as one tool among many to ensure the continued trustworthiness of those using and disseminating sensitive FBI information. The FBI would be pleased to work with DOJ and Congress to develop language that meets the needs of the FBI in fulfilling its intelligence and law enforcement missions.

**49. (Follow-up to Leahy 7A) When did the FBI begin drafting the provision "currently under review" that "clearly prohibits an FBI agent from having any sexual relationship with a cooperating witness? Has the review process been completed and can I have a copy of the new policy? Would violations of this policy be deemed a "performance" issue or a "misconduct" issue?**

**Response:**

The FBI policy prohibiting inappropriate relationships between Agents and Confidential Informants (CIs) extends to the handling of all FBI human sources. In August 2003, a provision was drafted to clearly prohibit an FBI Agent from having any sexual relationship with a cooperating witness (CW). This provision was approved for inclusion in existing policy in November 2003, and was subsequently published in the Manual of Investigative Operations and Guidelines, Part 1, Section 270-4(12)(a). This provision states: "While an Agent is permitted to socialize with a CW to the extent necessary and appropriate for operational reasons, the Agent is never permitted to engage in an intimate and/or sexual or unduly familiar social relationship with a CW." Violation of this policy would be handled as a "misconduct" issue.

**50. (Follow-up to Leahy 7C) Did any FBI employee report any suspicions with respect to Agent Smith's relationship with Katrina Leung and, if so, how was such report handled?**

**Response:**

No suspicions of a possible relationship between SA Smith and Ms. Leung were reported to the FBI's Office of Professional Responsibility, which is responsible for addressing allegations of employee criminality and misconduct.

**51. (Follow-up to Leahy 10) How many full-time agents were assigned to civil rights investigations through the end of FY 2003 and how many have been assigned to date in FY 2004? Given that there were at least "the equivalent of" 74 fewer full-time agents in FY 2003 working civil rights than there were in FY 1999, what happened to open civil rights investigations that the 74 agents were working when reassigned? How many cases have been declined because no agents or analysts were available to work them?**

**Response:**

In FY 2003, the equivalent of approximately 114 full-time Agents were assigned to civil rights investigations. Through the end of March 2004, the number of full-time Agents working civil rights matters rose to just over 120.

Although there has been a decrease in the number of full-time Agents working civil rights matters since a high of 190 in FY 1999, all civil rights investigations

continue to be investigated aggressively and thoroughly. If an Agent who is assigned to investigate civil rights matters is reassigned to another investigative program or otherwise leaves the FBI through resignation or retirement, the Agent's civil rights cases are reassigned to another Agent, who will be responsible for those cases until all investigative leads are exhausted. Every civil rights investigation is forwarded from the field to the Civil Rights Unit (CRU) for review with respect to completeness, among other things. In addition, the Criminal Section of DOJ's Civil Rights Division and the local United States Attorney's Office (USAO) receive copies of civil rights investigations, and either office can request additional investigation.

The CRU is aware of no instance in which the FBI declined to investigate a civil rights complaint due to the unavailability of civil rights personnel. Any civil rights complaint that appears on its face to be a violation of a federal civil rights statute is opened and investigated thoroughly.

**52. (Follow-up to Leahy 11) Based on the summaries you provided, the FBI successfully concluded 41 civil rights cases in FY 2002 through the 3<sup>rd</sup> quarter of FY 2003 as the "lead investigative agency." Of those, approximately 20 appeared to fall under your definition of a "hate crime"; 15 were "color of law", 2 were "freedom of access," and 4 were "involuntary servitude and slavery" cases. I appreciate that these are complex, difficult cases, but these low numbers concern me, particularly because the number of agents working these time-intensive investigations is rapidly declining. Given the importance of these cases, which State and local authorities often cannot handle or have requested Federal assistance in handling, what recommendations do you have to ensure that the FBI continues to dedicate good agents and analysts to these prosecutions?**

**Response:**

Any civil rights complaint that appears on its face to be a violation of federal criminal law must be opened and investigated. The results of civil rights investigations are submitted to DOJ and the USAO for a prosecutorial opinion. It is the prosecutor's responsibility to decide whether the case merits prosecution. The premise of the question, that the number of Agents working civil rights investigations is rapidly declining, is not accurate. While there was a dramatic decrease immediately following the events of 9/11/01, these numbers are beginning to increase. In addition, the Civil Rights Program (CRP) is among the FBI's top 10 priorities; and appropriate resources have been allocated to the program. It is the responsibility of each field division's Special Agent in Charge (SAC) to ensure that these resources are employed according to the FBI's and the field division's priorities. At least three in-service training sessions are conducted by the CRU annually to ensure that all those working civil rights matters receive adequate training. When needed, additional training is provided.

53. (Follow-up to Leahy 11) It appears that of the two freedom of access to clinics matters, one was instituted by the prior Administration. Thus, there has been only one freedom of access prosecution since President Bush took office. How many reports alleging possible violations of FACE were received in this time frame, and how many investigations were referred for prosecution? What is the status of the government appeal in U.S. v. Bird?

**Response:**

The below chart reflects the number of Freedom of Access to Clinic Entrances (FACE) Act investigations the FBI has initiated and the number of federal indictments, arrests, and convictions obtained beginning in FY 2001.

FY	FACE Cases Initiated	Federal Indictments	Federal Arrests	Federal Convictions
2001	42	0	0	1
2002	23	0	1	1
2003	20	2	1	1
2004 (thru end of 2d qtr)	9	0	0	0

As reflected by the steady decline in case initiations, traditional FACE Act incidents (such as telephone threats and vandalism) have declined since their peak in the 1990s. While this decline has been observed by both law enforcement and non-governmental organizations (NGOs) alike, matters that fall within the FACE subprogram often overlap with other FBI programs and are classified with those programs. For example, FACE investigations involving bio-terrorism threats to reproductive health care facilities (such as letters threatening to contain anthrax) previously investigated as FACE Act violations are now opened as terrorism matters. Similarly, a bombing at a reproductive health care facility where organized hate groups are believed to be involved may be classified as a domestic terrorism matter.

As indicated above, civil rights investigations are subject to a greater level of routine outside scrutiny than most investigations; unlike other FBI criminal programs, the results of all civil rights investigations, to include FACE matters, are provided to DOJ and the local USAO for review.

The case of United States v. Bird arises from an incident on 3/7/03, when Bird drove a vehicle into the entrance of a Planned Parenthood building in Houston, Texas. In August 2003, a United States District Court ruled that the Commerce Clause of the FACE Act, under which Bird was indicted, was unconstitutional.

DOJ has appealed this ruling to the 5th Circuit Court of Appeals, and briefs have been filed. A hearing date has not yet been set.

**54. (Follow-up to Leahy 11) Based on the summaries you provided, it appears that only 9 prosecutions involving the FBI as the lead investigative agency were hate crimes directly related to the events of September 11, 2001. Is that correct? How many complaints did the FBI receive following September 11, 2001, that involved possible violations in the "Hate Crime" category of cases you described?**

**Response:**

As indicated above, any civil rights complaint that appears on its face to be a violation of federal civil rights law is opened and investigated thoroughly. While the FBI maintains statistics on hate crimes, it does not maintain statistics on the number of civil rights complaints received, and the specific number of hate crimes apparently committed in retaliation for the attacks of 9/11/01 is unknown. Between 9/11/01 and June of 2004, approximately 531 hate crime investigations were initiated in which it appeared that Arabs, Muslims, or Sikhs were targeted. Because there may be a delay between the filing of an allegation (particularly when it is lodged with an entity outside the FBI), the initiation of the investigation in the field, and the field's report to FBIHQ, this number may not be a true reflection of the total number of such cases. Of the reported 531 investigations, 13 cases resulted in 18 subjects being charged federally, and another 178 subjects were charged on the local level. Because these cases are typically worked jointly between local law enforcement officials and the FBI, local prosecutions often proceed before federal cases are brought. In cases in which the federal interest has been satisfied by a successful local prosecution, the federal government may choose not to pursue an additional conviction. The federal prosecutor's decision not to proceed with a prosecution in no way reflects on the quality of the FBI's investigation.

**55. (Follow-up to Leahy 15) What specific policy changes have you made in response to the Inspector General's report on 9/11 detainees?**

**Response:**

DOJ and DHS have signed an MOU relating to information sharing, and the FBI is working with others in DOJ to draft an MOU governing the detention of aliens of interest to the FBI. In addition, DOJ is working with DHS to draft an MOU establishing criteria and procedures for future investigations of alien detainees of national security interest. The FBI has also worked to establish the Terrorist Screening Center (TSC) and to assist in establishment of TTIC, which will substantially improve the FBI's ability to obtain information about alien detainees from various agencies and to process this information in a timely fashion. The

FBI continues to work with the National Security Law Division of DHS Immigration and Customs Enforcement (ICE) to review alien detainee cases of national security interest on a case-by-case basis.

**56. (Follow-up to Leahy 16C) Has a final decision been made as to whether prior approval is mandatory for visiting a public place or attending a public event to detect or prevent terrorist activity?**

**Response:**

The policy regarding attendance at public events and places is articulated in Part VI of the revised Attorney General's Guidelines on General Crimes, Racketeering Enterprise, and Terrorism Enterprise Investigations (General Crimes Guidelines). In implementing this guidance, FBI policy provides that a supervisor's approval is recommended but not required. There are no current plans to change this policy, because there has been no indication that the authority has been misused or that greater oversight is needed for any other reason. Should these circumstances change, the need for greater oversight will be re-evaluated.

Part VI of the General Crimes Guidelines is only one of several authorities governing attendance at public events or visitation of public places. Agents may also engage in these activities as part of a full field investigation or a preliminary inquiry under the General Crimes Guidelines or appropriate provisions of the Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection. (NSIG). Since internal FBI policy requires that international terrorism investigations be conducted pursuant to the NSIG, attendance at public places and events to detect or prevent international terrorism would typically be authorized under those guidelines.

**57. (Follow-up to Leahy 17) Why didn't the FBI participate in the review of the 4,500 intelligence files? To your knowledge, did the FBI receive any referrals from DOJ based on this review? If so, please provide details to the extent possible (without jeopardizing a current investigation).**

**Response:**

The review of intelligence files was undertaken at the direction of the Attorney General specifically to enable criminal prosecutors to identify and evaluate information in intelligence files which prosecutors found appropriate for criminal investigation. These files had been developed by FBI agents, many of whom had been involved only in intelligence investigations and had no experience in criminal investigations. Turning a prosecutor's eye on this information was the precise purpose of this review. The FBI fully cooperated with this review, making files available and responding to questions as needed. Following this

review, the FBI, working in conjunction with prosecutors, conducted further investigation where appropriate with an eye to developing criminal cases. More than 500 criminal investigations were initiated following the file review, some of which have resulted in prosecutions.

**58. (Follow-up to Leahy 18A) When will the FISA Management System (FISAMS) be fully operational? With whom is the contract for development of FISAMS? How much will it cost and what funds are being used to pay for it?**

**Response:**

The FISA Management System (FISAMS) became operational at the end of January 2004. The FBI has trained the largest 13 FBI field offices on the system. These 13 offices are currently processing their FISA requests, which account for approximately 75% of FBI FISAs, through the FISAMS. The remaining FBI field offices are in the process of being trained, and all FBI offices will be operational in the FISAMS by the end of CY 2004.

High Performance Technologies, Inc. (HPTi) is the contractor responsible for development of the FISAMS. The FBI allocated \$900,000 for Version 1.0 of the FISAMS in FY 2003, and is contracting with HPTi for an additional \$1 million in enhancements, funded by the Wartime Supplemental appropriation, beginning in the fall of 2004. While several follow-up versions are anticipated to further enhance FISAMS in the future, FY 2006 is the first budget cycle in which targeted funding for this project has been requested.

**59. (Follow-up to Leahy 18C) Did you personally review the 4 FISA applications reportedly not approved by the FISA court last year? Can you provide any details on why the 4 applications were not approved?**

**Response:**

The Director of the FBI personally certifies each FISA application submitted to him. Details about the four applications were provided in the Department's highly classified, statutorily mandated semi-annual report on the FISA process, "The Attorney General's Report on Electronic Surveillance and Physical Search under the Foreign Intelligence Surveillance Act," for the reporting period in which those applications were presented to the Foreign Intelligence Surveillance Court. That report was filed with the Senate Select Committee on Intelligence and access to it by other appropriately cleared Senate staff may be obtained in coordination with that committee.

**60. (Follow-up to Leahy 18D) Can you provide us with a blank copy of the FISA Request Form referenced in your response? Will you provide us with a blank copy of the form that the FBI created for requesting business records from the FISA court?**

**Response:**

This response is classified and is, therefore, provided separately.

**61. (Follow-up to Leahy 21) Did you refer the question to DOJ OIPR? When? Have you been asked to assist in the response? When?**

**Response:**

The FBI forwarded its response to Senator Leahy's question 21 to DOJ on 10/22/03, indicating that the question called for classified information that is ordinarily supplied to Congress by DOJ's Office of Intelligence Policy and Review (OIPR). By letter to the Committee dated 3/4/04, DOJ's Office of Legislative Affairs forwarded the responses to the Committee, which included the FBI's original response to this question in which the FBI deferred to OIPR as the more appropriate component to whom the Committee should direct such questions.

**62. (Follow-up to Leahy 22) Can you provide a copy of the "collection baseline that defines the sum total of resources the FBI can bring to bear on a given threat" when it is completed (estimated mid-November 2004?) to respond to the "connect the dots" issue? Have you yet identified gaps in your knowledge about threats? How can Congress help to ensure there are no such gaps?**

**Response:**

The collection baseline is a large database and, consequently, providing a copy is problematic. In addition, the baseline tool, data, and the reports that can be generated cannot be fully understood without contextual knowledge. The FBI would be pleased to provide a classified briefing and demonstration of the baseline.

The FBI's collection baseline tool allows us to "know what we could know," and the work to identify what we don't know (i.e., the work to identify gaps) continues. Once gaps are identified, the FBI develops collection strategies to fill those gaps through a variety of intelligence collection methods. There will always be gaps in any intelligence organization's knowledge about threats. The key to the FBI's success is the creation of an independent entity, the Intelligence Requirements and Collection Management Unit, that focuses full time on identifying gaps and developing strategies for filling them. The FBI understands



its responsibility to ensure customers and stakeholders are aware of collection gaps and are confident in the FBI's plans to fill them, and we would be pleased to provide Congress with classified briefings on the status of FBI intelligence collection capabilities.

The FBI appreciates the support Congress has demonstrated by providing resources and legislation to strengthen the FBI's ability to protect the American public and U.S. interests around the world. We would appreciate your continued support with respect to our plans for a robust intelligence capability in the FBI, especially in the areas of Intelligence Analyst staffing and retention; intelligence training; and information technology support for our intelligence activities, including the infrastructure improvements needed to support secure information networks.

**63. (Follow-up to Leahy 31) Is TTIC the "one place" where all terrorism-related information is brought together? How is such information disseminated (e.g. through email, a website, faxes, telexes, etc.)?**

**Response:**

The NCTC (formerly TTIC) serves as the organization in the U.S. Government (USG) primarily responsible for analyzing intelligence pertaining to terrorism that is possessed or acquired by the USG (except purely domestic terrorism). Although the NCTC has primary responsibility for terrorism threat analysis, a number of organizations throughout the federal government have been assigned responsibilities with respect to terrorism information by statute, Presidential Directive, regulation, and policy. These include primarily the CIA, FBI, and DHS. In addition, the Departments of State, Defense, Treasury, and numerous others analyze the terrorist threat from their particular perspectives.

Among other means, the NCTC's terrorism threat analysis is disseminated by the FBI, DHS, and other federal officials assigned to this interagency organization, who push threat information out to state and local officials and law enforcement personnel through the JTTFs, state emergency management agencies, and other organizations operating at the state and local level. In addition, NCTC uses production and dissemination mechanisms that are commonly employed in the federal government based on customer needs and their communication technology capabilities, including classified and unclassified faxes, hard copy dissemination, and cables. Because NCTC is mindful of the need to produce intelligence information at the lowest possible classification level in order to ensure that it reaches the widest possible audience, it frequently prepares reports on a given subject at multiple classification levels. This ensures that the dissemination of important information is not delayed by the need to declassify intelligence.

Additional information responsive to this question is classified and is, therefore, provided separately.

**64. (Follow-up to Leahy 32) Please answer the question asked: Were there other instances directly or indirectly connected with the September 11 attacks where, because of the "perception" within the FBI that the "FISA process was lengthy and fraught with peril," investigative avenues were not pursued? Please describe any such instance where FISA was considered but not used.**

**Response:**

The FBI is aware of no instances directly or indirectly connected with the 9/11 attacks in which a FISA was considered but not pursued because of the nature of the FISA process.

**65. (Follow-up to Leahy 33) What financial support networks have been "closed down" using the PATRIOT Act? Please describe your efforts and results in detail.**

**Response:**

The USA PATRIOT Act has provided the means to disrupt terrorist financial support networks. The FBI has used the USA PATRIOT Act to pursue several significant investigations throughout the U.S. Given the global nature of financial support networks, the actual "closure" of a financial support network can only be achieved with complete international cooperation. Through the United Nations' designation process, which triggers international obligations on the part of all member countries with regard to individuals and entities associated with the Taliban, Usama bin Laden, or al Qaeda, several corrupt nongovernmental organizations (NGOs), such as charities ostensibly operating to provide humanitarian aid, have been blocked from transmitting or receiving money, goods, services, or other material support. The designation process requires member nations to take affirmative steps to ensure that designated organizations and individuals cannot use their remaining infrastructure or finances to fund or otherwise support terrorism. The public identification of terrorists, terrorist organizations, and terrorist supporters assists in terminating their activities, since this prohibits other entities from having dealings with them.

These blocking actions are critical to combating the financing of terrorism. When a blocking action is put into place, any property -- including assets -- that exists in the U.S. is frozen, and U.S. persons and persons within the jurisdiction of the United States are prohibited from transacting or dealing with individuals and entities who are the subject of the blocking action. Blocking actions serve additional functions as well, including serving as a deterrent for nondesignated parties who might otherwise be willing to finance terrorist activity; exposing

terrorist financing "money trails" that may generate leads to previously unknown terrorist cells and financiers; disrupting terrorist financing networks by encouraging designated terrorist supporters to disassociate themselves from terrorist activity and renounce their affiliation with terrorist groups; terminating terrorist cash flows by shutting down the pipelines used to move terrorist related assets; forcing terrorists to use alternative, more costly, and riskier means of financing their activities; and engendering international cooperation and compliance with obligations under U.N. Security Council Resolutions. To date, the United States and our international partners have designated 368 individuals and organizations as terrorists and terrorist supporters and have frozen approximately \$139 million and seized more than \$60 million in terrorist related assets.

A notable disruption of an NGO using the USA PATRIOT Act's material support statutes was effected through the investigation of the United States office of the Benevolence International Foundation (BIF) in Chicago, Illinois. The chairman of BIF ultimately pled guilty to a lesser charge and the BIF office closed.

Also of note is the series of actions taken against the umbrella charities of the Al-Haramain Foundation (AHF). Before the removal of the Taliban from power in Afghanistan, the AHF in Pakistan supported the Taliban and other fundamentalist groups. AHF was linked to the UBL-financed terrorist organization, Maktab al Khidemat (MK). On one occasion in 2000, MK directed the deposit of funds in AHF accounts in Pakistan and, from there, the transfer of these funds to other accounts. At least two former AHF employees who worked in Pakistan are suspected of having al Qaeda ties. One AHF employee in Pakistan is detained at Guantanamo Bay on suspicion of financing al Qaeda operations. Another former AHF employee in Islamabad was identified as an alleged al Qaeda member who reportedly planned to carry out several devastating terrorist operations in the United States.

A search warrant was executed in 2004 at the United States branch of the AHF in Ashland, Oregon. The search was led by Agents of the Internal Revenue Service Criminal Investigations section as part of a joint FBI/DHS (ICE) investigation into possible violations of the Internal Revenue Code, the Money Laundering Control Act, and the Bank Secrecy Act. The suspected crimes relate to possible violations of the currency reporting and tax return laws by two officers of the Ashland, Oregon, office of AHF. In a separate administrative action, based in large part on a JTTF investigation, the Department of Treasury Office of Foreign Assets Control (OFAC) blocked AHF accounts to ensure the preservation of its assets pending further OFAC investigation.

In March 2002, the Department of Treasury and the Kingdom of Saudi Arabia jointly designated the Bosnian and Somalian Branches of AHF as supporters of

terrorism. In December 2003, the reconstituted branch of AHF in Bosnia, now called Vazir, was also designated by both governments as a supporter of terrorism. In January 2004 these two governments also jointly designated AHF branches in four additional countries as being supporters of terrorism: Indonesia, Tanzania, Kenya, and Pakistan. The United Nations has adopted these AHF designations and imposed asset freezes, travel bans, and arms embargoes pursuant to United Nations Security Council Resolutions.

The AHF activities resulting in these sanctions took place under the control of Aqeel Abdulaziz Al Aqil, the founder and longtime leader of AHF and a suspected al Qaeda supporter. Al Aqil has been identified as AHF's Chairman, Director General, and President by a variety of sources and reports. Having been under investigation since late 2003, by March 2004 Al Aqil was reportedly no longer leading AHF activities. Under Al Aqil's leadership, numerous AHF field offices and representatives operating throughout Africa, Asia, Europe, and North America appear to have provided financial and material support to the al Qaeda network. Terrorist organizations designated by the U.S., including Jemmah Islamiya, Al Ittihad Al Islamiya, Egyptian Islamic Jihad, HAMAS, and Lashkar E Taibah, have received funding from AHF and have used AHF as a front for fund raising and operational activities. AHF has offices and representatives in more than 50 countries and includes nine general committees and several other "active committees," including the Continuous Charity Committee, African Committee, Asian Committee, Da'wah and Sponsorship Committee, Masjid Committee, Seasonal Projects Committee, Doctor's Committee, European Committee, Internet and the American Committee, the Domestic Committee, Zakaat Committee, and the Worldwide Revenue Promotion Committee. On 6/3/04 the USG announced the joint Saudi-U.S. designation of five AHF offices: Afghanistan, Albania, Bangladesh, Ethiopia, and the Netherlands. The USG independently designated Al-Aqil, the former head of AHF operations in Saudi Arabia.

In addition, the USG has designated other NGOs which support terrorist-related activities, including:

Makhtab al Khidamat/Al Kifah (formerly based in the U.S.)  
Al Rashid Trust (Pakistan)  
Wafa Humanitarian Organization (Pakistan, Saudi Arabia, Kuwait, and UAE)  
Rabita Trust (Pakistan)  
The Holy Land Foundation for Relief and Development (U.S.)  
Ummah Tamer E Nau (Pakistan)  
Revival of Islamic Heritage Society (Kuwait, Afghanistan, and Pakistan)  
Afghan Support Committee (Pakistan)  
Aid Organization of the Ulema (Pakistan)  
Global Relief Foundation (U.S.)

Benevolence International Foundation (U.S.)  
Benevolence International Fund (Canada)  
Bosanska Idealna Futura (Bosnia)  
Lajnat al Daawa al Islamiyya (Kuwait)  
Stichting Benevolence International Nederland (Netherlands)  
Al Aqsa Foundation (U.S., Europe, Pakistan, Yemen, and South Africa)  
Comité de Bienfaisance et de Secours aux Palestiniens (France)  
Association de Secours Palestinien (Switzerland)  
Interpal (UK)  
Palestinian Association in Austria (Austria)  
Sanibil Association for Relief and Development (Lebanon)  
Al Akhtar Trust (Pakistan)  
Islamic African Relief Agency (U.S., Sudan)

**66. (Follow-up to Leahy 34B) Has the FBI implemented any new professional rules of conduct or code of ethics policies that provide safeguards against FBI abuse of its PATRIOT Act authorities? What, if any, internal or disciplinary punishments are in place for abuses by employees?**

**Response:**

The FBI's existing rules of professional conduct, which require Agents to uphold the Constitution and to adhere to the highest standards of personal and professional behavior, safeguard against the abuse of USA PATRIOT Act provisions. For the most part, the USA PATRIOT Act provisions relevant to the FBI's mission amend existing federal investigative processes (e.g., search warrants) for which there is, in varying degrees, oversight by the executive, judicial, or legislative branches of government, or a combination thereof. For example, most FBI activities pursuant to FISA require approval by the DOJ Office of Intelligence Policy and Review and the FISA Court. Similarly, delayed notice search warrants and search warrants for voice mail must be approved by a U.S. District Court. As another example, requests for bank account information under Section 314 of the USA PATRIOT Act require approval by the Treasury Department's Financial Crimes Enforcement Network (FinCEN). Other provisions, such as Section 215, require annual reports to the Congress. In addition to these checks on abuse, information sharing must be conducted in compliance with the Privacy Act of 1974 and with various internal policies that ensure Privacy Act compliance, such as those promulgated by the FBI's Privacy Council. For example, the Privacy Act prohibits the collection and maintenance of record information about individuals based solely on the exercise of their First Amendment rights. In sum, there is already in place a network of checks and balances which will operate to guard against abuse and, if abuse does occur, to detect and correct it.

If abuse should occur, it would be addressed through the FBI's disciplinary process, which is overseen by the FBI's Office of Professional Responsibility (OPR) and the DOJ OIG. The OPR/OIG process aggressively and impartially addresses allegations of employee misconduct, including alleged violations of individuals' Constitutional or statutory rights, ensuring that the FBI maintains its integrity and professionalism. In addition, each FBI field office is inspected every three years for compliance with rules and regulations by the Inspection Division.

The FBI also ensures that Agents are trained to respect the Constitutional rights of individuals through extensive instruction on Constitutional law and criminal procedure and guidance on the importance of sensitivity to other cultures. As part of this training, new Agents also visit the Holocaust Museum so that they can see, graphically, what can occur when law enforcement becomes a tool for oppression.

**67. (Follow-up to Leahy 35) Have you seen an "increase" in global computer hacking activities in either the United States or Iraq because of growing tensions between the two countries? Please explain your answer.**

**Response:**

The FBI is unable to attribute any change in global computer hacking activities to the relationship between the United States and Iraq.

**68. (Follow-up to Leahy 36) Will you provide a response to Leahy 36 in a classified document and submit it for review by appropriate staff? Why did you not just submit the response in classified form as you have done on other occasions?**

**Response:**

The FBI was not directed to develop the referenced guidelines and defers to the Administration with respect to the existence or status of such guidelines.

**69. (Follow-up to Leahy 37) Please provide details on the "successful disruptions" of al Qaeda financing operations that have been accomplished? Have there been any indictments brought, informations filed, or convictions obtained as a result of the Joint Saudi Financial Investigative Unit? Please explain your answer.**

**Response:**

The joint USG-Saudi task force, known as the Joint Task Force on Terrorist Finance (JTFTF), has been in operation for less than a year. Information obtained thus far has been folded into several other CT and criminal investigations which

have yet to reach the indictment stage. Valuable information continues to be exchanged with respect to CT matters and classified intelligence investigations.

### Questions Posed by Senator Kennedy

70. On May 13, 2004, the *New York Times* reported that the Central Intelligence Agency has used a variety of coercive intelligence methods, including a technique known as "water boarding," against certain terrorist suspects. It stated that these rules for interrogation have been endorsed by the Justice Department and the C.I.A. The *Times* further reported: "The methods employed by the C.I.A. are so severe that senior officials of the Federal Bureau of Investigation have directed its agents to stay out of many of the interviews of the high-level detainees, counterterrorism officials said. The F.B.I. officials have advised the bureau's director, Robert S. Mueller III, that the interrogation techniques, which would be prohibited in criminal cases, could compromise their agents in future criminal cases, the counterterrorism officials said."

a. Please provide a copy of these rules for interrogation.

b. Who at the Justice Department approved these rules of interrogation?

Please provide all documentation pertaining to their proposal, consideration, and approval.

#### Response to a and b:

The FBI defers to DOJ with respect to these questions.

c. Which officials at the FBI told you about the rules of interrogation, and who informed you that they might compromise your efforts to prosecute suspected terrorists? Did these officials or any other official at the Justice Department provide an opinion as to the legality of these methods? Please provide a copy of every legal opinion you have received on this issue.

d. The *New York Times* reported that one set of legal memorandums prepared by the C.I.A. and the Justice Department "advises government officials that if they are contemplating procedures that may put them in violation of American statutes that prohibit torture, degrading treatment or the Geneva Conventions, they will not be responsible if it can be argued that the detainees are formally in the custody of another country." Are you familiar with this legal opinion? Do you agree with it? Has the FBI participated in any effort to place a detainee in the arguable "formal custody" of another country so that more severe interrogation methods may be used?

#### Response to c and d:

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



e. Since 9/11, there have been multiple reports about detainees in the custody of U.S. military or intelligence officials being transferred for interrogation to governments that routinely torture prisoners. A December 2002 article in the *Washington Post* reported that detainees who refuse to cooperate with American interrogators have been "rendered" to foreign intelligence services known to practice torture. The Convention Against Torture – to which the United States is a party – provides that "No State Party shall expel, return or extradite a person to another State where there are substantial grounds for believing he would be in danger of being subjected to torture." Can you assure the Committee that the FBI has fully complied with this legal requirement and not participated in any way in any "renditions" of detainees to countries known to practice torture?

Response:

Consistent with Article 3 of the Convention Against Torture as ratified by the United States, the FBI has not transferred custody of any detainee to a country where it is more likely than not that the detainee would be subject to torture.

71. Last year the Attorney General announced that information regarding more than 400,000 persons with removal orders and an unknown number of alleged NSEERS violators would be included in the NCIC database. As you know, these are cases of persons with administrative warrants, not criminal warrants. What is the legal authority for the FBI to enter administrative warrants into its principal criminal law database? What other immigration-related records does the Administration plan to include in NCIC? Are there any restrictions regarding the type of cases that can be entered into NCIC?

Response:

The authority of the Attorney General to acquire, collect, classify, and preserve identification, criminal identification, crime, and other records is provided by 28 U.S.C. 534. Pursuant to this authority, which is exercised within DOJ by the FBI, many of these records are obtained from state and local criminal justice agencies and managed by the FBI, which serves as the national focal point and central repository for criminal justice information records. In addition, 8 U.S.C. 1252c(a) provides that "[s]tate and local law enforcement officials are authorized to arrest and detain an individual who - (1) is an alien illegally present in the United States; and (2) has previously been convicted of a felony in the United States and deported or left the United States after such conviction, but only after the State or local law enforcement officials obtain appropriate confirmation from the Immigration and Naturalization Service of the status of such individual and only for such period of time as may be required for the Service to take the individual into Federal custody for purposes of deporting or removing the alien from the United States."

8 U.S.C. 1252c(b) requires that the Attorney General "cooperate with the States to assure that information in the control of the Attorney General, including information in the National Crime Information Center, that would assist State and local law enforcement officials in carrying out duties under subsection (a) of this section is made available to such officials." In satisfaction of this requirement, and under the authority afforded by 28 U.S.C. 534, the Attorney General promulgated 28 Code of Federal Regulations (C.F.R.), Part 20. 28 C.F.R. 20.32 defines the offenses includable in criminal history records as follows.

(a) Criminal history record information maintained in the III System and the FIRS [Fingerprint Identification Records Systems] shall include serious and/or significant adult and juvenile offenses.

(b) The FIRS excludes arrests and court actions concerning nonserious offenses, e.g., drunkenness, vagrancy, disturbing the peace, curfew violation, loitering, false fire alarm, non-specific charges of suspicion or investigation, and traffic violations (except data will be included on arrests for vehicular manslaughter, driving under the influence of drugs or liquor, and hit and run), when unaccompanied by a § 20.32(a) offense. These exclusions may not be applicable to criminal history records maintained in state criminal history record repositories, including those states participating in the NFF.

(c) The exclusions enumerated above shall not apply to federal manual criminal history record information collected, maintained, and compiled by the FBI prior to the effective date of this subpart.

In December 2003, the FBI's Criminal Justice Information Services Division (CJIS) Advisory Policy Board (APB) considered the inclusion of Student and Exchange Visitors Information System violators and non-felony deported aliens in the NCIC Immigration Violator File (IVF). Although the addition of these two categories of information was approved in concept, implementation must be delayed until:

- These actions are supported by criminal warrants;
- This change is directed by appropriate authority; or
- These actions can be documented in an "information only" file with acceptable caveats.

This is the only proposed addition of which the FBI is aware.

**72. The error rate in immigration records has always been very high. Numerous reports by the Inspector General of DOJ have confirmed the unreliability of INS records. What precautions are being taken to ensure that the immigration records being put into NCIC are accurate so that persons with legal status are not falsely arrested as a result of an inaccurate entry? What mechanism exists for updating and correcting information in the NCIC database?**

**Response:**

The primary responsibility for the entry and maintenance of accurate, timely, and complete records lies with the entering agency. A record may be modified only by the agency that entered the record. ICE's Law Enforcement Support Center (LESC) is the only entity that can enter records into the NCIC IVF, and it must comply with all NCIC policies. The following information, provided by ICE, describes the steps ICE takes to comply with NCIC policies.

NCIC policies require that every record entered be based on a valid original source document. For deported felons, that document is an executed warrant of removal; for alien absconders it is a warrant of removal; and for National Security Entry-Exit Registration System violators it is an administrative warrant of arrest. NCIC policies require that hit confirmation be conducted 24 hours a day, seven days a week, and within ten minutes. To meet the ten minute response time requirement, the LESL maintains fingerprints and photographs, as well as the original documentation to support a record's entry in the NCIC IVF.

The LESL reviews each alien file to determine if a record should be entered in one of the IVF categories. These reviews involve comprehensive research of the source documents and electronic data contained in the separate ICE databases to ensure data integrity and suitability for an NCIC entry.

Additionally, validation procedures exist to ensure that accurate records are entered into NCIC. Validation obliges the LESL to confirm that the record is complete, accurate, and still outstanding or active. IVF records must be validated 60 to 90 days after entry and every year thereafter. Validation is accomplished by reviewing the original entry and current supporting documents.

As the manager of NCIC, the FBI helps maintain the integrity of the system through: 1) automatic computer edits which reject certain common types of errors in data, 2) automatic purging of records after they are in a file for a prescribed period of time, 3) quality control checks by the FBI's Data Integrity staff, and 4) periodically furnishing lists of all records on file for validation by the agencies that entered them.

Each federal and state CJIS System Agency is audited at least once every three years by the FBI's audit staff. This audit includes a sample of state and local criminal justice agencies and their records. The objective of this audit is to verify adherence to FBI policies and regulations, and is termed a compliance audit. The FBI audit staff also conducted an informational NCIC audit of LESC in August 2003. Since the LESC acquired sole responsibility over the entry and maintenance of the NCIC IVF, there has been an improvement in the validity, accuracy, and completeness of both the records and the supporting documentation.

**73. The CLEAR Act would require that records of minor immigration violators be included in NCIC. This bill is opposed by many law enforcement agencies around the country. This particular provision in the bill was soundly criticized last month by the conservative Heritage Foundation, which stated that this mandate "may hinder law enforcement by undermining the usefulness" of the NCIC database. The report further states: "Filling the database with records of minor immigration violators could also distract or impede police officers from using the database to obtain information about violent criminals and terrorists." The report concludes that "NCIC should be reserved for serious, significant immigration violations." What is your view of the conclusions reached by the Heritage Foundation? Can we afford to jeopardize the integrity of the NCIC database?**

**Response:**

The main issue of concern for the law enforcement community, as voiced through the CJIS APB, has been the authority to arrest immigration violators. The law enforcement community does not want to retrieve records from NCIC with respect to individuals on whom they can take no action. The inclusion of immigration violators in NCIC and local law enforcement's right of arrest are currently the basis of a lawsuit filed by the American Civil Liberties Union.

**74. In June 2003, Glenn Fine, the Inspector General for the Justice Department, found "significant problems in the way the detainees were handled" following 9/11. These problems included a failure by the FBI to distinguish between detainees whom it suspected of having a connection to terrorism and detainees with no connection to terrorism; the inhumane treatment of the detainees at a federal detention center in Brooklyn; and the unnecessarily prolonged detention resulting from the Department's "hold until cleared" policy – made worse by the FBI's failure to give sufficient priority to carrying out clearance investigations. In your opinion, has the Justice Department responded in an appropriate manner to all the abuses identified in the Inspector General's report? What steps has the FBI taken to prevent such abuses from occurring in the future?**

**Response:**

The FBI worked diligently to determine whether the detainees, all of whom were in the United States illegally, did, in fact, have terrorism connections. When the FBI was able to determine that an alien was not of interest to the 9/11 investigation, the immigration authorities were notified as soon as possible. While many of the investigations of detainees took some time, for reasons discussed in the Inspector General's report, thorough investigation was necessary to ensure that these detainees posed no danger to our national security.

Several steps have been taken to ensure that future detainee matters are handled as efficiently and effectively as possible. As the Acting Deputy Attorney General explained in his 11/20/03 Memorandum to the Inspector General in response to the Inspector General's report, the FBI will work with DHS to establish criteria for future investigations (the specific criteria will depend on the nature of the national emergency). For example, an effort is underway to prepare an MOU between DHS and DOJ regarding criteria and procedures for identifying alien detainees of national security interest. In addition, the creation of TSC and TTIC will greatly improve the FBI's ability to gather information concerning aliens of national security interest and to work with the appropriate federal agencies to determine the best means of averting any national security threat, whether through criminal or immigration proceedings. Other initiatives, such as the Foreign Terrorist Tracking Task Force (FTTTF) and the National Joint Terrorism Task Force (NJTTF), have enhanced the flow of information with our law enforcement counterparts and will improve the handling of such cases.

**75. Enacted in 1990, the Hate Crime Statistics Act (HCSA) requires the Justice Department to acquire data on crimes which "manifest prejudice based on race, religion, sexual orientation, disability, or ethnicity" from law enforcement agencies across the country and to publish an annual summary of the findings. The HCSA, implemented by the FBI as part of its Uniform Crime Reporting (UCR) Program, now provides the best national picture of the magnitude of the hate violence problem in America – though it is still clearly incomplete.**

On November 12, 2003, the FBI released its annual report, *Hate Crime Statistics 2002*, of data collected under the HCSA. The FBI documented 7,462 hate crime incidents: 48.8% based on racial bias, 19.1% based on religious bias, 16.7% based on sexual orientation bias, and 14.8% based on ethnicity bias. The number of national law enforcement agencies reporting to the FBI in 2002 increased slightly from 11,987 to 12,073: the second highest total of participating agencies in the twelve-year history of the data collection effort. However, of the 12,073 agencies that participated, only 1,868 agencies (15.5%) reported even a single hate crime, a slight increase from the 17.6% that reported incidents in 2001. Thus, for 2002, 10,205 agencies (84.5%) reported *zero* hate crimes.

**a. How much training is the FBI providing to state and local law enforcement authorities to improve identification, reporting, and response to hate violence nationally?**

**Response:**

The FBI recognizes the importance of meaningful training to an individual's ability to perform effectively. Such training benefits state and local law enforcement agencies' recognition of hate crimes, which in turn assists the Uniform Crime Reporting (UCR) Program in identifying the magnitude of the problem nationwide. Over the last 4 fiscal years, the FBI's UCR Program has provided hate crime training to 1,857 law enforcement personnel during 38 training sessions in over 20 states and the District of Columbia. Year-by-year figures are as follows.

Fiscal Year	Number of Training Sessions	Number of States in Which Training was Conducted	Number of Agencies Represented	Number of Persons Trained
2001	14	8 + D.C.	438	771
2002	18	10	249	498
2003	4	3	366	577
2004 (9 months)	2	2	5	11

Face-to-face training sessions typically last 4-6 hours and include potential elements of bias motivation, how to identify the types of bias motivation for which the national UCR Program is required to collect data, and how to properly score and report an incident depending on the agency's reporting method (i.e., the Summary reporting system or the National Incident-Based Reporting System (NIBRS)).

The FBI also recognizes that, because of work schedules, location, budget restrictions, and a host of other factors, training is not always easy to obtain. Consequently, the UCR Program worked more than 2 years to develop and test effective Web-based hate crime identification and scoring training, which became available on the Law Enforcement OnLine (LEO) intranet in the summer of 2002. The FBI encourages those agencies wanting hate crime training to explore this Web-based option for their officers on LEO at: [http://home.leo.gov/lesig/cjis/programs/crime\\_statistics/hate\\_crime\\_web\\_training/](http://home.leo.gov/lesig/cjis/programs/crime_statistics/hate_crime_web_training/). (The access path from the LEO Home Page is LEOSIGs | CJIS | Programs | Uniform Crime Reporting | Hate Crime Web Training.) Law enforcement personnel requiring a LEO application may call the LEO Help Desk at 888-334-4536. The recent decrease in training is attributable both to the availability of this on-line training and to a temporary

reduction in training while the FBI uses those resources to develop the Law Enforcement National Data Exchange (N-DEx) Program, the purpose of which is the development of an improved, more useful UCR program. Although the FBI needed to commit the skills of those experienced in UCR to the development of N-DEx, N-DEx will substantially enhance the FBI's ability to provide hate crime information. The FBI is developing the training requirements necessary to implement the N-DEx Program and to ensure common reporting standards are achieved. Training will be incorporated into the N-DEx curriculum to improve Hate Crimes reporting through this process.

In addition to the above UCR Program training, the FBI's CRU and 56 FBI Field Offices routinely provide training to local and state law enforcement agencies regarding civil rights matters, including hate crimes. Hate crime training is also provided in quarterly National Academy (NA) courses, attended by specially nominated and selected representatives of state, local, and international law enforcement agencies. Approximately 1,000 NA attendees receive this training annually, enabling them to provide instruction to their respective departments.

**b. What steps is the FBI taking to increase participation in the HCSA data collection effort?**

**Response:**

In addition to the face-to-face and Web-based courses geared specifically to hate crime instruction, the national UCR Program briefs law enforcement personnel with respect to the hate crime data collection effort in its mainstream UCR training for Summary reporting and for NIBRS training. The FBI also keeps state UCR Programs and direct contributors informed of hate crime reporting procedures and training opportunities via the *UCR State Program Bulletin* and *UCR Newsletter*, respectively.

**c. Excellent FBI training materials on how to identify, report, and respond to hate crime are now available online: <http://www.fbi.gov/ucr/trainingd99.pdf> and <http://www.fbi.gov/ucr/hatecrime.pdf>. Are there any plans to update these 1999 resources to better reflect post-9/11 realities?**

**Response:**

The FBI periodically updates all of its training materials. The update of both *Hate Crime Data Collection Guidelines* and *Hate Crime Training Guide* will include post-9/11 realities.

**76. Professor Jack McDevitt, Director of The Center for Criminal Justice Policy Research at Northeastern University in Boston, has stressed the need for an expanded narrative in reporting hate crimes. In his September 2002 report, *Improving the Quality and Accuracy of Bias Crime Statistics Nationally*, funded by the Justice Department's Bureau of Justice Statistics, Professor McDevitt suggested that more detailed reporting can reduce the occurrence of "information disconnect" between the investigating officer and UCR reporting officials. Do you agree that the FBI's Hate Crime Incident Report forms should be revised to provide space to encourage additional narrative about the bias motivation present?**

**Response:**

Because participation in the UCR Program is voluntary, it would be counterproductive to participation to impose additional reporting burdens on law enforcement. In 2002, for example, law enforcement officers would have been required to write narratives concerning 7,462 hate crime incidents. Though the information collected from the Hate Crime Incident Report is somewhat limited, the FBI is able to collect more comprehensive data about hate crimes (and a wider scope of crime in general) from agencies that report crime using the 56 data elements of the NIBRS. The FBI is involved in an extensive national effort to redevelop and automate the UCR Program to enhance hate crime reporting.

**77. As states continue to enact hate crime statutes, the clear trend has been to include gender-based crimes in these laws. In 1990, only seven of the statutes in the thirty-one states that had hate crime laws included gender. Today, including the District of Columbia, twenty-eight of the forty-seven states with penalty-enhancement hate crimes statutes include gender-based crimes. Eight states now include gender in their hate crime data collection mandate. Gender-based crimes are also subject to Federal sentencing enhancements under 28 U.S.C. § 994. Do you share my view that the FBI's Hate Crime Incident Report should include a box in the Bias Motivation section for gender-based hate crimes? Is there some legal impediment to making that change, or could the Bureau take this step on its own?**

**Response:**

The FBI's UCR Program was assigned the task of collecting hate crime data according to the specific bias motivations stipulated in various hate crime statutes. The 1990 Hate Crime Statistics Act (HCSA) mandated a 4-year collection of data regarding biases against race, religion, sexual orientation, and ethnicity. In September 1994, the Violent Crime Control and Law Enforcement Act amended the HCSA to add bias against disabilities. Subsequently, the Church Arson Prevention Act of 1996 amended the collection duration to require collection "for



each calendar year," making the data collection effort a permanent part of the UCR Program. Should future legislation mandate the collection of gender-biased hate crimes, the FBI would comply.

**78. The current reporting form provides boxes only for "Anti-Hispanic" and "Anti-Other Ethnicity." In light of the disturbing number of post-9/11 "backlash incidents" directed at individuals in the aftermath of the September 11th terrorist attacks, wouldn't the FBI benefit from including on its form at least one additional box for "Anti-Arab" crimes?**

**Response:**

Though early hate crime data collection criteria included a code to indicate Anti-Arab as a subcategory of Ethnicity/National-Origin Bias, the code became invalid in 1996 as a result of changes from the Office of Management and Budget (OMB) concerning the administrative reporting of statistics as they pertain to race and ethnicity. On 10/30/97, OMB published "Revisions to the Standards for the Classification of Federal Data on Race and Ethnicity" in the Federal Register. The revised standards have five categories for data on race: American Indian or Alaska Native, Asian, Black or African American, Native Hawaiian or Other Pacific Islander, and White. Additionally, there are two categories for data on ethnicity: "Hispanic or Latino" and "Not Hispanic or Latino." The FBI complies with these guidelines in its data collection programs.

**79. Last October, after discussions with the FBI and others, I pointed out that the "sniper shootings" in the Washington, D.C. area could have been prevented if all states had the systems necessary to quickly transmit latent fingerprints from crime scenes to the FBI. In the sniper case, some three dozen prints from a murder-robbery in Alabama were not sent to the FBI until it was too late. I am pleased that since I identified that problem to the Bureau, five of the fifteen states that did not have the necessary connections to the FBI, including Alabama, have joined the system. However, there are still ten states where these connections do not exist. What can you do to bring these states into the system, not only to protect their own citizens but also to protect those in other states who might become the victims of offenders whose prints are already in the federal databases? If you need legislation to accomplish this, please specify what your needs are.**

**Response:**

As of the fall of 2004, 12 states lacked the IAFIS connectivity needed to process remote latent searches from their state systems: Arkansas, Louisiana, Delaware, Vermont, Indiana, Missouri, Nebraska, New Mexico, Oregon, Nevada, Utah, and Wyoming. (In Louisiana, Oregon, and Nevada, a few local agencies can submit

to IAFIS; Indiana, Missouri, and Nebraska are in the process of establishing the needed IAFIS connectivity.) The FBI has successfully assisted many states in overcoming the hurdles of securing IAFIS latent print functionality. The FBI currently provides latent print workstation software and latent print mailer software to state and local law enforcement agencies free of charge. In return, these agencies are responsible for obtaining the workstations, scanners, printers, and compression software necessary to capture, store, and transmit latent fingerprint searches to the FBI's IAFIS. Although many non-participating states continue to show a sustained interest in pursuing IAFIS latent print functionality, obstacles encountered within these agencies have slowed their progress.

Agencies have expressed concern over the lack of funding at the state and local levels to support the purchase, installation, and operation of latent print equipment. A source of funding could help to offset costs incurred for the implementation, operation, and maintenance of latent print programs in the non-participating states. Costs include those associated with the purchase of the equipment identified above and technical maintenance contracts, as well as the costs of additional personnel, including trained operators. Additional resources would also assist participating states in further enhancing their existing operations.

Networking requirements often serve as another obstacle for agencies attempting to secure IAFIS latent print functionality. The FBI has established high speed telecommunications infrastructures between primary state locations and IAFIS; however, state and local latent print operations frequently reside in multiple locations. Therefore, these locations must employ their own networks to support the electronic routing of latent print transactions to the FBI-provided central connection. Many states have experienced problems in providing this service to users.

The FBI has developed and implemented alternate connectivity solutions to assist agencies in overcoming these challenges. Laboratories and law enforcement agencies can connect directly to the FBI by using an FBI-provided modem and encrypted dial-up service or through crime laboratory connections. To further enhance access to regional, state, and national latent print search resources, the FBI is currently developing a connectivity option that will provide access through LEO, which offers a virtual private network permitting users to securely access information through an Internet Service Provider. This service would increase the access of latent print examiners by establishing connectivity through widely available internet connections. Even with these low-cost connectivity options, agencies would still incur costs to purchase the platform and to operate and maintain the workstations.

The FBI will continue to promote the latent print functionality of IAFIS to the law enforcement community; focusing these efforts on educating the remaining states as to the importance and benefits of this service.

**Questions Posed by Senator Feinstein**

80. The authority to arrest and detain a person whose "testimony . . . is material in a criminal proceeding" is set forth at 18 U.S.C. 1444, "Release or detention of a material witness." The following questions pertain to the use of that provision in counterterrorism investigations and prosecutions during the period of time from September 11, 2001 to the present.

- a. In how many cases have the authorities of 18 U.S.C. 1444 been used?
- b. How many individuals are currently detained under the authority of 18 U.S.C. 1444?
- c. In how many cases where the authority of 18 U.S.C. 1444 has been used has the individual arrested and detained in fact testified in "a criminal proceeding."
- d. 18 U.S.C. 1444 prohibits the detention of any individual where "testimony of such witness can adequately be secured by deposition." In how many cases where the authority of 18 U.S.C. 1444 has been used has a deposition been taken and the witness released?
- e. In how many cases in which an individual has been arrested or detained pursuant to 18 U.S.C. 1444 has the witness been subsequently charged with a crime?
- f. In how many cases in which an individual has been arrested or detained pursuant to 18 U.S.C. 1444 has the witness be[en] subsequently transferred to the custody of the Department of Defense? Please describe the facts and circumstances of each such case.
- g. In how many cases in which an individual has been arrested or detained pursuant to 18 U.S.C. 1444 has the witness be[en] subsequently transferred to the custody of a foreign government? Please describe the facts and circumstances of each such case.

**Response to questions a-g:**

The correct U.S. Code citation for "Release or Detention of a Material Witness" is 18 U.S.C. § 3144. We have consistently taken the view that any details about material witness warrants are grand jury material and cannot be disclosed. Therefore, we cannot address subparts a-g of question 80.

**h. What procedures and safeguards are in place to ensure that the authorities of 18 U.S.C. 1444 are not being used for purposes of preventive detention, or to hold individuals suspected of criminal activity without charging them with the commission of a crime?**

**Response:**

Detaining an individual on a material witness warrant under 18 U.S.C. 3144 requires a showing of probable cause that: 1) the testimony of the individual is material to a federal criminal proceeding; and 2) it is impractical to secure the individual's presence by lesser means. The judicial officer issuing the warrant must be satisfied by the facts and circumstances set forth in a sworn affidavit that these criteria are met. An individual detained pursuant to a material witness warrant has the right to contest the basis for detention before the court and has the right to the assistance of an attorney. This judicial oversight and opportunity to contest the basis for detention provide safeguards against misuse of the material witness process.

**I. What written policies or directives of the Department of Justice or the Federal Bureau of Investigation govern the application of the authorities set forth in 18 U.S.C. 1444?**

**Response:**

The FBI has no internal written policies or directives governing the application for material witness warrants because an FBI Agent's role in this process is limited. While an FBI Agent may be an affiant in an application for a material witness warrant, and will work closely with a prosecutor in the drafting of the affidavit supporting the application for a material witness warrant, the application itself is drafted and submitted by a federal prosecutor.

**81. In briefs filed with the Supreme Court in the matter of Padilla v. Rumsfeld, as well as in related cases and in public statements, the President and the Attorney General have asserted that the President, in his capacity as Commander-in-Chief may detain individuals, including United States citizens, as "enemy combatants." The following questions pertain to the exercise of this authority during the period from September 11, 2001 to present.**

**a. What role has the Federal Bureau of Investigation played in the arrest, detention, and interrogation of individuals held in custody pursuant to this authority as "enemy combatants?"**

**Response:**

In general, the FBI does not play a role in the arrest or detention of persons designated as enemy combatants, since this is within the purview of DOD's role in the global war on terrorism. Padilla was arrested by FBI Agents in Chicago and detained in federal custody as a material witness. While in federal custody, he was designated an enemy combatant and custody was transferred to the U.S. military.

The FBI has interviewed Padilla and other enemy combatants. FBI Agents conducting interviews of enemy combatants adhere to the FBI policy governing interviews of persons in the U.S., with the one exception that enemy combatants are not advised of Miranda rights prior to the interrogation.

- b. How many individuals have been arrested or detained pursuant to this authority?
- c. How many United States citizens have been arrested or detained pursuant to this authority?
- d. How many United States persons, as defined in Executive Order 12333, Section 3.4(D), and excepting United States citizens, have been arrested or detained pursuant to this authority?

**Response to b through d:**

Information concerning the designation and detention of enemy combatants is not maintained by the FBI. The Department of Defense, which is responsible for the custody and control of enemy combatants, would be the appropriate source for this information.

- e. What rules, procedures or practices govern the conditions of confinement and the methods of interrogation used in cases where an individual has been arrested or detained pursuant to this authority?

**Response:**

Rules, procedures, and practices concerning the conditions of confinement and methods of interrogation of enemy combatants by DOD are not maintained by the FBI. When FBI Agents interview enemy combatants or detainees, standard FBI

interview policies and practices apply. The Department of Defense, which is responsible for the custody and control of enemy combatants, would be the appropriate source for this information.

**82. Title 18 Section 3103a, as amended by Section 213 of the USA-Patriot Act (P.L. 107-56), provides authority for delaying notice of the execution of search warrants. The following question pertains to the use of the authority provided in this section in investigations or prosecutions related to terrorism during the period of time from September 11, 2001 to the present.**

**a. In how many such cases has the authorities to delay notification been used?**

**b. In how many such cases has the authority added by Section 213(b)(1), which allows a delay where "the court finds reasonable cause to believe that providing immediate notification of the execution of the warrant may have an adverse result" been used? Please describe the circumstances in each of these cases.**

**c. In how many such cases has the authority set forth in 18 U.S.C. 2705(E), which provides for delay in cases which would "otherwise seriously jeopardize an investigation or unduly [delay] a trial" been used? Please describe the circumstances in each of these cases?**

**Response:**

The FBI does not collect this information. However, we understand the Department has queried various U.S. Attorneys' Offices for this information and will forward it under separate cover as soon as it is compiled.

**83. Sections 201 and 202 of the USA-Patriot Act added a number of offenses to the "predicate offense list" applicable to criminal wiretaps pursuant to Chapter 119 of Title 18. The following question pertains to the time period since the passage of the USA-Patriot Act, October 26, 2001.**

**a. In how many cases . . . have the newly-added predicate offenses been used to support an application for a criminal wiretap under the authority of Chapter 119 of Title 18?**

**Response:**

The FBI applied for Title 18 wiretap orders in eight investigations into international terrorism since passage of the USA PATRIOT Act. In only one of those investigations was a newly added terrorism offense used as the sole predicate; traditional criminal offenses were used as the predicates for the remaining seven. It cannot be determined, however, whether probable cause as to one or more of the new terrorism predicate offenses was also established, but simply not listed, in those seven cases.

**b. In how many such cases has the newly-added predicate offense been the only predicate offense asserted as the basis for the warrant, i.e., where a warrant could not have been lawfully issued but for the passage of the additional criminal predicates?**

**Response:**

In the one case referred to above, the terrorism predicate was the only one asserted. It is not known, however, whether there was probable cause to believe the subjects were engaging in other predicate offenses which were simply not listed, or whether there was probable cause only with respect to the terrorism offense.

**c. Has the Department of Justice or the Federal Bureau of Investigation received any complaints regarding the application or implementation of Sections 201 or 202 of the USA-Patriot Act? If so, please describe the nature and disposition of any such complaint.**

**Response:**

The DOJ OIG is required under section 1001 of the USA PATRIOT Act to report to Congress every six months on allegations received by the OIG alleging abuses of civil rights or civil liberties by DOJ employees. The OIG issued its fifth report under section 1001 in September 2004.

The OIG has advised that, with the possible exception of the pending Mayfield investigation, none of the complaints submitted to the OIG alleging misconduct by employees of the Department has related to the use of a provision of the USA PATRIOT Act. Additionally, the FBI's Inspection Division, which reviews allegations of FBI misconduct, is aware of no complaints with respect to the FBI's application or implementation of this section.



d. Based upon the application of this provision of law during the period since its passage, are there changes to this statute, including the addition of predicate crimes, which the Congress should consider?

**Response:**

Sections 201 and 202 of the USA PATRIOT Act are currently scheduled to expire at the end of 2005. The FBI strongly supports making these important statutory provisions permanent. In addition, the FBI would ask Congress to consider amending 18 U.S.C. 2516 to allow for the use of existing electronic surveillance authorities in investigating the full-range of terrorism related crimes. In particular, Congress should consider adding the following predicate offenses to those currently listed in 18 U.S.C. 2516(1): 1) 18 U.S.C. 37 (relating to violence at international airports); 2) 18 U.S.C. 930(c) (relating to an attack on a federal facility with a firearm); 3) 18 U.S.C. 956 (conspiracy to harm persons or property overseas); 4) 18 U.S.C. 1993 (relating to mass transportation systems); 5) an offense involved in or related to domestic or international terrorism as defined in 18 U.S.C. 2331; 6) an offense listed in 18 U.S.C. 2332b(g)(5)(B); and 7) 18 U.S.C. 2332d.

While the few statistics listed in response to questions 83 a and b, above, may be understood to indicate limited use of this new authority and limited value of these new USA PATRIOT Act sections, this would not be correct. In most international terrorism investigations since October 2001, electronic surveillance has been successfully pursued under FISA authority and, therefore, the criminal terrorism predicates under Title 18 were not necessary. Nevertheless, in future investigations in which probable cause regarding connection to a foreign power cannot be as easily established (and thus FISA surveillance is not an option), these new USA PATRIOT Act provisions will permit the use of a federal wiretap in response to significant terrorist threats. The flexibility to use either foreign intelligence collection tools or criminal evidence gathering processes, and to share the results, is an important feature of the USA PATRIOT Act in the war against terrorism.

**84. Sections 203(b) and 203(d) of the USA-Patriot Act provide specific authority for the provision of intelligence information acquired in the course of a criminal investigation to elements of the Intelligence Community. Section 901 of the same [A]ct makes such disclosure in most cases mandatory. The following questions pertain to the implementation of these sections.**

**a. Section 203(c) of the USA-Patriot Act requires the Attorney General to "establish procedures for the disclosure of information" as provided for in Section 203.**

**Have such procedures been promulgated? If so, please provide a copy of those procedures to the Committee.**

**Response:**

On 9/23/02, the Attorney General promulgated guidelines that established the procedures for disclosure of information under Section 203 of the USA PATRIOT Act. Those guidelines, and the FBI's instructions to the field with respect to those guidelines, follow.



**Office of the Attorney General**  
**Washington, D. C. 20530**

September 23, 2002

**MEMORANDUM FOR HEADS OF DEPARTMENT COMPONENTS**

**FROM** THE ATTORNEY GENERAL *John Ashcroft*  
**SUBJECT** Guidelines for Disclosure of Grand Jury and Electronic, Wire, and Oral  
Interception Information Identifying United States Persons.

The prevention of terrorist activity is the overriding priority of the Department of Justice and improved information sharing among federal agencies is a critical component of our overall strategy to protect the security of America and the safety of her people.

Section 203 of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Pub. L. 107-56, 115 Stat. 272, 278-81, authorizes the sharing of foreign intelligence, counterintelligence, and foreign intelligence information obtained through grand jury proceedings and electronic, wire, and oral interception, with relevant Federal officials to assist in the performance of their duties. This authorization greatly enhances the capacity of law enforcement to share information and coordinate activities with other federal officials in our common effort to prevent and disrupt terrorist activities.

At the same time, the law places special restrictions on the handling of intelligence information concerning United States persons ("U.S. person information"). Executive Order 12333, 46 FR 59941 (Dec. 8, 1981) ("EO 12333"), for example, restricts the type of U.S. person information that agencies within the intelligence community may collect, and requires that the collection, retention, and dissemination of such information must conform with procedures established by the head of the agency concerned and approved by the Attorney General. Section 203(c) of the USA PATRIOT Act, likewise, directs the Attorney General to establish procedures for the disclosure of grand jury and electronic, wire, and oral interception information "that identifies a United States person, as that term is defined in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801)."

Pursuant to section 203(c), this memorandum specifies the procedures for labeling information that identifies U.S. persons. Information identifying U.S. persons disseminated pursuant to section 203 must be marked to identify that it contains such identifying information prior to disclosure.

Section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. § 1801) provides:

"United States person" means a citizen of the United States, an alien lawfully admitted for permanent residence (as defined in section 1101(a)(20) of Title 8), an unincorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation which is incorporated in the United States, but does not include a corporation or an association which is a foreign power, as defined in subsection (a)(1), (2), or (3) of this section.

Information should be marked as containing U.S. person information if the information identifies any U.S. person. The U.S. person need not be the target or subject of the grand jury investigation or electronic, wire, and oral surveillance; the U.S. person need only be mentioned in the information to be disclosed. However, the U.S. person must be "identified." That is, the grand jury or electronic, wire, and oral interception information must discuss or refer to the U.S. person by name (or nickname or alias), rather than merely including potentially identifying information such as an address or telephone number that requires additional investigation to associate with a particular person.

Determining whether grand jury or electronic, wire, and oral interception information identifies a U.S. person may not always be easy. Grand jury and electronic, wire, and oral interception information standing alone will usually not establish unequivocally that an identified individual or entity is a U.S. person. In most instances, it will be necessary to use the context and circumstances of the information pertaining to the individual in question to determine whether the individual is a U.S. person. If the person is known to be located in the U.S., or if the location is unknown, he or she should be treated as a U.S. person unless the individual is identified as an alien who has not been admitted for permanent residence or circumstances give rise to the reasonable belief that the individual is not a U.S. person. Similarly, if the individual identified is known or believed to be located outside the U.S., he or she should be treated as a non-U.S. person unless the individual is identified as a U.S. person or circumstances give rise to the reasonable belief that the individual is a U.S. person.

Grand jury and electronic, wire, and oral interception information disclosed under section 203 should be received in the recipient agency by an individual who is designated to be a point of contact for such information for that agency. Grand jury and electronic, wire, and oral interception information identifying U.S. persons is subject to section 2.3 of EO 12333 and the procedures of each intelligence agency implementing EO 12333, each of which place important limitations on the types of U.S. person information that may be retained and disseminated by the United States intelligence community. These provisions require that information identifying a U.S. person be deleted from intelligence information except in limited circumstances. An intelligence agency that, pursuant to section 203, receives from the Department of Justice (or

another Federal law enforcement agency) information acquired by electronic, wire, and oral interception techniques should handle such information in accordance with its own procedures implementing EO 12333 that are applicable to information acquired by the agency through such techniques.

In addition, the Justice Department will disclose grand jury and electronic, wire, and oral interception information subject to use restrictions necessary to comply with notice and record keeping requirements and as necessary to protect sensitive law enforcement sources and ongoing criminal investigations. When imposed, use restrictions shall be no more restrictive than necessary to accomplish the desired effect.

These procedures are intended to be simple and minimally burdensome so that information sharing will not be unnecessarily impeded. Nevertheless, where warranted by exigent or unusual circumstances, the procedures may be modified in particular cases by memorandum of the Attorney General, Deputy Attorney General, or their designees, with notification to the Director of Central Intelligence or his designee. These procedures are not intended to and do not create any rights, privileges, or benefits, substantive or procedural, enforceable by any party against the United States, its departments, agencies, or other entities, its officers or employees, or any other person.

The guidelines in this memorandum shall be effective immediately

**Precedence:** PRIORITY

**Date:** 11/05/2002

**To:** All Divisions  
Directors

**Attn:** Assistant Directors  
Deputy Assistant

Section Chiefs  
SACs  
ASACs  
Chief Division Counsels  
JTTF Supervisors

**From:** Office of the General Counsel  
Front Office, Room 7159  
**Contact:** Charles M. Steele, (202) 324-8089  
Elaine N. Lammert, (202) 324-5640

**Approved By:** Gebhardt Bruce J  
Ashley Grant D  
D'Amuro Pasquale J  
Wainstein Kenneth L  
Steele Charles M

**Drafted By:** Steele Charles M:cms

**Case ID #:** 62F-HQ-C1382989

**Title:** GUIDANCE ON NEW ATTORNEY GENERAL  
GUIDELINES ON SHARING FOREIGN  
INTELLIGENCE INFORMATION ACQUIRED  
IN CRIMINAL INVESTIGATIONS AND  
RELATED GUIDELINES

**Synopsis:** This EC provides guidance on the new Attorney General Guidelines on sharing foreign intelligence information acquired in the course of criminal investigations.

**Details:** On 9/23/02 the Attorney General issued three new sets of guidelines implementing sections 905 and 203 of the USA PATRIOT Act. Copies of the guidelines are enclosed; they are

To: All Divisions From: Office of the General Counsel  
Re: 62F-HQ-C1382989, 11/05/2002

also posted on the Office of the General Counsel's (OGC) website, in the Law Library webpage.<sup>2</sup> All employees should become familiar with the guidelines and with the guidance set forth in this EC.

1. **Guidelines Regarding Disclosure to the Director of Central Intelligence and Homeland Security Officials of Foreign Intelligence Acquired in the Course of A Criminal Investigation**

From an operational standpoint, these are the most important of the new guidelines. They will significantly affect the way in which the FBI approaches criminal investigations. The guidelines implement the mandate of section 905(a) of the PATRIOT Act that federal law enforcement agencies "shall expeditiously disclose to the Director of Central Intelligence [DCI], pursuant to guidelines developed by the Attorney General in consultation with the Director, foreign intelligence acquired ... in the course of a criminal investigation."<sup>3</sup> This is an affirmative statutory duty: the FBI (and other federal law enforcement agencies) must share foreign intelligence information (as defined in the guidelines) acquired in criminal investigations. The new guidelines are intended to institutionalize, formalize, and enhance such information sharing, which has been going on since passage of the PATRIOT Act, in order to further the FBI's primary mission of detecting and preventing acts of terrorism.

---

<sup>2</sup> On 9/24/02, the new guidelines were announced and posted on the FBI Intranet homepage. On 9/25/02, OGC notified all Chief Division Counsels (CDCs) by e-mail of the issuance of the guidelines. On 10/8/02, OGC notified all HQ Divisions by e-mail of the issuance of the guidelines, and directed them to the OGC webpage.

<sup>3</sup> The guidelines also require that foreign intelligence information be disclosed to designated Homeland Security officials. No such officials have yet been designated for purposes of receiving foreign intelligence. OGC will provide notification when such designations are made.

To: All Divisions From: Office of the General Counsel  
Re: 62F-HQ-C1382989, 11/05/2002

The procedures established by the guidelines for the sharing of foreign intelligence information with intelligence agencies are not intended to replace or supersede existing operational or information sharing mechanisms (e.g., information sharing that goes on in the context of Joint Terrorism Task Forces (JTTFs)). Agents should continue to use such mechanisms; subject to the guidelines.

The disclosure obligation extends to grand jury and Title III information which contains foreign intelligence information. Section 203 of the PATRIOT Act permits disclosure of such information to the CIA, notwithstanding prior legal impediments (e.g. the grand jury secrecy rule). Section 905(a), however, goes further, and requires that all such information be expeditiously disclosed.

"Foreign intelligence," as used in the guidelines, is defined as "information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities." This definition comes from the National Security Act of 1947, 50 U.S.C. § 401a.

Some of the more important provisions of the guidelines are summarized below.

#### Training (Guidelines ¶ 3)

The guidelines, and Section 908 of the PATRIOT Act, require the Department of Justice (DOJ) (in consultation with the DCI and other officials) to develop a training curriculum and program to ensure that law enforcement officials receive sufficient training to identify foreign intelligence subject to the disclosure requirement. Training is critical to the successful implementation of the guidelines; it is crucial that law enforcement agents be able to recognize foreign intelligence information subject to the disclosure requirement. In some



To: All Divisions From: Office of the General Counsel  
Re: 62F-HQ-C1382989, 11/05/2002

instances it will be obvious that certain information constitutes foreign intelligence information; in other cases it may not be so clear.

DOJ and the FBI are consulting with the CIA to formulate and implement a training curriculum and program, which will include training for both new and onboard Agents. CIA personnel will participate, providing instruction on how to identify the types of foreign intelligence information needed by the Intelligence Community.

Further details will be provided when the training curriculum is finalized.

Entities to Whom Disclosure Shall be Made  
(Guidelines, ¶ 4)

The guidelines require the DCI, in consultation with the Assistant to the President for Homeland Security, to designate appropriate offices, entities and/or officials of intelligence agencies and homeland security offices to receive the disclosure of section 905(a) information not covered by an established operational or information sharing mechanism. The DCI is to ensure that sufficient numbers of recipients are identified to facilitate expeditious sharing and handling of section 905(a) information. The DCI has not yet identified recipients pursuant to this provision; OGC will provide notification when recipients are designated.

Note that these designated recipients will come into play only where there isn't already "an established operational or information sharing mechanism." Guidelines, paragraph 4. Where there are already established mechanisms (e.g. JTTFs), FBI Agents can and should use them to disclose 905(a) information.

Methods for Disclosure of Section 905(a) Information

To: All Divisions From: Office of the General Counsel  
Re: 62F-HQ-C1382989, 11/05/2002

(Guidelines, ¶ 5)

The guidelines divide foreign intelligence information into two categories: (1) information relating to terrorism or weapons of mass destruction (WMD),<sup>4</sup> and (2) all other types of foreign intelligence information. Similarly, the guidelines address two different categories of terrorism/WMD information: that which relates to "a potential ... threat," and "other" terrorism/WMD information.

Foreign intelligence information relating to a "potential terrorism or WMD threat to the United States homeland, its critical infrastructure, key resources (whether physical or electronic), or to United States persons or interests worldwide" must be disclosed "immediately." Guidelines, ¶ 5(a). All other foreign intelligence information (including all other foreign intelligence information relating to terrorism or WMD information, e.g. information relating to the financing of a terrorist organization, or to an organization's long-term recruitment plans) must be disclosed "as expeditiously as possible."<sup>5</sup>

Whether particular terrorism/WMD foreign intelligence information relates to a "potential threat" (i.e. requiring immediate disclosure) will depend on the facts and circumstances of the particular situation. Clearly, information indicating the planning or commission of an imminent act of terrorism will fall into this category. On the other hand, foreign intelligence information relating to long-term recruiting efforts by a terrorist organization will have to be disclosed

---

<sup>4</sup> "Terrorism information" and "weapons of mass destruction," for purposes of the guidelines, are defined in ¶ 5(a), at page 4.

<sup>5</sup> As to section 905(a) information other than that relating to terrorism and WMD, the guidelines require federal law enforcement agencies, in consultation with DOJ and the DCI, to develop (or continue to follow existing) protocols to provide for expeditious sharing. ¶ 5(b), at page 4.

To: All Divisions From: Office of the General Counsel  
Re: 62F-HQ-C1382989, 11/05/2002

expeditiously, but not immediately. The upcoming training will help clarify what information is so related to a "potential threat" that it must be disclosed immediately; for the time being, Agents should exercise sound judgment in making the determination, keeping in mind that the ultimate purpose for the disclosure requirement is to help "disrupt[] terrorist plans, prevent[] terrorist attacks, and preserv[e] the lives of United States persons." Guidelines, ¶ 5(a).

Disclosure may be made in the following ways: (1) through existing field-level operational or information sharing mechanisms (e.g. JTTFs); (2) through existing headquarters operational or information sharing relationships; or (3) when the law enforcement officer reasonably believes that time does not permit the use of any such established mechanisms, through any other field level or other mechanism intended to facilitate immediate action, response or other efforts to address a threat. (I.e., if an Agent reasonably believes that the circumstances require immediate action, he or she should take whatever steps are necessary to share the information with the appropriate intelligence agency immediately. This could mean, for example, picking up the phone and calling a point of contact he or she has with the CIA.)

As soon as practicable after disclosing section 905(a) information (under any of the above-referenced mechanisms), the disclosing Agent must notify the relevant JTTF (e.g., the JTTF supervisor) of the disclosure. JTTFs, in turn, must keep the relevant Anti-Terrorism Task Force (ATTF) (e.g., the United States Attorney's Office representative on the ATTF) apprised of the nature of information disclosed under the guidelines. JTTFs are not required to notify ATTFs of every disclosure of foreign intelligence information; DOJ recognizes that such a requirement would be impractical. JTTFs, however, should take steps to keep ATTFs generally apprised of the nature of section 905(a) information disclosed; JTTFs should also ensure that ATTFs are specifically advised of particularly important disclosures (e.g. disclosures relating to specific threats). Whether a particular

To: All Divisions From: Office of the General Counsel  
Re: 62F-HQ-C1382989, 11/05/2002

disclosure is important enough to warrant specific notice to the ATTF is a judgment call. ATTFs shall, in turn, apprise DOJ's Terrorism and Violent Crime Section (TVCS) of section 905(a) disclosures. (Also: where section 905(a) information is disclosed at the headquarters level, the disclosing headquarters entity shall, as soon as practicable and to the extent reasonable, notify TVCS of all disclosures.)

It has not yet been decided whether a single, standard procedure will be developed to govern how JTTFs will notify ATTFs, or rather whether each JTTF will be asked to develop its own mechanism. That matter is under consideration at FBIHQ. In the meantime, each JTTF should preliminarily develop its own mechanism for notifying ATTFs, taking into account its own particular structure, personnel, existing communication channels with ATTFs, etc.

Consultation With Prosecutors With Respect to  
Title III and Grand Jury Information (Guidelines, ¶ 5(c))

In order to avoid harm to pending or anticipated prosecutions, the guidelines establish requirements for pre-disclosure consultation with prosecutors in certain situations. Specifically, the guidelines state that, except as to terrorism/WMD information related to a potential threat, the law enforcement agent must consult with the prosecutor assigned to the case if (1) the information was developed through investigation occurring after a formal referral for prosecution, and (2) the information was produced by a Title III interception or solely as a result of a grand jury subpoena or testimony occurring before a grand jury receiving information concerning the particular investigation.

This consultation requirement serves the important purpose of allowing the prosecutor to decide whether to impose use restrictions (as set forth in ¶ 8 of the guidelines) or to

To: All Divisions From: Office of the General Counsel  
Re: 62F-HQ-C1382989, 11/05/2002

seek an exception to the disclosure requirement (as set forth in ¶ 9 of the guidelines).

This pre-disclosure consultation with the prosecutor must be accomplished expeditiously. An Agent who consults with a prosecutor pursuant to this provision should document the fact of the consultation, including the date and time of the contact with the prosecutor. If the prosecutor concurs with disclosure, the Agent must make the disclosure no later than 48 hours after the prosecutor is initially notified. If the prosecutor objects, the Agent should obtain and document the prosecutor's reasons and, if the Agent disagrees with the prosecutor's position, consult with his or her supervisors. (The Agent should not disclose the information, however, until the disagreement with the prosecutor is fully resolved.) If the Agent does not have a decision from the prosecutor as of 48 hours after the initial contact, the Agent should contact the prosecutor to determine the prosecutor's position.

Title III or grand jury-generated section 905(a) information which an Agent reasonably believes is related to a potential terrorism or WMD threat shall be disclosed immediately, without need for advance consultation with the prosecutor. Contemporaneously or as soon after making such disclosures as possible, the Agent shall notify the prosecutor (to enable the prosecutor to make any required notice to the court).

Requests for Additional Information (Guidelines, ¶ 6)

Initial disclosure of section 905(a) information shall be accomplished automatically, without specific prior request to the disclosing agency. Requests by any recipient for additional information, or for clarification or amplification of the initial disclosure, should be coordinated through the component that provided the initial information or the designated HQ office of the disclosing agency.

To: All Divisions From: Office of the General Counsel  
Re: 62F-HQ-C1382989, 11/05/2002

Disclosure of Grand Jury and Title III Information  
(Guidelines, ¶ 7)

Where grand jury or Title III information is shared under the guidelines, notice of such disclosures must be promptly provided to DOJ's Office of Enforcement Operations (OEO).<sup>6</sup> Agents do not have to contact OEO themselves; that is the obligation of the AUSA or DOJ prosecutor assigned to the grand jury matter or Title III.

The PATRIOT Act also requires special procedures for the disclosure of grand jury and Title III information that identifies United States persons. Those procedures are set forth in the second set of guidelines issued on 9/23/02 and discussed below. Also, all of the procedures established pursuant to those guidelines are made applicable to all disclosures under these guidelines of section 905(a) information that identifies United States persons.

Use Restrictions (Guidelines, ¶ 8)

Generally, the guidelines contemplate that 905(a) information will be disclosed without imposition of use restrictions. However, the disclosing official may impose appropriate use restrictions necessary to protect sensitive law enforcement sources and pending criminal investigations and prosecutions.

The scope and duration of any such restrictions must be tailored to address the particular situation. Any such restrictions must be no more restrictive than necessary to accomplish the desired effect. Also, the originator of the information must periodically review the restrictions to

---

<sup>6</sup> The guidelines require OEO to establish appropriate record keeping procedures to ensure compliance with notice requirements related to the disclosure of grand jury information. Guidelines, ¶ 7.

To: All Divisions From: Office of the General Counsel  
Re: 62F-HQ-C1382989, 11/05/2002

determine whether they can be narrowed or lifted at the request of the recipient.

Finally, disclosures of grand jury and Title III information must be subject to any use restrictions necessary to comply with record or notice keeping requirements, and to protect sensitive law enforcement sources and pending criminal investigations and prosecutions. Agents should consult with the AUSA or DOJ prosecutor assigned to the grand jury matter or Title III to determine what use restrictions, if any, are necessary in each case.

AG Exceptions to Mandatory Disclosure  
(Guidelines, ¶ 9)

Section 905(a) authorizes the Attorney General, in consultation with the DCI, to exempt from the disclosure requirement one or more classes of foreign intelligence or foreign intelligence relating to one or more targets or matters. Paragraph 9 of the guidelines implements this provision. It states that pending the development of permanent exceptions, exemptions will be determined by the Attorney General, in consultation with the DCI and the Assistant to the President for Homeland Security, on a case-by-case basis.

No permanent exceptions have yet been developed. OGC will provide notification if and when permanent exceptions are developed.

Requests for exceptions must be submitted "by the department, component or agency head in writing with a complete description of the facts and circumstances giving rise to the need for an exception and why lesser measures such as use restrictions are not adequate." Guidelines, ¶ 9(c). Authority to request exceptions has not yet been delegated below the level of component agency head (and it is not clear whether it will

To: All Divisions From: Office of the General Counsel  
Re: 62F-HQ-C1382989, 11/05/2002

be). For now, therefore, FBI requests for exceptions can only be submitted by the Director.

Any FBI requests for exceptions should be submitted for review and approval to CID and CTD. CID and/or CTD will then forward the requests to the Director's Office. OGC will be available to provide assistance with regard to any such requests.

#### Closed Investigations

OGC has concluded, in consultation with DOJ, that there is no legal impediment to sharing foreign intelligence information acquired in criminal investigations which have been closed. Field offices should therefore identify closed criminal investigations which appear likely to have developed foreign intelligence information; if any such information is found, it must be disclosed pursuant to the guidelines.

Field offices need not conduct comprehensive general searches of all closed files, or of broad categories of closed files. If, however, there is reason to believe it is likely that particular closed files contain foreign intelligence information, the field office should conduct reviews of those files.

#### **2. Guidelines for Disclosure of Grand Jury and Electronic, Wire, and Oral Interception Information Identifying United States Persons**

Section 203 of the PATRIOT Act authorizes the sharing of foreign intelligence, counterintelligence, and foreign intelligence information obtained through grand jury proceedings



To: All Divisions From: Office of the General Counsel  
Re: 62F-HQ-C1382989, 11/05/2002

and Title III interceptions with relevant Federal officials<sup>7</sup> to assist in the performance of their duties. At the same time, section 203(c) requires the Attorney General to establish procedures for the disclosure of grand jury and Title III information that identifies United States persons.<sup>8</sup>

These new guidelines implement section 203(c) by establishing the required procedures for labeling grand jury and Title III information which identifies United States persons. Such information must be marked, prior to disclosure, to indicate that it contains such identifying information. Information should be marked if it identifies any United States person (i.e. the person need not be a target or a subject). However, the United States person must be "identified," i.e., the grand jury or Title III information must discuss or refer to the U.S. person by name (or nickname or alias), rather than merely including potentially identifying information (e.g. an address or telephone number) which requires additional investigation to link to a particular person.

For the time being, no particular language or method of marking is required.<sup>9</sup> The information must be clearly marked, however, in a manner which will ensure that the recipient will immediately understand that the information identifies United States persons. One way to do this, for example, would be to place the information in a sealed envelope marked with the following language in conspicuous lettering:

---

<sup>7</sup>The information may be shared with any Federal law enforcement, intelligence, protective, immigration, national defense, or national security officials receiving that information in the performance of his official duties. Fed. R. Crim. P. 6(e)(3)(C)(V) (grand jury information); 18 U.S.C. § 2517(6) (Title III information).

<sup>8</sup>"United States person" means a citizen of the United States, an alien lawfully admitted for permanent residence (as defined in section 1101(a)(20) of Title 8), an unincorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation which is incorporated in the United States, but does not include a corporation or an association which is a foreign power, as defined in subsection (a)(1), (2), or (3) of this section. 50 U.S.C. § 1801.

<sup>9</sup>FBIHQ is considering whether to institute a single, standard method of marking.

To: All Divisions From: Office of the General Counsel  
Re: 62F-HQ-C1382989, 11/05/2002

"NOTE: THIS PACKAGE CONTAINS INFORMATION WHICH IDENTIFIES UNITED STATES PERSON(S)." Agents should also specifically direct the recipient to the references to identified U.S. persons.

Agents need not rely solely on the grand jury or Title III information itself in determining whether the information identifies a United States person; Agents may also use the context and circumstances of the information in making that determination.

If the person is known to be located in the U.S. (or if his or her location is unknown), he or she should be treated as a U.S. person unless circumstances give rise to the reasonable belief that he or she is not a United States person. Similarly, if the person is known or believed to be located outside the U.S., he or she should be treated as a non-United States person unless he or she is identified as, or circumstances give rise to the reasonable belief that he or she is, a United States person.

Receiving agencies are to designate individuals as points of contact for purposes of receiving this information. (No such designations have yet been made; OGC will provide notification when designations are made.) Also, receiving agencies are to handle such information in accordance with their own procedures implementing Executive Order 12333 (which governs such agencies' collection and use of such information).

**3. Guidelines Regarding Prompt Handling of  
Reports of Possible Criminal Activity  
Involving Foreign Intelligence Sources**

These guidelines implement section 905(b) of the PATRIOT Act, which requires the Attorney General to develop guidelines to ensure that DOJ responds within a reasonable period of time to reports from the intelligence community of

To: All Divisions From: Office of the General Counsel  
Re: 62F-HQ-C1382989, 11/05/2002

possible criminal activity involving foreign intelligence sources or potential foreign intelligence sources.

Section 905(b) and the guidelines reflect a recognition that in such situations the referring intelligence community agency may have a strong interest in knowing on an expedited basis whether DOJ intends to investigate potential crimes.

Accordingly, the guidelines require DOJ to confer expeditiously (and not later than seven days after the referral) with the referring intelligence community agency. After conferring, DOJ shall inform the referring agency within a reasonable period of time (not more than 30 days, except in extraordinary circumstances) whether it intends to commence or decline a criminal investigation.

**LEAD(s):**

**Set Lead 1: (Adm)**

ALL RECEIVING OFFICES

This communication should be distributed to all employees within your division. In particular, please ensure prompt distribution to all Special Agents and other appropriate investigative personnel.

♦♦

CC: 1 - Mr. Bruce Gebhardt  
1 - Mr. Grant Ashley  
1 - Mr. Pasquale D'Amuro  
1 - Mr. Kenneth Wainstein  
1 - Mr. Charles Steele  
1 - Mr. M.E. Bowman

To: All Divisions From: Office of the General Counsel  
Re: 62F-HQ-C1382989, 11/05/2002

- 1 - Mr. Patrick Kelley
- 1 - Ms. Elaine Lammert
- 1 - Mr. James Lovelace
- 1 - Mr. John Livingston

**b. Section 203(b) specifically provides authority "to share electronic, wire, and oral interception information" where such information is foreign intelligence information. What is the method for disseminating such information to the Intelligence Community?**

**Response:**

Electronic, wire, and oral interception information derived through standard criminal procedures may be disseminated to the IC through any means appropriate to the circumstances, including Intelligence Information Reports (IIRs), Teletype Memoranda, Intelligence Assessments, Intelligence Bulletins, and FBI Letterhead Memoranda.

**(i) In your testimony you made reference to newly-created procedures by which the Federal Bureau of Investigation disseminates intelligence via "electronic intelligence reports" - is this the mechanism used for dissemination of Section 203(b) material?**

**Response:**

The FBI disseminates intelligence information via the IIR, which is an electronic communication format widely accepted in the IC as the standard intelligence dissemination vehicle. IIRs consist of raw intelligence (intelligence which has not been finally evaluated) and associated clarifying information that puts the raw intelligence into context. IIRs are drafted and prepared by the FBI's cadre of Intelligence Analysts/Reports Officers. Before FBI intelligence is disseminated, it is analyzed and sanitized to protect intelligence sources and methods and, if applicable, United States persons and entities that may be compromised or negatively impacted if left unprotected. FBI Program Managers and Intelligence Analysts concurrently identify intelligence that is consistent with IC intelligence requirements and interests.

**(1) If so, how many such reports have been issued?**

**Response:**

Although CTD is not the only FBI producer of IIRs, that Division reports that, during the period from August 2002 (when statistical data was first collected) through August 2004, CTD has disseminated approximately 3,860 IIRs, 240 of which have contained FISA-derived intelligence. The remaining IIRs have been

derived from various sources and methods which may or may not include Title III information.

The FBI does not track or maintain a central database with respect to the number of IIRs containing 203(b) material, if any.

**(2) Has the Federal Bureau of Investigation developed procedures to ascertain the quality and value of such intelligence reports?**

**Response:**

Determinations to disseminate electronic, wire, and oral intercept information are made with input from Operational Program Managers, Intelligence Analysts, the National Security Law Branch, and, when appropriate, DOJ. This evaluation considers the value of the information not only to the IC but also, depending on the proposed use, context, and nature of any threat-related information, to federal, state, and local law enforcement entities and, when authorized by DOJ, to foreign intelligence services and foreign law enforcement agencies.

The quality and value of IIRs are evaluated through several means. On each IIR, the Reports Officer provides information by which the customers can contact the Reports Officer directly. The quality and relevance of the reporting is also reflected by the submission of additional collection requirements; IC members often forward formal Requests for Information (RFIs) with respect to information that has been protected (not provided) in the IIR, such as U.S. Person information. Such RFIs provide an excellent indication of IC interest in FBI reporting. In addition, IC members often provide feedback with respect to specific IIRs directly to the FBI Intelligence Analysts/Reports Officers who author the reports. The FBI's OI also often receives evaluations of FBI reporting, and is working to establish a formal IIR evaluation mechanism by which recipients can rate or provide feedback on FBI intelligence reporting.

**c. Section 203(d), the so-called "catch-all" provision, provides a general authority to share foreign intelligence information with the Intelligence Community. What is the method for disseminating such information to the Intelligence Community?**

**Response:**

The FBI shares foreign intelligence information, as defined in Section 203(d)(2), with the IC through several conduits. Dissemination can be through direct classified and unclassified IIRs, Intelligence Assessments, Intelligence Bulletins,

Teletype Memoranda, or IC web sites on classified networks. The FBI also shares intelligence information through the FBI's Joint Terrorism Task Forces (JTTFs), which include members of the IC and operate in 100 locations across the United States. Unclassified but "law enforcement sensitive" intelligence information is also disseminated to federal, state, and local law enforcement intelligence components through Law Enforcement Online (LEO), a computer network which provides finished intelligence products, assessments, and bulletins on significant developments and trends.

**(i) In your testimony you made reference to newly-created procedures by which the Federal Bureau of Investigation disseminates intelligence via "electronic intelligence reports" - is this the mechanism used for dissemination of Section 203(d) material?**

**Response:**

Electronic, wire, and oral interception information derived through standard criminal procedures may be disseminated to the IC through any appropriate means, including IIRs, Teletype Memoranda, Intelligence Assessments, Intelligence Bulletins, and FBI Letterhead Memoranda.

**(1) If so, how many such reports have been issued?**

**Response:**

While the FBI does not track or maintain a central database with respect to the number of IIRs containing 203(d) material, if any, the July 2004 DOJ "Report From the Field: The USA PATRIOT Act at Work" indicates that DOJ has made disclosures of vital information to the intelligence community and other federal officials under section 203 on many occasions. For instance, such disclosures have been used to support the revocation of visas of suspected terrorists and prevent their reentry into the United States, to track terrorists' funding sources, and to identify terrorist operatives overseas.

**(2) Has the Federal Bureau of Investigation developed procedures to ascertain the quality and value of such intelligence reports?**

**Response:**

There are various means by which IIRs are evaluated. Members of the IC often provide feedback assessing the quality and value of specific IIRs directly to the FBI Intelligence Analysts/Reports Officers who author the reports. On each IIR, the Reports Officers identify the means by which customers can contact them directly. IC members assess the quality and relevance of the reporting, and submit additional collection requirements when appropriate. Often, IC members forward formal Requests for Information (RFIs), which can provide an excellent indication of IC interest in FBI reporting. The FBI's OI also receives evaluations of FBI reporting. The OI is working to establish a formal IIR evaluation mechanism by which recipients can rate or provide feedback on FBI intelligence reporting.

**d. Section 905(c) of the USA-Patriot Act requires the Attorney General to "develop procedures for the administration of this section. . . ." Have such procedures been promulgated? If so, please provide a copy of those procedures to the Committee.**

**Response:**

Pursuant to Section 905, DOJ developed the Attorney General's Guidelines Regarding Information Sharing under the USA PATRIOT Act. These guidelines are available on the website of DOJ's Office of Legal Policy (OLP) ([www.usdoj.gov/olp](http://www.usdoj.gov/olp)). Additionally, among other Department materials relating to information sharing are the following:

- The Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection, Part VII.B. (10/31/03) (concerned in part with information sharing with intelligence agencies) – Portions of these guidelines are classified, but Part VII.B., relating to information sharing, is unclassified and appears without deletions on OLP's website.
- Memorandum of Understanding between the Intelligence Community, Federal Law Enforcement Agencies, and the Department of Homeland Security Concerning Information Sharing (3/4/03).
- Memorandum from the Attorney General entitled, "Guidelines Regarding Disclosure to the Director of Central Intelligence and Homeland Security Officials of Foreign Intelligence Acquired in the Course of a Criminal Investigation" (9/23/02) – Available on OLP's website.



- Memorandum from the Attorney General entitled, "Coordination of Information Relating to Terrorism" (4/11/02) (concerned in part with information sharing with other Federal agencies) – Available on OLP's website.
- Memorandum from the Attorney General entitled, "Prevention of Acts Threatening Public Safety and National Security" (11/8/01) (concerned in part with information sharing with other Federal agencies) – Available on OLP's website.
- Memorandum from the Attorney General entitled, "Disseminating Information to Enhance Public Safety and National Security" (Sept. 21, 2001) (concerned in part with information sharing with other Federal agencies) – Available on OLP's website.

**e. Has the Department of Justice, the Director of Central Intelligence (in his capacity as head of the Intelligence Community) or the Federal Bureau of Investigation received any complaints regarding the application or implementation of Section 203 of the USA-Patriot Act? If so, please describe the nature and disposition of any such complaint.**

**Response:**

The DOJ OIG is required under section 1001 of the USA PATRIOT Act to report to Congress every six months on allegations received by the OIG alleging abuses of civil rights or civil liberties by DOJ employees. The OIG issued its fifth report under section 1001 in September 2004.

The OIG has advised that, with the possible exception of the pending Mayfield investigation, none of the complaints submitted to the OIG alleging misconduct by employees of the Department has related to the use of a provision of the USA PATRIOT Act. Additionally, the FBI's Inspection Division, which reviews allegations of FBI misconduct, is aware of no complaints with respect to the FBI's application or implementation of this section.

**f. Based upon the application of this provision of law during the period since its passage, are there changes to this statute which the Congress should consider?**

**Response:**

Sections 203(b) and (d) should not be allowed to expire on 12/31/05, since the changes afforded by the USA PATRIOT Act have significantly increased the ability of the FBI to share information.

85. Section [ ] 206 of the USA-Patriot Act, the so-called "roving wiretap" provision, permits the issuance of a FISA warrant in cases where the subject will use multiple communication facilities. This question pertains (to) the implementation of this section during the time period since the passage of the USA-Patriot Act, October 26, 2001.

a. How often has this authority been used, and with what success?

Response:

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

b. In your testimony you made reference to newly-created procedures by which the Federal Bureau of Investigation disseminates intelligence via "electronic intelligence reports" - is this the mechanism used for dissemination of material acquired pursuant to the FISA?

Response:

FBI intelligence products are an important vehicle for the dissemination of both FISA-derived and non-FISA foreign intelligence information, but not the only one. The FBI shares many forms of foreign intelligence with other members of the IC through direct classified and unclassified disseminations, through web sites on classified IC networks, through its participation in Joint Terrorism Task Forces (JTTFs), and through its collaboration in activities abroad.

FBI intelligence products shared with the IC include IIRs, Intelligence Assessments, and Intelligence Bulletins. The FBI also disseminates intelligence information through LEO, a virtual private network that reaches federal, state, and local law enforcement agencies at the Sensitive But Unclassified (SBU) level. LEO makes available to all users finished FBI intelligence products, including intelligence assessments resulting from the analysis of criminal, cyber, and terrorism intelligence, finished intelligence concerning significant developments or trends, and IIRs that are available at the SBU level. In addition, the FBI recently posted the requirements document on LEO, providing to state and local law enforcement a shared view of the terrorist threat and the information needed in every priority area.

(i) If so, how many such reports have been issued?

**Response:**

In the past two years, CTD's Terrorism Reports and Requirements Section has disseminated 76 IIRS containing information derived from FISA-authorized surveillance and/or searches. (Statistics are not maintained in a way that would enable us to advise whether any of the FISA-derived information in the reports was obtained using roving wiretap authority.) Other FBI Divisions have also issued reports containing FISA-derived information. For example, the Cyber Division has written a total of 24 IIRs containing FISA-derived information.

**(ii) Has the Federal Bureau of Investigation developed procedures to ascertain the quality and value of such intelligence reports?**

**Response:**

The OI promulgated the FBI's Intelligence Information Report Handbook on 7/9/04. The Handbook establishes the first comprehensive FBI-wide guide for the format and content of raw intelligence reports. The OI is also working to develop evaluation guidelines based, in part, on the criteria established in the Handbook for the types of information to be reported and shared with law enforcement and IC partners.

In addition, the FBI's Inspection Division has established criteria for assessing: the value of human source reporting; access to and the responsiveness of local FBI field offices; and FBI program and national intelligence requirements. The OI is developing guidelines for using these same criteria to assess the value of raw intelligence. Initial discussions on this issue have been held with the CI, CT, Criminal, and Cyber Divisions, and the results of these discussions are being incorporated into evaluation guidelines.

**c. Some have read this section as providing for surveillance in cases where neither the identity of the subject or the facility to be used is known – in effect, allowing for the authorization of FISA surveillance against all phones in a particular geographic area to try to intercept conversation of an unknown person. Is this the reading of the statute being adopted by the Federal Bureau of Investigation and the Department of Justice? If not, please provide your interpretation of this authority.**

**Response:**

No, DOJ does not interpret the statute as allowing for the authorization of FISA surveillance against all phones in a particular geographic area to try to intercept

the conversations of an unknown person. In order to make a showing of probable cause, the FISA statute requires a statement of the facts and circumstances relied upon by the applicant for surveillance to justify the belief that: (1) the target of the electronic surveillance is a foreign power or an agent of a foreign power; and, (2) each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power. Thus, the FISA statute does not permit coverage to be authorized, with or without the "roving wiretap" provision, for surveillance of all persons in a particular geographic area. The FBI has interpreted the "roving" authority as permitting the FBI to request that the FISA Court issue, along with the primary order, a "generic" secondary order with respect to a specifically identified FISA target that the FBI can serve in the future on a currently unknown cell phone carrier, Internet service provider, or other communications provider, if the target rapidly switches from one provider to another. The roving wiretap order still requires that a federal law enforcement agent swear, in a detailed affidavit, to facts establishing probable cause, and still requires a court to make a finding of probable cause before issuing the order. While the roving order carries the additional requirement of a judge's approval to monitor more than one telephone, it permits government agents to continue to monitor the target, even if the target changes to a different cellular telephone, rather than first going through the lengthy application process to monitor that new phone. This will allow the FBI to go directly to the new carrier and establish surveillance on the authorized target without having to return to the FISA Court for a new secondary order. The FBI views this as a vital tool to follow targets who change cell phone providers or other communication channels as a deliberate means of evading surveillance.

**(i) Have any briefs been filed with the Foreign Intelligence Surveillance Court on this subject? If so, please provide copies of such briefs to the Committee.**

**Response:**

The FBI does not file briefs with the FISA Court. While OIPR files briefs with that Court on behalf of DOJ and the government, it has filed no such briefs on this subject.

**d. Has the Department of Justice, the Director of Central Intelligence (in his capacity as head of the Intelligence Community) or the Federal Bureau of Investigation received any complaints regarding the application or implementation of Section 206 of the USA-Patriot Act? If so, please describe the nature and disposition of such a complaint.**

**Response:**

The DOJ OIG is required under section 1001 of the USA PATRIOT Act to report to Congress every six months on allegations received by the OIG alleging abuses of civil rights or civil liberties by DOJ employees. The OIG issued its fifth report under section 1001 in September 2004.

The OIG has advised that, with the possible exception of the pending Mayfield investigation, none of the complaints submitted to the OIG alleging misconduct by employees of the Department has related to the use of a provision of the USA PATRIOT Act. Additionally, the FBI's Inspection Division, which reviews allegations of FBI misconduct, is aware of no complaints with respect to the FBI's application or implementation of this section.

**e. Based upon the application of this provision of law during the period since its passage, are there changes to this statute which the Congress should consider?**

**Response:**

No. The FBI requests only that the provision be preserved.

**86. Section 207 of the USA-Patriot Act extends the time limits provided in the FISA which govern surveillance against agents of a foreign power.**

**a. Has the Federal Bureau of Investigation or the Department of Justice conducted any review to determine whether, and if so, how many, personnel resources have been saved by this provision? If so, please provide the results to the Committee.**

**Response:**

We are not aware of any systematic reviews in this area, either by the FBI or DOJ.

**b. Have there been any cases where, after the passage of the now-extended deadlines it was determined, either by the Department of Justice, the Federal Bureau of Investigation or the Foreign Intelligence Surveillance Court, that surveillance should have been terminated at an earlier point because of the absence of a legally required predicate?**

**Response:**

None of which the FBI is aware.

**c. Has the Department of Justice, the Director of Central Intelligence (in his capacity as head of the Intelligence Community) or the Federal Bureau of Investigation received any complaints regarding the application or implementation of Section 207 of the USA-Patriot Act? If so, please describe the nature and disposition of any such complaint.**

**Response:**

The DOJ OIG is required under section 1001 of the USA PATRIOT Act to report to Congress every six months on allegations received by the OIG alleging abuses of civil rights or civil liberties by DOJ employees. The OIG issued its fifth report under section 1001 in September 2004.

The OIG has advised that, with the possible exception of the pending Mayfield investigation, none of the complaints submitted to the OIG alleging misconduct by employees of the Department has related to the use of a provision of the USA PATRIOT Act. Additionally, the FBI's Inspection Division, which reviews allegations of FBI misconduct, is aware of no complaints with respect to the FBI's application or implementation of this section.

**d. Based upon the application of this provision of law during the period since its passage, are there changes to this statute which the Congress should consider?**

**Response:**

None at this time.

**87. Section 209 of the USA-Patriot Act clarified the law with regarding the applicability of criminal search warrants to voice mail. This question pertains to application of this provision since its passage.**

**a. How many such search warrants have been issued since passage of this act?**

**Response:**

The FBI does not collect or maintain statistics concerning the types of search warrants issued in FBI investigations, including those seeking access to voice mail. Because federal search warrants are requested by U.S. Attorneys' Offices and issued by U.S. District Courts, these statistics may be maintained by one or both of those offices.

**b. In such cases, have there been any instances in which a wiretap, as opposed to a search[ ] warrant[,] would not have been supported by the facts asserted in support of the search warrant.**

**Response:**

This information is unavailable, as indicated above. It is clear, however, that the support needed for a federal wiretap is considerably greater than that required for a search warrant.

**c. Has the Department of Justice or the Federal Bureau of Investigation received any complaints regarding the application or implementation of Section 209 of the USA-Patriot Act? If so, please describe the nature and disposition of any such complaint.**

**Response:**

A private citizen who has lodged numerous complaints against the FBI, all of which have been determined to be unfounded pursuant to appropriate inquiry, complained that she was a former FBI employee whose home, vehicles, telephone, and internet had been subject to "aggressive surveillance" since August 2000. FBI investigation revealed that the complainant was, in fact, not a former FBI employee and that the FBI had conducted no surveillance of her for any reason. Based on these findings, this matter was closed by the FBI in July 2003. The FBI has construed this as a complaint with respect to both Section 209 and 217 of the USA PATRIOT Act.

**d. Based upon the application of this provision of law during the period since its passage, are there changes to this statute which the Congress should consider?**

**Response:**

The FBI is not aware of any substantive changes to this provision warranting Congressional consideration. Section 209 is, however, currently scheduled to expire at the end of 2005, and the FBI strongly supports making this provision permanent. Section 209 allows investigators to use court-ordered search warrants to obtain voice-mail messages held by a third party provider when supported by probable cause. Previously, the Electronic Communications Privacy Act (ECPA), 18 U.S.C. 2703, allowed law enforcement authorities to use search warrants to gain access to stored electronic communications such as e-mail, but not stored wire communications such as voice-mail. Instead, the wiretap statute, 18 U.S.C. 2110(1), governed access to stored wire communications, requiring law enforcement officers to use wiretap orders to gain access to unopened voice-mail. This resulted in voice-mail messages being treated differently than e-mail messages. Voice-mail messages are also treated differently than answering machine messages inside a home, access to which requires a search warrant, because answering machine messages are not regulated under the wiretap statute. Section 209 of the USA PATRIOT Act eliminates the disparate treatment of similar information. If this section is sunsetted, voice-mail messages will again be treated in a different manner than answering machine messages and stored e-mail information beginning in 2006.

**88. Section 212 of the USA-Patriot Act permits communications service providers to provide customer records or the content of customer communications to the FBI in an emergency situation. This question pertains to application of this provision since its passage, and to all instances, not only to terrorism investigations.**

**a. In how many cases has this provision been used? Please provide a short description of each such case to the Committee.**

**Response:**

Service providers have voluntarily provided information on at least 141 occasions under this provision. Such disclosures have often included both e-mail content and associated records. Several of these disclosures have directly supported terrorism cases under the emergency of a possible pending attack. For example, this provision has been used to obtain access to e-mail accounts used by terrorist groups to discuss various terrorist attacks. It has also been used to respond quickly to bomb and death threats, as well as in an investigation into a threat to a high ranking foreign official. This provision has additionally been used to locate kidnaping victims and to protect children in child exploitation cases. In one kidnaping case involving the abduction of a 14-year-old girl, reliance on this



provision allowed the FBI to quickly locate and rescue the child and to identify and arrest the perpetrator. Because of this provision, additional harm to the girl was prevented and she was returned to her family in a matter of hours.

Because many international service providers are located within the United States (such as Hotmail and AOL), Legal Attachés have used this provision to assist foreign law enforcement officials with similar emergencies, such as death threats on prosecutors and other foreign officials. Where time is of the essence, giving service providers the option of revealing this information without a court order or grand jury subpoena is crucial to receiving the information quickly and preventing loss of life or serious injury.

Additional examples are provided in DOJ's July 2004 "Report from the Field: The USA PATRIOT Act at Work."

**b. In any such case have there been any cases in which, except for the time constraints imposed by the emergency situation, a conventional wiretap or search warrant, would not have been supported by the facts available to the Government at the time of the emergency request? If so, please describe such situations.**

**Response:**

We are aware of no such circumstances. However, it is important to recognize that the information that may be disclosed under this emergency authority is limited to the contents of communications that are in electronic storage and records associated with customers or subscribers. Given this limitation, a conventional wiretap would generally not apply, and a search warrant would be required only for the contents of communications in 'electronic storage' (e.g., incoming email not yet retrieved by the subscriber) less than 181 days old. Emergency authority is appropriate for the disclosure of information held by a third party and, to the extent the information is constitutionally protected, disclosure of the information under exigent circumstances is entirely consistent with the emergency exception to the warrant requirement of the Fourth Amendment.

**c. Has the Department of Justice or the Federal Bureau of Investigation received any complaints regarding the application or implementation of Section 212 of the USA-Patriot Act? If so, please describe the nature and disposition of any such complaint.**

**Response:**

The DOJ OIG is required under section 1001 of the USA PATRIOT Act to report to Congress every six months on allegations received by the OIG alleging abuses of civil rights or civil liberties by DOJ employees. The OIG issued its fifth report under section 1001 in September 2004.

The OIG has advised that, with the possible exception of the pending Mayfield investigation, none of the complaints submitted to the OIG alleging misconduct by employees of the Department has related to the use of a provision of the USA PATRIOT Act. Additionally, the FBI's Inspection Division, which reviews allegations of FBI misconduct, is aware of no complaints with respect to the FBI's application or implementation of this section.

**d. Based upon the application of this provision of law during the period since its passage, are there changes to this statute which the Congress should consider?**

**Response:**

There is currently a discrepancy between the emergency provisions applicable to contents and records that appears illogical and unjustified. Currently a provider is arguably required under 18 U.S.C. 2702(c)(4) to meet a higher burden for disclosing a record or other subscriber information than is required by § 2702(b)(7) for divulging the contents of a communication in electronic storage. Moreover, the entities to whom a provider may disclose are significantly more restricted for records than for content. The language in (b)(7) was enacted by Pub. L. 107-296 as part of the Homeland Security Act of 2002, with the objective that all entities with responsibility for ensuring our domestic security would have access to this information in an emergency. It does not appear that the discrepancies between the disclosure of content and records are supported by differing privacy interests inherent in the respective information or by other factors. Accordingly, reconciling these provisions would be appropriate.

**89. Section 214 of the USA-Patriot Act permits the use of FISA pen register/trap & trace orders with respect to electronic communications, and eliminates the requirement that such use be only in the context of a terrorist or espionage investigation. This question pertains to application of this provision since its passage, and to all instances, not only terrorism investigations.**

**a. In how many cases has this authority been used?**

**(i) How many of such cases were terrorism-related?**

**Response to a and a(i):**

The FBI does not maintain this information. It is, instead, maintained by DOJ's OIPR, to whom the FBI defers for response.

**b. Of the cases in which such authority was used, in how many was a subsequent application for a full surveillance order made pursuant to the FISA, or Chapter 19 of Title 18?**

**Response:**

The FBI does not track the number of pen registers that evolve into full FISA's.

**c. Has the Intelligence Community, Department of Justice, or Federal Bureau of Investigation developed regulations or directives defining the meaning of non-content communications? If such regulations or directives have been issued, please provide copies to the Committee.**

**Response:**

The FBI has not developed any such regulations or directives, nor is it aware that the IC or DOJ have issued guidance defining "non-content communications" in relation to the use of FISA pen register/trap and trace authorities.

**d. In your testimony you made reference to newly-created procedures by which the Federal Bureau of Investigation disseminates intelligence via "electronic intelligence reports" - is this the mechanism used for dissemination of material acquired pursuant to this section of the FISA?**

**Response:**

See response to Question 85b, above.

**(i) If so, how many such reports have been issued?**

**Response:**

See response to Question 85b(i), above.

**(ii) Has the Federal Bureau of Investigation developed procedures to ascertain the quality and value of such intelligence reports?**

**Response:**

See response to Question 85b(ii), above.

**90. Section 215 of the USA-Patriot [A]ct authorizes the Foreign Intelligence Surveillance Court to issue orders permitting FBI to access "tangible" items in the course of a terrorism or espionage investigation. The following questions pertain to the application of this provision since its inception.**

**a. How many times has this authority been used, and with what success?**

**Response:**

By letter of 12/23/04, the Department provided to the Committee the number of times, if any, authorities under section 1861 of the Foreign Intelligence Surveillance Act (FISA), as amended, had been approved by the Foreign Intelligence Surveillance Court. This semiannual report was submitted pursuant to section 1862(b) of the FISA, and covered the period 1/1/04 through 6/31/04.

**b. Has this provision been used to require the provision of information from a library or bookstore? If so, please describe how many times, and in what circumstances.**

**Response:**

The Department provides information pertaining to the operational use of authorities under section 1861 of the FISA to the Senate and House Intelligence Committees on a semiannual basis, pursuant to section 1862(a) of the FISA. The last semiannual report under this section was dated 12/23/04, and covered the period 1/1/04 through 6/31/04. It is our understanding that under applicable Senate Rules and procedures, all Senators are permitted to review this semiannual report upon request to the Senate Select Committee on Intelligence.

c. In your testimony you compared this provision with existing authority in the criminal context, noting that records such as library records are subject to a grand jury subpoena. However, in criminal cases the propriety and lawfulness of subpoenas are to some extent tested in the adversary process of a trial - how, in the context of the FISA, does such a check occur?

Response:

The checks on the use of the business record provision are numerous. First, requests for such orders must be approved by several authorities within the FBI and DOJ to ensure they comply with FISA requirements. In addition, however, business record requests must be approved by a FISA Court judge. FISA judges are part of an independent judiciary, appointed pursuant to Article III of the U.S. Constitution.

Business record orders require a showing that the record is relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities. "Authorized investigations" may only be initiated when consistent with Attorney General guidelines, so the existence of such an investigation and the relevance of the record to this investigation represent two "checks" on this authority. Under both the Attorney General guidelines and section 215 of the USA PATRIOT Act, such investigations may not be conducted solely on the basis of activities protected by the First Amendment.

Once an appropriate FBI authority determines that a business record order request is relevant to a properly authorized investigation, the request itself requires numerous layers of approval (as do requests for electronic surveillance, physical search, and pen register/trap and trace orders under FISA). At the FBI field level, such requests must be approved by the Supervisory Special Agent (SSA), the SAC or appropriate Assistant SAC, and the Chief Division Counsel. At the FBIHQ level, the request must be approved by an attorney in the National Security Law Branch, and signed by one of the several designated high-ranking FBI officials to whom certification authority has been delegated. Thereafter, the request is submitted to DOJ's OIPR, and must be approved by OIPR before it is presented to the FISA Court. When presented to the FISA Court, the FISA judge must determine that the request meets FISA requirements before issuing the order.

Lastly, section 215 imposes Congressional oversight by requiring the Attorney General to report to Congress annually on the FBI's use of the section.

**d. As of October 2004 the Department of Justice advised that this provision had not been used. If that is true, is there a necessity to maintain this provision in law? Why?**

**Response:**

The only instance when the Department has declassified the number of times section 215 has been used was on 9/18/03 – not in October 2004. At that time (September 2003), Attorney General Ashcroft indicated section 215 had never been used. However, section 215 requires the Department to transmit on a semi-annual basis a report informing Congress of the number of times section 215 has been used. The most recent report was dated 12/23/04.

The PATRIOT Act specifically protects Americans' First Amendment rights, and terrorism investigators have no interest in the library habits of ordinary Americans. Historically, however, terrorists and spies have used libraries to plan and carry out activities that threaten our national security, and it is important that we not permit these facilities to become safe havens for terrorist or other illegal activities. The PATRIOT Act permits those conducting national security investigations to obtain business records – whether from a library or any other business – with the permission of a federal judge.

**(i) With respect to the potential applicability of this section to libraries and bookstores, there has been some concern that the mere prospect of use of the statute has a "chilling effect" on the use of these facilities. Can this chilling effect be minimized, if not eliminated, by incorporating a higher threshold for use in the limited context of libraries and bookstores? If not, why not?**

**Response:**

In the context of this question, the FBI can initiate investigations of individuals or groups only under specific conditions articulated in the Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection (NSIG). Additionally, FBI guidelines place strict limits on the types of investigative activities that can be undertaken when investigations are opened, requiring, for example, that no investigation of a U.S. person may be conducted solely upon the basis of activities protected by the First Amendment to the Constitution.

Individuals' rights are additionally safeguarded by other authorities, such as Executive Order (E.O.) 12333, which is the primary authority for intelligence

activities conducted by the IC. E.O. 12333 establishes goals for the collection of intelligence information; assigns responsibilities among the various intelligence components; prescribes what information may be collected, retained, and disseminated; and prescribes or proscribes the use of specified techniques in the collection of intelligence information. As noted above, the NSIG establishes limits and requirements governing FBI international terrorism investigations with respect to foreign intelligence, CI, and intelligence support activities. Another important internal safeguard is the Intelligence Oversight Board (IOB), which reviews the FBI's practices and procedures relating to foreign intelligence and foreign CI, requiring the FBI to report violations of foreign CI or other guidelines designed in full or in part to ensure the protection of the individual rights of a U.S. person.

**e. In your testimony you made reference to newly-created procedures by which the Federal Bureau of Investigation disseminates intelligence via "electronic intelligence reports" - is this the mechanism used for dissemination of material acquired pursuant to this section of the FISA?**

**Response:**

The IIR is the mechanism by which the FBI disseminates raw intelligence information to the Intelligence, Defense, and law enforcement communities. The intelligence information contained in these IIRs is information generally derived from FBI operations, investigations, or sources. Intelligence information acquired pursuant to Section 215 of the USA PATRIOT Act could be disseminated via an IIR in appropriate circumstances. Between August 2002 and August 2004, the FBI has disseminated approximately 3,860 terrorism-related IIRs.

**(i) If so, how many such reports have been issued?**

**Response:**

None of the information contained in the 3,860 terrorism-related IIRs disseminated between August 2002 and August 2004 was acquired pursuant to section 215 of the USA PATRIOT Act.

**(ii) Has the Federal Bureau of Investigation developed procedures to ascertain the quality and value of such intelligence reports?**

**Response:**

Although the FBI has procedures to evaluate the quality of intelligence reports, no reports have been disseminated which contained information acquired pursuant to section 215 of the USA PATRIOT Act.

**f. Has the Department of Justice, the Director of Central Intelligence (in his capacity as head of the Intelligence Community) or the Federal Bureau of Investigation received any complaints regarding the application or implementation of Section 215 of the USA-Patriot Act? If so, please describe the nature and disposition of any such complaint.**

**Response:**

The DOJ OIG is required under section 1001 of the USA PATRIOT Act to report to Congress every six months on allegations received by the OIG alleging abuses of civil rights or civil liberties by DOJ employees. The OIG issued its fifth report under section 1001 in September 2004.

The OIG has advised that, with the possible exception of the pending Mayfield investigation, none of the complaints submitted to the OIG alleging misconduct by employees of the Department has related to the use of a provision of the USA PATRIOT Act. Additionally, the FBI's Inspection Division, which reviews allegations of FBI misconduct, is aware of no complaints with respect to the FBI's application or implementation of this section.

**g. Based upon the application of this provision of law during the period since its passage, are there changes to this statute which the Congress should consider?**

**Response:**

The FBI has identified no need for change at this time.

**91. Section 217 of the USA-Patriot Act authorizes, without court order, the interception of communications to and from a trespasser with a protected computer. This question pertains to the implementation of this provision since its passage.**

**a. How many times has the authority under this section been used, and with what success? Please provide descriptions of the circumstances where it has been used.**



**Response:**

While the FBI does not maintain statistics on the frequency with which the trespasser authority has been used, we can provide examples of some such cases.

Under this provision, the FBI was able to monitor the communications of an international group of "carders" (individuals who use and trade stolen credit card information). This group used chat rooms and fraudulent web sites, creating false identities to obtain e-mail accounts and then transmitting their communications through a computer that had been "hacked" and set up to operate as their proxy server. A proxy server changes an Internet user's original Internet protocol (IP) address to that of the proxy server so that only the proxy server knows the true point of origin. The owner of the hacked computer was not aware that it was being used as a proxy server, and considered all individuals using the system as a proxy server to be trespassers. The owner provided the FBI with consent to monitor the communication ports solely used by the trespassers, and this monitoring led to the subject's true identity. The subject was indicted in September 2003. Without this authority to monitor, the real identities of the trespassers could easily have remained anonymous.

In another example, a former employee was suspected of illegally accessing a company's e-mail system to gain inside information regarding company concepts and client information, as well as privileged information regarding legal proceedings between the company and the former employee. The computer intruder used a variety of means to access the system, including wireless modems in laptops and hand-held Blackberry devices, making it more difficult to identify the intruder and to link the computer intrusions to the former employee. The victim company authorized the FBI to monitor the intruder's communications with and through its computer systems.

In another case, a computer-intruder obtained control of a school's network and reconfigured it to establish additional IP addresses that were separate and distinct from those used by the school. This allowed hackers, and others using the Internet who did not want to be located, to jump through the school's system before committing their illegal acts. Monitoring accomplished pursuant to the school's consent resulted in the FBI's identification of over 200,000 different IP addresses using the school system as a proxy to further illegal activity such as fraud, computer intrusions, and spamming.

As these cases make clear, this authority is critical not only to the FBI's ability to identify criminals who engage in computer intrusions but also its ability to

identify and investigate additional criminal activities conducted through victims' computers.

**b. Section 217(2)(I) requires authorization by the owner of the computer before the section can be applied. Can this authorization be withdrawn or limited by the owner of the computer? If so, how and in what circumstances?**

**Response:**

Yes. As with any form of consent, which must be freely and voluntarily given to be valid, the consenting party has the right to terminate the consent at any time. The FBI encourages the use of a written consent form containing an express acknowledgment by the consenting owner or operator that states: "I understand my right to refuse authorization for interception and have accordingly given this authorization freely and voluntarily."

**c. Has the Department of Justice, the Director of Central Intelligence (in his capacity as head of the Intelligence Community) or the Federal Bureau of Investigation received any complaints regarding the application or implementation of Section 217 of the USA-Patriot Act? If so, please describe the nature and disposition of each such complaint.**

**Response:**

See response to Question 87c, above.

**92. Section 218 of the USA-Patriot Act created the so-called "significant purpose" test for applications pursuant the FISA, clarifying the law to recognize that in many cases such surveillance may implicate both a law enforcement and an intelligence interest. This question pertains to the implementation of this provision since its passage.**

**a. Please provide the Committee with specific examples, in unclassified form if possible, of cases in which both law enforcement and intelligence interests were "significant."**

**Response:**

As indicated in the July 2004 DOJ publication entitled, "Report from the Field: The USA PATRIOT Act at Work," the removal of the "wall" played a crucial role in the Department's successful dismantling of a Portland, Oregon, terror cell, popularly known as the "Portland Seven." Members of this terror cell had

attempted to travel to Afghanistan in 2001 and 2002 to take up arms with the Taliban and al Qaeda against United States and coalition forces fighting there. Law enforcement agents investigating that case learned through an undercover informant that, before the plan to go to Afghanistan was formulated, at least one member of the cell, Jeffrey Battle, had contemplated attacking Jewish schools or synagogues, and had even been casing such buildings to select a target for such an attack. By the time investigators received this information from the undercover informant, they suspected that a number of others were involved in the Afghanistan conspiracy. While several of these other individuals had returned to the United States from their unsuccessful attempts to reach Afghanistan, investigators did not yet have sufficient evidence to arrest them. Before the USA PATRIOT Act, prosecutors would have faced a dilemma in deciding whether to arrest Battle immediately. If prosecutors had failed to act, lives could have been lost through a domestic terrorist attack; if prosecutors had arrested Battle in order to prevent a potential attack, the other suspects in the investigation would undoubtedly have scattered or attempted to cover up their crimes. Because of sections 218 and 504 of the USA PATRIOT Act, however, FBI agents could conduct FISA surveillance of Battle to detect whether he had received orders from an international terrorist group to reinstate the domestic attack plan on Jewish targets, and could keep prosecutors informed as to what they were learning. This gave prosecutors the confidence not to arrest Battle prematurely, but instead to continue to gather evidence on the other cell members. Ultimately, prosecutors were able to collect sufficient evidence to charge seven defendants and then to secure convictions and prison sentences ranging from three to eighteen years for the six defendants taken into custody. Charges against the seventh defendant were dismissed after he was killed in Pakistan by Pakistani troops on 10/3/03.

DOJ shared information pursuant to sections 218 and 504 before indicting Sami al-Arian and several co-conspirators on charges related to their involvement with the Palestinian Islamic Jihad (PIJ). PIJ is alleged to be one of the world's most violent terrorist organizations, responsible for murdering over 100 innocent people, including Alisa Flatow, a young American killed in a bus bombing near the Israeli settlement of Kfar Darom. The indictment states that al-Arian served as the secretary of the PIJ's governing council ("Shura Council"). He was also identified as the senior North American representative of the PIJ. Sections 218 and 504 of the USA PATRIOT Act enabled prosecutors to consider all evidence against al-Arian and his co-conspirators, including evidence obtained pursuant to FISA that provided the necessary factual support for the criminal case. By considering the intelligence and law enforcement information together, prosecutors were able to create a complete history for the case and put each piece of evidence in its proper context. This comprehensive approach was essential to prosecutors' ability to build their case and pursue the proper charges.

Prosecutors and investigators also used information shared pursuant to sections 218 and 504 of the USA PATRIOT Act in investigating the defendants in the so-called "Virginia Jihad" case. This prosecution involved members of the Dar al-Arqam Islamic Center, some of whom trained for jihad in Northern Virginia by participating in paintball and paramilitary training or traveled to terrorist training camps in Pakistan or Afghanistan between 1999 and 2001. These individuals are associates of a violent Islamic extremist group known as Lashkar-e-Taiba (LET), which primarily operates in Pakistan and Kashmir and has ties to the al Qaeda terrorist network. As the result of an investigation that included the use of information obtained through FISA, prosecutors were able to bring charges against several individuals. Nine of these defendants have received sentences ranging from four years to life imprisonment (six of these sentences were pursuant to guilty pleas and three were contrary to their pleas; charges have included conspiracy to levy war against the United States and conspiracy to provide material support to the Taliban).

Information sharing between intelligence and law enforcement personnel made possible by sections 218 and 504 of the USA PATRIOT Act was also pivotal in the investigation of two Yemeni citizens, Mohammed Ali Hasan Al-Moayad and Mohshen Yahya Zayed, who were charged in 2003 with conspiring to provide material support to al Qaeda and HAMAS. Based upon information obtained through an FBI undercover investigation, the complaint alleges that Al-Moayad had boasted that he had personally handed Usama Bin Laden \$20 million from his terrorist fund-raising network and that Al-Moayad and Zayed had flown from Yemen to Frankfurt, Germany, in 2003 with the intent to obtain \$2 million from a terrorist sympathizer (portrayed by a confidential informant) who wanted to fund al Qaeda and HAMAS. During their meetings, Al-Moayad and Zayed specifically promised the donor that his money would be used to support HAMAS, al Qaeda, and any other mujahideen, and "swore to Allah" that they would keep their dealings secret. Al-Moayad and Zayed were extradited to the United States from Germany in November 2003 and are currently awaiting trial.

Sections 218 and 504 were also used to gain access to intelligence that facilitated the indictment of Enaam Arnaout, the Executive Director of the Illinois-based Benevolence International Foundation (BIF). Arnaout conspired to fraudulently obtain charitable donations in order to provide financial assistance to Chechen rebels and organizations engaged in violence and terrorism. Arnaout had a long-standing relationship with Usama Bin Laden, and used his charities both to obtain funds for terrorist organizations from unsuspecting Americans and to serve as a channel for people to contribute money knowingly to such groups. Arnaout pled guilty to a racketeering charge, admitting that he diverted thousands of dollars from BIF to support Islamic militant groups in Bosnia and Chechnya. He was sentenced to over 11 years in prison.

The broader information sharing and coordination made possible by sections 218 and 504 of the USA PATRIOT Act assisted the San Diego prosecution of several persons involved in an al Qaeda drugs-for-weapons plot, which culminated in several guilty pleas. Two defendants admitted that they had conspired to distribute approximately five metric tons of hashish and 600 kilograms of heroin originating in Pakistan to undercover United States law enforcement officers. Additionally, they admitted that they had conspired to receive, as partial payment for the drugs, four "Stinger" anti-aircraft missiles that they then intended to sell to the Taliban, an organization they knew at the time to be affiliated with al Qaeda. The lead defendant in the case is currently awaiting trial.

Sections 218 and 504 were also critical in the successful prosecution of Khaled Abdel Latif Dumeisi, who was convicted by a jury in January 2004 of illegally acting as an agent of the former government of Iraq and of two counts of perjury. Before the Gulf War, Dumeisi passed information on Iraqi opposition members located in the United States to officers of the Iraqi Intelligence Service stationed in the Iraqi Mission to the United Nations. During this investigation, intelligence officers conducting surveillance of Dumeisi pursuant to FISA shared information with law enforcement agents and prosecutors investigating Dumeisi. Through this coordination, law enforcement agents and prosecutors learned from intelligence officers that an April 2003 telephone conversation between Dumeisi and a co-conspirator corroborated evidence that Dumeisi was acting as an agent of the Iraqi government, providing a compelling piece of evidence at Dumeisi's trial.

**b. Has the Department of Justice, the Director of Central Intelligence (in his capacity as head of the Intelligence Community) or the Federal Bureau of Investigation received any complaints regarding the application or implementation of Section 218 of the USA-Patriot Act? If so, please describe the nature and disposition of each such complaint.**

**Response:**

The Department's Office of the Inspector General (OIG) is required under section 1001 of the USA PATRIOT Act to report to Congress every six months on allegations received by the OIG alleging abuses of civil rights or civil liberties by DOJ employees. The OIG issued its fifth report under section 1001 in September 2004.

The OIG has advised that, with the possible exception of the pending Mayfield investigation, none of the complaints submitted to the OIG alleging misconduct by employees of the Department has related to the use of a provision of the USA

PATRIOT Act. Additionally, the FBI's Inspection Division, which reviews allegations of FBI misconduct, is aware of no complaints with respect to the FBI's application or implementation of this section.

c. Based upon the application of this provision of law during the period since its passage, are there changes to this statute which the Congress should consider?

**Response:**

The FISA Court of Review has made clear that the "significant purpose" standard is constitutional. Accordingly, additional changes are unnecessary.

**93. Section 220 of the USA-Patriot Act, "Nationwide Service of Search Warrants for Electronic Evidence" allows for the execution of a search warrant seeking electronic data anywhere in the country. This question pertains to the implementation of this provision since its passage.**

a. In how many cases has this authority been used?

**Response:**

While the FBI does not require or maintain centralized statistics on the use of search warrants, Field Offices indicate that they have routinely relied on this provision (codified at 18 U.S.C. 2703(a)) and can safely estimate that, nationwide, this search authority has been used at least 100 times since its passage.

In section 220 of the USA PATRIOT Act, Congress adapted federal law to changing technology by allowing courts to order the release of stored communications through a search warrant valid in another specified judicial district. The ability to obtain this information with greater efficiency has proven invaluable in numerous cases, including: several terrorism investigations (such as the Virginia Jihad case described above and a complex terrorism financing case in which it was used to obtain a subject's e-mail related to a 7/4/02 shooting at Los Angeles International Airport); child pornography cases in which it is used to obtain information from ISPs regarding those trading sexually exploitive images of children; investigations of "carders" (those who use and trade stolen credit card information); and numerous investigations into Internet sales of counterfeit products, which have led to several indictments and the seizure of bank and financial accounts.

Child pornography cases highlight the benefit of Section 220, because the ability to obtain a search warrant in the jurisdiction of a child pornography investigation rather than in the jurisdiction of the ISP is critical to the success of a complex, multi-jurisdictional child pornography case. In the absence of section 220, law enforcement agents would either have to spend hours briefing other agents across the country so they could obtain warrants in those jurisdictions, or travel hundreds or thousands of miles to present warrant applications to local magistrate judges. Without Section 220, one of two things would often occur in light of limited law enforcement resources: either the scope of the investigation would be narrowed or the case would be deemed impractical at the outset and dropped.

The following case, included in DOJ's July 2004 "Report from the Field: The USA PATRIOT Act at Work," provides an additional example of the benefits afforded by Section 220. A man, armed with a sawed-off shotgun, abducted his estranged wife and sexually assaulted her. Then, after releasing his wife, he fled West Virginia in a stolen car to avoid capture. While in flight, he contacted cooperating individuals by e-mail using an Internet service provider (ISP) located in California. Using the authority provided by section 220, investigators in West Virginia were able to obtain an order from a federal court in West Virginia for the disclosure of information regarding the armed fugitive's e-mail account, including the California ISP. Within a day of the order's issuance, the ISP released information revealing that the fugitive had contacted individuals from a public library in a small town in South Carolina. The very next day, Deputy U.S. Marshals went to the town and noticed a carnival set up next to the public library. Because they were aware that the fugitive had previously worked as a carnival worker, the Deputy Marshals went to the carnival and discovered the stolen car, arresting the fugitive as he approached the car. He later pled guilty in state court and was sentenced to imprisonment for 30 years. In this case, the fast turn-around on the order for information related to the fugitive's e-mail account, made possible by section 220 of the USA PATRIOT Act, was crucial to his capture.

Section 220 has also made the process of obtaining a warrant for ISP information much more efficient. Before the USA PATRIOT Act, judicial districts that are home to large ISPs were inundated with search warrant requests for electronic evidence. For example, the U.S. Attorney's Office in Alexandria, Virginia, was receiving approximately 10 applications each month from United States Attorney's Offices in other districts for search warrants for the records of an ISP located there. For each of these applications, an Assistant United States Attorney in Virginia and a law enforcement agent in the district had to learn all the details of another district's investigation in order to present an affidavit to the court in support of the search warrant application. Because of section 220, however, these attorneys and Agents can now spend their time on local cases and investigations rather than on learning the details of unrelated investigations being worked

through distant offices. Given the short time for which ISPs typically retain records, this provision has enabled the FBI to obtain critical information that may otherwise have been lost or destroyed in the ordinary course of the ISP's business. Section 220 also results in a more efficient use of judicial resources by allowing the judge with jurisdiction over the offense to issue the warrant and retain oversight over the search.

**b. Has the Department of Justice or the Federal Bureau of Investigation received any complaints regarding the application or implementation of Section 220 of the USA-Patriot Act? If so, please describe the nature and disposition of each such complaint.**

**Response:**

The DOJ OIG is required under section 1001 of the USA PATRIOT Act to report to Congress every six months on allegations received by the OIG alleging abuses of civil rights or civil liberties by DOJ employees. The OIG issued its fifth report under section 1001 in September 2004.

The OIG has advised that, with the possible exception of the pending Mayfield investigation, none of the complaints submitted to the OIG alleging misconduct by employees of the Department has related to the use of a provision of the USA PATRIOT Act. Additionally, the FBI's Inspection Division, which reviews allegations of FBI misconduct, is aware of no complaints with respect to the FBI's application or implementation of this section.

**c. Based upon the application of this provision of law during the period since its passage, are there changes to this statute which the Congress should consider?**

**Response:**

No. The FBI requests only that the provision be preserved.

**94. Section 223 of the USA-Patriot Act creates a cause of action for willful violations of Title III's electronic surveillance procedures. Have any such lawsuits been brought? If so, please provide details of each such case.**

**Response:**

No such lawsuits have been brought.



**95. Section 225 of the USA-Patriot Act provides immunity for those who aid in the execution of a FISA order. Has such immunity been invoked? If so, please describe any such case.**

**Response:**

No. Immunity has not been claimed under this section with respect to FBI investigations in either the civil or criminal context.

**96. The following question pertains to surveillance conducted pursuant to the FISA.**

**a. What is the backlog on processing of intercepts? What is the average time between interception and first monitoring.**

**b. What percentage of intercepts that are not in English are translated within 24 hours? A week?**

**c. How many hours of FISA intercepts remain untranslated as of May 20, 2004?**

**Response to a through c:**

FBI Director Mueller has made clear his interest in having all material derived from the FBI's use of FISA authority reviewed and analyzed as quickly as possible. Since the majority of this material is in languages other than English, FBI Language Services Section personnel meet with the FBI's National FISA Manager and other management officials every two weeks to discuss national operational priorities and the most effective utilization of finite linguist resources. The operational plan established by this meeting is modified almost daily based on ever-shifting investigative priorities. These tactics ensure that all of the highest priority intelligence collected in a foreign language is reviewed immediately and that any outstanding work is limited to matters assigned a lower relative priority.

The FBI currently has sufficient translation capacity to promptly address all translation needs with respect to its highest priority, CT operations, often within 12 hours. While there are instances in which the FBI is not able to address translation needs as quickly as it would like, such as when the language or dialect involved is initially unidentifiable, this usually pertains to lower priority matters.

Conventional digital systems used to collect FISA-derived materials were not designed to measure the average time between intercept and initial monitoring. Recognizing the tactical value of having such aging reports for command and control purposes, a nationally integrated FISA statistical collection and reporting system has been developed and is undergoing a test and evaluation process to validate the mapping of meta data. This system should be fully functional by the end of calendar year 2004. It is clear, however, based on information provided by FBI field office managers, that the vast majority of communications in a foreign language relating to terrorism operations are being afforded full review by a qualified linguist within, at most, a few days of collection.

**d. Please describe the process of indexing and retrieving FISA material.**

**Response:**

Intelligence summaries from FISA intercepts are indexed and archived according to strict electronic surveillance (ELSUR) rules that make these summaries part of the official FBI record and allow these records to be searched in the Field Offices where the cases reside. Although recent progress has been made in creating an electronic archive of CI material that can be searched by authorized users fieldwide, CT summaries from FISA audio intercepts are not searchable in a central database at this time. The phased deployment of the ELSUR Data Management System (EDMS), starting in FY 2005, will make all intelligence summaries from FISA intercepts available in a searchable archive.

**e. In the past 5 years, has there been a review or audit of the accuracy of FBI translations of intercepted or seized foreign language material?**

**Response:**

Historically, translation reviews were normally conducted by field office managers on a semi-annual basis in conjunction with a linguist's performance appraisal rating. In order to standardize this procedure, the FBI's Language Services Section implemented minimum quality control standards and guidelines and assumed central management of the language services quality control program in January 2003. Quality control program guidelines stipulate which linguists' translations must be reviewed and at what intervals. The guidelines also identify those materials that must always be reviewed prior to dissemination.

**Questions Posed by Senator Feingold**

**FBI Role in Iraq**

97. a. How many special agents, translators, and other FBI employees have been assigned to work in Iraq since March 2003 and how many are currently there?

**Response:**

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

b. Where were these agents, translators, and other employees assigned before they were sent to Iraq?

**Response:**

They were assigned to many of the FBI's offices, both in the field and at FBIHQ.

c. How many of these agents, translators, and other employees were working in the United States on terrorism cases?

**Response:**

15 percent of the FBI employees sent to Iraq were working on terrorism cases prior to that deployment.

**FBI DNA Lab**

98. The U.S. Department of Justice and Jacqueline Blake, a former biologist at the FBI DNA laboratory, recently entered into a plea agreement. Blake pled guilty to authoring and submitting over 100 reports containing false statements regarding DNA analysis she performed during a 2-1/2 year period from 1999 to 2002.

a. According to a Justice Department press release, the FBI has retested evidence in many of Blake's cases and has concluded that her false statements did not affect the outcome of any of the criminal cases in which she was involved. I assume that the FBI has notified the prosecutors in those cases. Has the FBI notified the courts and defense attorneys in each case in which Blake's falsified reports were involved? If not, why not?

**Response:**

In April 2002, DNA Analysis Unit I (DNAU I) discovered that one of its biological laboratory technicians, Jacqueline Blake, had systematically and repeatedly violated the Unit's standard operating procedure (SOP) by failing to process to completion mandatory negative control samples within the Short Tandem Repeat (STR) process. Ms. Blake worked under the direction of a qualified DNA examiner, who relied upon the data generated by Ms. Blake for the development and issuance of the corresponding reports of examination. Promptly following this discovery, the FBI reported the violation to the DOJ OIG through the FBI's Office of Professional Responsibility (OPR).

The DNAU I determined that Ms. Blake had inaccurately represented that negative control samples had been utilized properly, and had been involved in the processing of 103 case submissions. OIG attorneys obtained an affidavit from Ms. Blake, in which she acknowledged willful misconduct. Ms. Blake subsequently pled guilty to falsifying documentation on which DNAU I examiners relied for interpretation and reporting purposes.

Since the discovery of Ms. Blake's misconduct, the FBI Laboratory has made it a priority to notify those law enforcement entities and prosecutors affected by Blake's misconduct. Because these entities represent the entry point of any laboratory results into the criminal justice system, the FBI believes this notification will ensure that Blake's actions, and the FBI Laboratory's response to these actions, are properly disseminated. In addition to prosecution and law enforcement officials, all agencies that received DNA reports in which Ms. Blake performed STR processing were also notified of Blake's failure to complete testing of the negative control samples, rendering the written report unsuitable for investigation or prosecution purposes. This notification included telephonic, mail, and facsimile contact. In the majority of these cases, no judicial action had occurred and no prosecutor had been assigned, largely because most of the reported cases did not have subjects identified for comparison. Where prosecutors had been assigned, they were notified and clearly informed of their disclosure obligations.

**b. As you know, after complaints and calls for reform in the 1990s and after a Justice Department Inspector General report in 1997 concluded that the lab's scientists engaged in bad science and gave inaccurate testimony, the FBI conducted an extensive overhaul of its DNA lab, which included implementing a peer review system to prevent the exact kind of situation that has occurred here. Please describe that peer review system and explain how and why it failed in this case.**

**Response:**

While the 1997 OIG report did not address the FBI's DNA analysis, a May 2004 OIG report does address this issue. Since the establishment of DNAUI in 1988, it has routinely applied two forms of review on every case, including a technical review to ensure the completeness and accuracy of the interpretive data and conclusions and an administrative review to check for overall content and adherence to unit reporting policies. Ms. Blake's misconduct went undetected primarily because her willful falsification of case file documentation deceived the technical review process and enabled her to conceal her misconduct. As indicated below, the FBI Laboratory is implementing procedural changes to prevent such deception in the future.

**c. As a result of the peer review system's failure in this case, what is the FBI doing to revise its system to prevent this kind of breakdown from happening again?**

**Response:**

As previously indicated, the technical or peer review process did not fail, but rather was compromised by Ms. Blake's falsification of documents. Upon discovery of this misconduct, the DNAUI immediately expanded the scope of its peer review process to specifically address Ms. Blake's breach of integrity. The peer review process now requires documentation demonstrating verification of the complete processing of all negative control samples, and this documentation is verified by the examiner of record, the peer reviewer, and the administrative reviewer. Additionally, the DNAUI is implementing procedural changes to further augment its quality practices, consistent with the OIG's May 2004 recommendations regarding the protocols and practices of the FBI's nuclear DNA laboratory.

**d. I understand that the Inspector General has been pushing the FBI to conduct regular audits of state and local labs that place DNA evidence into the national DNA registry. What steps are you taking to improve oversight of state and local labs to ensure that labs placing information in the national registry are placing accurate information?**

**Response:**

The FBI Laboratory's interim plan for review of the accuracy, completeness, and acceptability of DNA profiles in the National DNA Index System (NDIS) will consist of having FBI auditors evaluate the classification, accuracy, and

completeness of the DNA profiles when performing case file reviews during Quality Assurance audits. The Audit document has been revised to include a reminder that FBI auditors must conduct this review, and a form has been prepared to record review results. Additional guidance for NDIS participants and auditors on the standards for including DNA profiles in NDIS is contained in the CODIS Administrator's Handbook. The FBI is also creating positions for CODIS auditors, who will develop a permanent plan for the review of DNA profiles uploaded to NDIS. These positions have been approved and the hiring process has begun.

U.S.S. Cole Bombing Investigation

**99. In October 2000, the U.S.S. Cole was attacked during its stop in the harbor of Aden, Yemen, resulting in the deaths of 17 crew members, including one of my constituents, and wounding 39 others. On April 11, 2003, 10 men, including men suspected of involvement in the Cole bombing, escaped from a prison in Yemen. I understand that the suspects have now been recaptured.**

**a. What steps did the FBI take to determine how the suspects escaped? Has the FBI determined who facilitated their escape?**

**Response:**

Although an FBI Legal Attaché reported to Sana'a in March 2004, there was no FBI Legal Attaché assigned in Yemen at the time of the April 2003 escape. Therefore, the FBI obtained information related to this escape from the U.S. Embassy in Sana'a and other members of the IC.

Additional information with respect to this question is classified and is, therefore, provided separately.

**b. What steps have been taken by the FBI to evaluate the security of the detention facility in which these suspects are currently being held?**

**Response:**

The defendants in the U.S.S. Cole trial are being held in a secure facility in Sana'a, Yemen, rather than in the Aden facility from which Al-Badawi and Al-Quso escaped. While the FBI team in Sana'a is working closely with Yemeni authorities with respect to this trial, we are not in a position to assess the security

of this detention facility. Information related to the security of Yemeni detention facilities is better addressed by the U.S. Embassy in Sana'a.

c. Has the FBI interviewed the suspects since they have been recaptured?

**Response:**

Upon the re-capture of Al-Badawi and Al-Quso, the FBI requested authority to interview them, particularly with respect to the April 2003 escape. These suspects were then in the custody of the Yemen Political Security Organization (PSO), which ultimately authorized these interviews. By that time, however, Al-Badawi and Al-Quso had been transferred from the PSO's custody to that of the Prosecutor General's Office for prosecution. The trial of Al-Badawi, Al-Quso, and other U.S.S. Cole defendants began on 7/7/04 in Sana'a, Yemen.

d. What is the status of the FBI's investigation of these suspects and the Justice Department's plans to pursue a prosecution?

**Response:**

The FBI's investigation into the attack on the U.S.S. Cole is ongoing. In May 2003, Al-Badawi and Al-Quso were indicted by a Federal Grand Jury in the Southern District of New York for their roles in the Cole attack. In April 2004, the FBI requested the renditions of Al-Badawi and Al-Quso via diplomatic note. The Yemen Ministry of Foreign Affairs (MFA) responded that "the rendition request must be supported by legal documents in order to look into the matter according to Yemeni Law." Based on this reply, the Southern District of New York was asked for the necessary documents (such as the U.S.S. Cole indictment and arrest warrants for Al-Quso and Al-Badawi) so they can be provided to the MFA.

**Timika, Indonesia Investigation**

100. a. Please provide an update on the status of the FBI investigation into the murder of American citizens in Timika, Indonesia, on August 31, 2002.

**Response:**

The FBI developed sufficient evidence to obtain an indictment in U.S. Federal Court on 6/16/04. The subject charged with the 8/31/02 murders is Anthonius

Wamang, a member of the military branch of the Free Papua Movement, commonly known as OPM.

**b. Has the FBI been able to conduct all the interviews it desires to conduct without the presence of Indonesian military minders undermining the integrity of the interview? Has the FBI obtained access to all the evidence to which it wants access? Is the FBI encountering any obstructions to the investigation at all?**

**Response:**

The FBI is satisfied with the current level of cooperation from the Indonesian military (TNI). Recent cooperation by the TNI reflects a commitment to allowing the FBI direct access to some of their most sensitive human sources in a way that will permit effective interviews by FBI Agents.

**c. What are the ramifications for the FBI's investigation of statements made by Indonesian military officers who have commented to the press about what the FBI has concluded about TNI involvement?**

**Response:**

These comments by TNI officers, as well as unofficial statements by U.S. officials, dramatically affect the level of cooperation offered by those who perceive themselves as subjects of the investigation. These leaks also negatively affect the security of FBI investigators and individuals cooperating with the FBI.

**Brandon Mayfield Fingerprint Identification and Detention**

**101. On May 24<sup>th</sup>, a federal court dismissed the material witness proceeding against Brandon Mayfield, an attorney and former U.S. Army officer. In written submissions to the court and in public statements the FBI has admitted that the fingerprint of Mayfield was mistakenly matched to a fingerprint recovered at the scene of the May 11, 2004, Madrid train bombing.**

**a. When were Mayfield's fingerprints taken and when and why were they entered and maintained in the Integrated Automated Fingerprint Identification System (IAFIS)? If Mayfield's fingerprints were maintained in the IAFIS system because of his prior military service, what percentage of former members of the military currently have their fingerprints in IAFIS?**



**b. The FBI has stated that members of the Latent Print Unit (LPU) went to Madrid on two occasions to discuss the accuracy of the Mayfield fingerprint identification.**

**(i) What were the dates of the two trips to Madrid?**

**(ii) In addition to members of the LPU, who from the FBI or DOJ also traveled to Madrid on each of the trips?**

**(iii) During the first trip to Madrid, what specific information did the Spanish National Police provide to the FBI and DOJ about the accuracy and reliability of the Mayfield fingerprint identification?**

**(iv) As a result of the first trip to Madrid, what if any efforts were taken to confirm that Mayfield's fingerprints had been correctly identified?**

**c. The FBI has stated that an international panel of fingerprint experts will review the LPU examination in the Madrid bombing.**

**(i) Will the Spanish National Police be involved in this review?**

**(ii) What will be the scope of the review of the international panel?**

**(iii) Will the international panel be allowed to review the process leading up to the inclusion of Mayfield's fingerprints in the IAFIS system?**

**(iv) Will the results of the international review be made available to Congress?**

**d. According to court records, no criminal charges were ever filed against Mayfield. Instead, he was detained as a material witness. Why was Mayfield held as a material witness and not charged with any criminal conduct?**

**e. Mayfield has stated that he believes that his home was secretly searched before he was declared a material witness and detained. Prior to, or during his detention, was the Mayfield residence or office searched pursuant to a warrant under the Foreign Intelligence Surveillance Act (FISA) or a delayed notification search warrant? If the latter, please indicate (a) the basis for seeking delayed notice of the search warrant and (b) the time period requested and granted for delaying notice.**

**Response to a through e:**

As indicated above, the FBI will defer response during the pendency of the OIG and OPR reviews and the Mayfield lawsuit.

**Use of the USA PATRIOT Act**

**102. In October 2003, the Department reported that as of April 1, 2003, it had sought, and courts had ordered, delayed notice warrants 47 times.**

**a. As of the date of your response to these questions, or some reasonable recent date, how many times has the Department sought and received authorization to execute a delayed notification search since enactment of the PATRIOT Act?**

**Response:**

The FBI does not collect this information. However, we understand the Department has queried various U.S. Attorneys' Offices for this information and will forward it under separate cover as soon as it is compiled.

**b. How many of the delayed notification warrants issued since passage of the PATRIOT Act were granted because contemporaneous notification would have "seriously jeopardized an investigation"? For each such delayed notice warrant, please describe how granting contemporaneous notice would have seriously jeopardized the investigation and please indicate whether seriously jeopardizing the investigation was the sole basis or one of multiple grounds for delaying notice.**

**c. How many of the delayed notification warrants issued since passage of the PATRIOT Act were granted because contemporaneous notification would have "unduly delayed a trial"? For each such delayed notice warrant, please describe how requiring contemporaneous notice would have unduly delayed a trial and please indicate whether unduly delaying a trial was the sole basis or one of multiple grounds for delaying notice.**

**Response to b and c:**

This information was not collected in the EOUSA survey and is not otherwise available except through individual U.S. Attorney's Offices. Nevertheless, because these questions focus on the sufficiency of the grounds offered to justify a delay, it should be noted that a district court judge or magistrate must find "reasonable cause" to believe the grounds forwarded in the affidavit exist and are

sufficient to justify the delay. In addition, notice is only delayed; it is never eliminated. The searched party will, therefore, have the opportunity to challenge the validity and sufficiency of the reasons for delay and, if those reasons prove to be insufficient, to seek an appropriate remedy.

d. How many of the delayed notice warrants were issued with a (i) seven-day or less delay; (ii) 8 to 30 day delay; (iii) 31 to 60 day delay; and (iv) time period of 61 days or more and what were those time periods?

e. How many of the delayed notification warrants issued since the PATRIOT Act was passed were used in non-terrorism criminal matters?

f. Please provide the case name, docket number, and court of jurisdiction for each case in which a delayed notice warrant was issued since enactment of the PATRIOT Act.

Response to d through f:

This information was not collected in the EOUSA survey and is not otherwise available except through individual U.S. Attorney's Offices.

103. In September 2003, the U.S. Department of Justice disclosed that it had not yet used section 215 of the USA PATRIOT Act. On March 9, 2004, I sent a letter to the Attorney General asking him to clarify whether section 215 has been used since September 18, 2003. (Copy of letter attached.)

a. Please indicate whether section 215 has been used since September 18, 2003.

Response:

By letter of 12/23/04, the Department provided to the Committee the number of times, if any, authorities under section 1861 of the Foreign Intelligence Surveillance Act (FISA), as amended, had been approved by the Foreign Intelligence Surveillance Court. This semiannual report was submitted pursuant to section 1862(b) of the FISA, and covered the period 1/1/04 through 6/31/04.

b. If section 215 has been used, please describe how it has been used. How many U.S. persons and non-U.S. persons were targets of the investigation? Was the section 215 order served on a library, newsroom, or other First Amendment sensitive place? Was the product of the search used in a criminal prosecution?

**Response:**

The Department provides information pertaining to the operational use of authorities under section 1861 of the FISA to the Senate and House Intelligence Committees on a semiannual basis, pursuant to section 1862(a) of the FISA. The last semiannual report under this section was dated 12/23/04, and covered the period 1/1/04 through 6/31/04. It is our understanding that under applicable Senate Rules and procedures, all Senators are permitted to review this semiannual report upon request to the Senate Select Committee on Intelligence.

104. The Security and Freedom Ensured (SAFE) Act (S. 1709) would amend the roving wiretaps provision of the PATRIOT Act (section 206) by placing reasonable safeguards to protect the conversations of innocent Americans.

a. The SAFE Act would require the FBI to determine whether the target of the wiretap is present at the place being tapped. Since the FBI must already comply with this requirement when conducting roving wiretaps in criminal investigations (*see* 18 U.S.C. § 2518(11), (12)), why shouldn't Congress require the FBI to comply with this important requirement when conducting roving wiretaps in foreign intelligence investigations? Please explain.

**Response:**

The requirements of the SAFE Act are inconsistent with, and more restrictive than, the requirements applicable to roving wiretaps in criminal investigations. In criminal cases, roving wiretap orders are limited to "such time as it is reasonable to presume that the [target] is or was reasonably proximate" to the facility. 18 U.S.C. 2518(11)(b)(iv). This does not require a conclusive determination that the target is actually present at the time of interception, as the SAFE Act would require, but only a reasonable belief under the circumstances that the facility or place is being used by the target. An analogous requirement is already contained in the Foreign Intelligence Surveillance Act (FISA). Under FISA, the FBI must demonstrate probable cause to believe that "each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power." 50 U.S.C. 1805(a)(3)(B). In addition to these safeguards, both Title III and FISA require the use of procedures

to minimize the acquisition, retention, and dissemination of information concerning innocent persons.

As a practical matter, the standard required by the SAFE Act would preclude most, if not all, roving wiretaps under FISA. Frequently, it is impossible or impractical to ascertain a target's presence through physical observation. A limited review of the context and substance of intercepted communications may be the only means of confirming the target's presence, particularly when multiple, similar-sounding individuals are using the same device. This is especially true when the intercepted communications are in a foreign language. Under the SAFE Act, electronic surveillance could not be used to ascertain the presence of the target. Thus, roving FISA wiretaps would be limited to those circumstances in which the target's presence could be confirmed by physical observation.

**b. The SAFE Act would also require the FBI to identify either the target of the wiretap or the place to be wiretapped. For example, in the event that the FBI has a physical description of the target but does not know the identity of the target, the SAFE Act would allow the FBI to conduct a "John Doe" wiretap by identifying the facilities to be wiretapped. This is a sensible requirement to protect innocent Americans who are not the target of an investigation, while still allowing the FBI to conduct surveillance of suspected terrorists or spies. Why shouldn't Congress enact this prudent safeguard? Please explain.**

**Response:**

A "roving" wiretap is one linked to a particular investigative target, regardless of the facility being used by that individual. The purpose of the "roving" authority is to allow uninterrupted, court-ordered monitoring of the target, even when the target changes facilities to thwart surveillance. Thus, by definition, the facility or place at which a "roving" surveillance is directed cannot be known at the time the order is issued. The SAFE Act would preclude this type of uninterrupted surveillance of investigative targets who successfully conceal their identities.

Under current law, a FISA wiretap application must include "the identity, if known, or a description of the target of the electronic surveillance." 50 U.S.C. 1805(c)(1)(A). The SAFE Act would eliminate roving wiretaps in cases where the FBI is able to provide a description of the target, but has been unable to determine the target's identity.

The SAFE Act's limitation of the roving authority under FISA appears unwarranted because, even in cases where the target's identity is unknown, the FBI must still describe the individual target with sufficient specificity to demonstrate probable cause to believe "the target of the electronic surveillance is

a foreign power or an agent of a foreign power." 50 U.S.C. 1805(a)(3)(A). This probable cause requirement, which must be read together with the "description" requirement of 50 U.S.C. 1805(c)(1)(A), protects innocent Americans who are not the targets of investigations.

### Questions Posed by Senator Durbin

**105. You testified that terrorism prevention is the top priority of the Bureau and that resources have been diverted within the Bureau in support of this important effort. However, the fight against terrorism should not come at the cost of diminished law enforcement in critical areas such as criminal civil rights violations. Please discuss what resources if any have been diverted away from the FBI's Civil Rights Program since September 11, 2001.**

**Response:**

Immediately after 9/11/01, there was an increase in the FBI resources dedicated to address the surge in backlash hate crimes committed against Arab, Muslim, and Sikh Americans. Once these backlash hate crimes became less frequent, the resources dedicated exclusively to the investigation of civil rights matters decreased to the pre-9/11 level. In spite of this decrease in civil rights resources, the FBI's response in addressing civil rights matters has not diminished. The CRP is among the FBI's top 10 priorities, and appropriate resources have been allocated to it. When an office's resources available to address civil rights matters are strained, the SAC of that field office has the authority to pull resources from other, lower-priority programs to address civil rights matters. This has allowed the FBI to remain vigilant and focused on assigning appropriate resources to address violations of federal civil rights statutes when they occur.

**106. I commend the FBI for its effectiveness in investigating troublesome increases in hate crimes and human trafficking. After September 11, our nation witnessed a disturbing increase in hate crimes committed against individuals in the United States who appear to be of Muslim, Middle Eastern, and South Asian descent, and the FBI has effectively investigated this spike in hate crimes and provided valuable assistance to prosecutors. Similarly, the Department of Justice has vigorously prosecuted human trafficking cases, and the FBI has played an important role in investigating these barbaric crimes. However, the FBI is also the lead investigative component within the Department of Justice involving other important criminal civil rights violations, such as police misconduct and the Freedom of Access to Clinic Entrances (FACE) Act. Has the focus on hate crime and trafficking investigations resulted in a reduction of investigations in other critical areas of civil rights enforcement? Please explain.**

**Response:**

The investigative resources the FBI devotes to address backlash hate crimes targeting the Arab, Muslim, and Sikh communities, and to the increasing focus on human trafficking matters, have not resulted in a diminished focus on the other subprograms within the CRP.

In articulating the FBI's top priorities after the tragic events of 9/11/01, the Director designated the protection of civil rights among the FBI's top 10 priorities. As a result, as indicated in response to Question 105, above, if a Field Office's resources available to address civil rights matters are strained, the SAC has the authority to pull resources from other, lower-priority programs to ensure that civil rights matters are appropriately addressed.

**107. Please indicate the number of investigations the FBI has opened each year over the past ten years regarding: (A) hate crimes, (B) human trafficking, (C) police misconduct and other "color of law" violations, (D) FACE violations, and (E) other criminal civil rights violations.**

**Response:**

The chart below reflects the number of Hate Crime, Involuntary Servitude/Slavery (ISS), Color of Law (COL), and FACE Act cases opened by the FBI since 1994. The chart does not contain a category for "other criminal civil rights violations" because these four subprograms capture all civil rights cases investigated by the FBI.

FY	Hate Crimes	ISS	COL	FACE	TOTAL
1994	1604	13	3063	0	4680
1995	736	28	2638	45	3447
1996	855	3	2582	227	3667
1997	919	9	2729	97	3754
1998	878	14	2799	84	3775
1999	801	18	2411	91	3321
2000	729	51	2276	59	3115
2001	751	54	1797	42	2644
2002	652	58	1385	23	2118
2003	478	65	1345	20	1908
(End 2 <sup>nd</sup> Qtr) 2004	167	26	614	9	816



**108. According to the FBI's website, there are two units within the Civil Rights Program that investigate criminal civil rights violations: the Color of Law Unit and the Hate Crimes Unit. Your website indicates that the Hate Crimes Unit has investigatory authority over not only hate crimes but also human trafficking and FACE violations.**

**a. Is your website accurate in this regard? If not, please explain the current organizational scheme for the investigation of criminal civil rights violations.**

**Response:**

No. In June 2002, the Hate Crimes Unit and the Color of Law Unit were combined to form the CRU. The FBI is currently in the process of updating the website to reflect this change in organizational structure.

**b. Has the Hate Crimes Unit received an increase in the number of agents over the past three years? Please provide data about the number of agents who have served in the Hate Crimes Unit each year over the past ten years. Please provide similar data about the number of agents who have served in the Color of Law Unit each year over the past ten years. Please indicate whether any other FBI agents are assigned to the Civil Rights Program.**

**Response:**

The number of Supervisory Special Agents (SSAs) in the former Hate Crimes Unit and Color of Law Unit, now combined to form the CRU, has remained relatively constant over the past ten years. The CRU, which has program and case management responsibilities, has a funded staffing level of six and is currently staffed with five SSAs.

Perhaps more helpful to an understanding of the FBI's commitment to civil rights investigations is the FBI's FSL of 153 Agents in the CRP. The chart below reflects the CRP's FSL and "work years" since 1997, the earliest year for which these numbers are available. The work years include all CRP work done, whether by Agents assigned to the CRP or to other programs. These work years exceed the FSL in years in which Agents outside the CRP worked on civil rights cases, but they are less than the FSL when Agents assigned to the CRP are required to work on other matters, such as on CT or CI investigations.

FY	Work Years	FSL
1997	182.12	156
1998	155.41	156
1999	189.55	155
2000	161.63	153
2001	141.38	153
2002	104.47	153
2003	114.16	153
(End 2 <sup>nd</sup> Qtr) 2004	120.32	153

**109. Some people have expressed concern that there may not be a sufficient number of agents working in the Bureau's Civil Rights Program to meet the challenges of increased numbers of hate crime and human trafficking violations, in addition to police misconduct and FACE.**

**a. Do you believe that the FBI has a sufficient number of agents in its Civil Rights Program, or do you believe that more agents are needed? If the latter, how many more agents are needed?**

**Response:**

Currently, the CRP's FSL is 153 Agents. Because only a few field offices are using more Agent work-hours for the CRP than they are allotted, it does not appear that an increase in the number of Agents assigned to the program is necessary. However, ISS cases have increased substantially over the last several years due to improved community awareness of these matters. If this trend continues, additional Agents may be needed. A future terrorist attack could also cause an increase in backlash hate crimes against those believed to be of the same ethnicity as the terrorists, which could require additional civil rights investigative resources. Finally, while the level of resources needed to address FACE Act crimes should remain relatively static, a single, high profile, violent act could reverse this trend and necessitate the dedication of additional program resources.

**b. What efforts if any have you undertaken to request more agents for the Civil Rights Program? Please discuss specific recommendations you have made, if any, to obtain additional personnel for this program.**

c. If you have requested more agents for the Civil Rights Program, have you been successful in obtaining them? If so, please indicate how many additional agents you have received. If not, please explain whether your requests were denied by Congress, by personnel within the Department of Justice, or by personnel within the White House or Office of Management and Budget.

**Response to b and c:**

The FBI works with DOJ and the Administration to determine its budget requirements. It is the Administration's policy that pre-decisional information concerning the level of these requirements not be released. In FY 2002 through 2005, no additional Civil Rights personnel were included in the budget request to Congress. However, in FY 2004 Congress added nine support positions to the FBI's Civil Rights complement.

110. According to the FBI's website, the two units within the Civil Rights Program "provide training to FBI New Agents, Field Agents, National Academy Attendees and other state/local police officers from around the country." Please describe all training that the Civil Rights Program has provided over the past three years regarding enforcement of human trafficking, hate crimes, FACE, and police misconduct laws for (A) new FBI agents, (B) FBI agents who serve in the Bureau's investigative programs other than the Civil Rights Program, (C) state and local police officers, indicating the departments in which those officers serve, and (D) other National Academy Attendees, indicating the law enforcement units in which those attendees serve.

**Response:**

As previously discussed in response to Question 108a, above, the FBI's website contains outdated information regarding the existence of two units responsible for civil rights violations, rather than reflecting that those two units have been combined to create the CRU. The CRU provides civil rights training to all FBI New Agents' classes, covering the four subprograms within the CRP. Since FY 2002, the CRU has conducted 56 two-hour blocks of New Agent instruction.

With few exceptions, Agents who serve in other FBI investigative programs do not receive training in civil rights matters aside from the initial training received as a New Agent trainee. One exception occurs when an Agent is temporarily assigned to the CRP, in which case the Agent would receive civil rights training.

Civil Rights training for state and local law enforcement agencies is provided regularly by the FBI Field Offices. A roster specifically identifying the agencies

that have received training from the FBI would be voluminous; over the past three years more than 180 agencies have received FBI training in more than 330 civil rights training sessions. CRU personnel also periodically conduct civil rights training for state and local law enforcement officials based upon requests from FBI field offices, United States Attorneys' Offices, and DOJ.

In addition, the CRU conducts quarterly training sessions for the FBI's NA attendees. A roster specifically identifying these agencies would be voluminous; approximately 1,000 NA attendees receive this training annually.

**111. Some FBI agents who have served in the Civil Rights Program have stated that this investigative program is not considered a prestigious program within the Bureau or a stepping stone to leadership within the Bureau.**

**a. What is your response to this assertion?**

**Response:**

The assertion that the CRP is not considered a stepping stone to leadership positions within the Bureau is inaccurate. The number of civil rights investigators who are ultimately promoted is comparable to the promotion rates in other programs, such as the White Collar Crime, Organized Crime, and Violent Crime/Major Offender Programs. Although CT promotional opportunities may be the greatest due to the size of that program, civil rights investigators are afforded an opportunity to gain the CT knowledge they need to be competitive for senior CT positions through readily available training and TDY opportunities.

**b. What is the Bureau doing to demonstrate to its personnel that civil rights positions within the Bureau are prestigious and career-advancing posts?**

**Response:**

The FBI demonstrates the importance of civil rights positions by acknowledging those who have contributed to and achieved within the program through promotions and awards, including Quality Step Increases and other incentive awards. In addition, a significant number of Agents assigned to civil rights matters have been nominated and have received national recognition for their investigative efforts through the highly prestigious Attorney General's Award for Excellence and the Director's Distinguished Service Award.

**112. The FBI website indicates that your agency co-chairs a subcommittee of the Attorney General's Hate Crimes Working Group.**

**a. Is this working group still in existence? If so, please describe its duties and responsibilities, how often it meets, and please identify the members of the subcommittee and working group.**

**Response:**

As DOJ advised in response to questions posed to Attorney General Ashcroft following his 6/8/04 hearing before the Senate Judiciary Committee, in 1997 Attorney General Janet Reno asked the Office of the Deputy Attorney General to establish a Hate Crimes working group to examine the problem of bias-motivated crimes including: legislative initiatives, data collection, community outreach, prosecution and enforcement, and coordination. The working group fulfilled its mandate in October 1997, when it submitted to the Attorney General a memorandum outlining specific proposals. These proposals were approved by the Attorney General, and formed the basis for the Department's hate crimes initiative. In December 1997, the Attorney General directed the implementation of the hate crimes initiative. The Department (including U.S. Attorneys' Offices, the Civil Rights Division, and the FBI) continues to vigorously investigate and prosecute bias-motivated crimes.

Since September 2001, federal, state, and local authorities have investigated over 600 alleged incidents of religiously or racially motivated backlash crime. State and local prosecutors have brought charges in nearly 150 of these incidents (in a number of cases, with federal assistance). In addition, federal charges have been brought in 22 cases against 27 defendants, resulting in 20 convictions and one acquittal (one defendant committed suicide prior to trial). Currently, eight defendants are awaiting trial or sentencing.

**b. Has the FBI taken a position on whether it supports the bipartisan Local Law Enforcement Enhancement Act of 2003, S. 966? If so, please indicate whether you support or oppose this bill.**

**Response:**

DOJ did not take a position with respect to this 108th Congress legislation.

ALL INFORMATION CONTAINED  
HEREIN IS UNCLASSIFIED  
DATE 04-16-2012 BY 65179 DMH/STP/MJS

**ENCLOSURE**

**QUESTION 16**  
**TRILOGY CONTRACT CHRONOLOGY**

**MEMORANDUM**

**TO:** Contract File  
GSA Contract No. GS00T99ALD0210  
Task Order T0001AJM028

**From:** Shelly Goergen  
FEDSIM Contracting Officer  
and  
Paul R. Thornton  
FEDSIM PM/COR, FBI Trilogy UAC

**Re:** Trilogy User Application Component (UAC) Task Order  
Historical Document - Trilogy UAC Task Order

**Date:** January 26, 2005

**INTENT OF TRILOGY UAC HISTORICAL DOCUMENT**

Intent of this document is to provide an ongoing objective historical account of the FBI TRILOGY UAC Task order in order to clearly demonstrate justification for ALL significant contractual actions and directions that have been executed by GSA FEDSIM to date on behalf of its client, the FBI.

**FBI VISION FOR TRILOGY UAC**

**TRILOGY** is intended to be a three year project for upgrading the IT capabilities and associated support services throughout all of the sites for the Federal Bureau of Investigation (FBI). TRILOGY organizes the FBI IT infrastructure into three functional components: User Applications Component (UAC), Information Presentation Component (IPC), and Transportation Network Component (TNC).

**The goal of the User Applications Component (UAC)** is to replace the available current investigative applications and present the data via an easier user interface with enhanced functionality. To achieve improved data access the FBI envisions an improved search and indexing capability to access all relevant data subject to security and access constraints. The FBI also envisions documenting and managing investigative cases from inception to closure via an electronic "Virtual" Case File (VCF), to include multimedia. The envisioned system will result in the consolidation and simplification of processes and significantly reduce the dependence on paper transfer and filing, as well as paper forms.

The VCF goal is to capture information once, organized by outcomes, not functions, on the premise that information will be widely shared and distributed. The FBI also envisions the UAC to provide a reliable, dynamic, centrally administered Web-site. The centrally administered Web-site will provide users the ability to employ the Intranet to search and retrieve information, upload and download information including manuals, FBI documents, forms and personnel announcements. To optimize performance, and to better administer, manage, and support users, the FBI envisions consolidating all Intranet pages into a centralized infrastructure.

The Enterprise Management System (EMS) lies within the TNC, at the intersection of all TRILOGY components (the UAC, IPC, and TNC). The EMS will provide FBI IT Infrastructure management for the IPC, TNC, and UAC. The EMS will provide basic management and control of network assets and software. The EMS will provide users with an around-the-clock TRILOGY Help Desk. The TRILOGY Help Desk support shall augment the current operations.

### TRILOGY UAC TIMELINE

<b>DATE:</b>	February 7, 2001
<b>ACTION:</b>	RFP To Millennia Contractors

On February 7, 2001, FEDSIM sent a notice to all Millennia Contractors regarding Task Order Request (TOR) GSC-TFMG-01-M028. This TOR provides support to the FBI to modernize the IT infrastructure across the FBI, and focuses solely on satisfying the requirements of the UAC of TRILOGY (i.e. TOR does not include IPC/TNC requirements).

The FBI established priorities for the TRILOGY UAC, based on FBI mission needs. The original priority of the Trilogy UAC TOR was to improve technology first, then address usability. The FBI needed to correct IT infrastructure problems, which made it difficult to use legacy investigative applications. The historical lack of an Enterprise IT strategy resulted in dozens of legacy stove-piped databases. In addition, the old system did not operate the way agents do their jobs, and there were incomplete on-line case files due to:

Lack of basic multi-media support

Low confidence/faith in the system by agents and users. They couldn't get to it, or they simply did not use it.

As a result, vendors were solicited to provide the following Technology Refreshment solutions:

- Update the system hardware and software
- Move the data to modernized databases
- Provide a web interface
- Re-host the applications

- It was NOT the FBI's original intent to
- Re-engineer the data and business processes
- Create a single physical database
- Build custom applications and software around Users' requirements
- Overhaul the security and access control mechanisms



<b>DATE:</b>	June 5, 2001
<b>ACTION:</b>	Trilogy UAC Task Order Award issued

On June 5, 2001, the FBI UAC Task Order was issued to Science Applications International Company (SAIC) under the Millennium Contract (GS00T99ALD0210), as a result of TOR GSC-TFMG-01-M028 and Amendments 0001 and 0002. Services for this award were specified in SAIC's proposal dated 3-19-2001. The total estimated value of the Task Order award was \$87,785,931.

**CLIN Ceilings**

CLIN 1 (Labor)	61,397,931.00
CLIN 2 (Long Dist. Travel)	300,000.00
CLIN 3 (ODCs)	25,000.00
CLIN 4	26,063,000.00
<b>Total Contract Value</b>	<b>87,785,931.00</b>

<b>DATE:</b>	September, 2001
<b>ACTION:</b>	POST 9-11
<b>IMPACT:</b>	PROBLEM AREAS IDENTIFIED (with current direction of Trilogy UAC Task Order)

The terrorist activities of 9-11-01 resulted in the identification of the following "problem areas" with the current direction of the existing Trilogy UAC Task Order:

- Potential scale and complexity of investigations (e.g., PENTTBOM) could not be managed with original approach
- Agents would have limited ability to analyze data across FBI cases and systems with the original approach (information still stovepiped) – "Don't know what we know."
- Information sharing with other federal agencies, state and local law enforcement not fully addressed
- Business processes needed to change – "How cases are managed."
- IT organization was driving the "process," instead of Agent community needs
- Technology upgrades were simply not going to address existing problems

Subsequent to September 11, 2001, the FBI identified the need to accelerate work under Task Order T0001AJM028 in support of the FBI Trilogy UAC. The UAC component of Trilogy will upgrade and enhance the five major existing (legacy) investigative software applications: Automated Case Support (ACS), Criminal Intelligence Support Program (CISP), Integrated Intelligence Information Application (IIIA), Criminal Law Enforcement Application (CLEA) and Telephone Application (TA) functionality and data. The terrorist attacks of September 11, 2001 ignited an effort to accelerate the development schedule of Trilogy, which already had an aggressive 3-year schedule. Trilogy has important impacts on all FBI locations and addresses the needs of both the agents and their support community. Trilogy is particularly important for the investigation of the September 11, 2001 terrorist attacks on the United States and the potential for further attacks, including the recent anthrax episodes. Approximately 50 percent of the FBI Field Offices, adjunct offices, headquarters, and other classified components of the FBI are involved in the terrorist attack investigation. In response to the events of September 11, the FBI Director instructed that Trilogy be deployed faster than the current contracted schedule with the deployment to be completed in July 2002. Congress recognized the importance of this schedule

acceleration and passed legislation to provide additional funding for the FBI's efforts. The FBI Director and a FBI team drove key Trilogy UAC decisions that included the following:

Stop Work on web-enabling existing applications (user interface updates would not improve effectiveness).

Recognition that adding functionality to initial UAC would be cost ineffective (marginal enhancements would be expensive and increase overall schedule risk).

FBI Agents and users must determine operational solutions via:

Re-engineering of the case management process & data relationships (system must support the process, not the reverse)

Re-engineering that is based on the VCF concept

Active and continuous user involvement

Replans between September 2001 and January 2002, included:

Web Enabling Replan (Sept. '01)

ACS Acceleration Mainframe Centric Architecture Replan (Sept. '01)

- Oracle Proposal Replan (Nov. '01)
- Programmatic Alternatives Replan (Nov./Dec. '01)
- Enterprise Solution (Dec. '01/Jan. '02)

<b>DATE:</b>	November 26, 2001
<b>ACTION:</b>	Trilogy UAC Task Order Mod #2
<b>IMPACT:</b>	COST (ceiling increase)

On November 26, 2001 modification #2 was approved to increase the ceiling of CLIN 0003.

**CLIN Ceilings**

CLIN 1 (Labor)	61,397,931.00
CLIN 2 (Long Dist. Travel)	300,000.00
CLIN 3 (ODCs)	100,000.00
CLIN 4	26,063,000.00

**Total Contract Value** 87,860,931.00

<b>DATE:</b>	December 17, 2001
<b>ACTION:</b>	STOP WORK on Web Enabling (Web Enabling began on 10-15-01)
<b>IMPACT:</b>	SCHEDULE (accelerated) REQUIREMENTS (stop work)

The support Contractor to the FBI for Trilogy UAC was asked to identify and present several alternatives to accelerate the efforts. The FBI, in conjunction with FEDSIM and the Contractor, determined that "Alternative 2" (which eliminated front end requirements of interim WEB Enablement to the FBI legacy systems) was the best approach to accelerate the schedule. This approach would allow the Contractor to immediately embark on the development of an Enterprise Solution (which has always been the end goal of Trilogy). On December 17, 2001, the FBI requested FEDSIM to provide notification to the Contractor to Stop Work on all WEB Enablement tasks under the Task Order to support Trilogy UAC. On December 21, 2001, the Contractor was given PRELIMINARY notification by FEDSIM to Stop Work on tasks C.3.3, Task 3 - Web-Enabled Replacement of User Interfaces; C.3.4, Task 4 - UAC Search Capability, and C.3.14.1, Subtask 14.1 HIS-UWG.

Per discussions with the Contractor, it was agreed that the Stop Work would be for a period of 60 days. During that timeframe a modification would be prepared to restructure the Statement of Work to reflect the elimination of the WEB Enablement tasks and the acceleration of Trilogy UAC.

<b>DATE:</b>	December 28, 2001
<b>ACTIONS:</b>	- Formal "Stop Work" on Web Enabling - Direction to re-focus efforts on Enterprise Solution development
<b>IMPACT:</b>	SCHEDULE (accelerated) REQUIREMENTS (redirect)

On December 28, 2001, the formal Stop Work notification was provided to the Contractor including a description of the work to be suspended and direction to re-focus their efforts on the remaining Task Order requirements for the development of an Enterprise Solution. In addition, the Contractor was requested to provide documentation identifying the final status of accomplishments to date on the WEB Enablement tasks and to provide a white paper on lessons learned on those efforts.

Based upon the above, issuance of a Stop Work on the identified tasks and entering into a modification by mutual agreement to delete those tasks from the Statement of Work was in the best interest of the Government. This minimized the administrative costs to the Contractor and the Government to realign tasking and costs under the Task Order.

<b>DATE:</b>	January 25, 2002
<b>ACTION:</b>	Authority-To-Proceed on ROM-Based Enterprise Solution
<b>IMPACT:</b>	REQUIREMENTS (redirect via an ATP)

Redirected tasks via an ATP. An ATP was issued in lieu of a modification because Enterprise Solution requirements had not yet been identified in full. Again, ATP was ROM-Based, NOT ECP-Based.

The Contractor was authorized to proceed with the development of the Enterprise Solution. In addition, the ATP letter relayed the intent of proposed modification PS05, which would delete the WEB Enabling tasks and combine the three yearly labor CLINs into a single labor CLIN.

Intent of the Government over the next several weeks was to define the changes to the Task Order and Attachment #5, in order to request a proposal (at that time Attachment #5 was recognized as a "Requirements Document" and is now recognized as an "informational supplement" only). Any adjustments to the task order ceiling would be made in a subsequent modification.

<b>DATE:</b>	February 8, 2002
<b>ACTION:</b>	FBI's Section C/F Revisions Request
<b>IMPACT:</b>	REQUIREMENTS (redirect)

Govt. drafted a contractual redirection in requirements/tasks via section C & F revisions.

On February 8, 2002, the FBI requested FEDSIM to solicit an Engineering Change Proposal (ECP) from the Contractor, to address the accelerated and new direction of the Trilogy UAC program. Changes to section C reflected the shift in FBI direction, which was to strike the task of web enabling FBI legacy systems, and implement an Enterprise Management System (EMS)

solution (changes were based on deletion of web enabling content – no new requirements were added). Changes to section F were also based on deletion of content – no new deliverables were added.

**DATE:** February 19, 2002  
**ACTION:** RFP/ECP Letter Issued to Contractor  
**IMPACT:** REQUIREMENTS (redirect/ECP request)

Govt. requested a contractual redirection in requirements/tasks via an ECP request.

FEDSIM requested a technical and cost proposal that would address appropriate changes to Section C and Section F for the accelerated Trilogy UAC Task Order. The Contractor was also invited to address any adjustments to the award fee evaluation criteria for Government consideration. Proposal deadline was set for March 18, 2002.

**DATE:** March 5 – May 2, 2002  
**ACTION:** ALPHA Sessions  
**IMPACT:** CONTRACTOR PERFORMANCE (in question)  
COST (BOE justification discussions)  
SCHEDULE (ECP submittal date extended twice)  
REQUIREMENTS (definition discussions)

Prior to proposal submittal, the government implemented the "Alpha Contracting Approach," which was intended to allow for trade-offs to be evaluated and incorporated into the proposal preparation process. The goal was to receive an acceptable proposal that could be incorporated by task order modification within two weeks following receipt.

Per discussions held during the "March, 2002" Alpha sessions ECP submittal date was moved to April 12, 2002 (from March 18, 2002).

Per discussions held during the "April, 2002" Alpha sessions ECP submittal date was again moved to May 13, 2002 (from April 12, 2002).

The March and April 2002 Alpha sessions resulted in the Government identification of several "concerns" and "problem areas" in regards to Contractor performance. These concerns/problem areas included, but were not limited to, the following areas:

- Contractor was not adequately prepared for Alpha sessions (hand-outs incorrect, managers not prepared, information was inconsistent).
- Contractor could not adequately define what work had been accomplished from the ATP issued on January 25, 2002 to the present (end of April, 2002).
- Contractor had failed to articulate/justify cost differentials to meet government satisfaction.
- Contractor could not adequately define UAC planning of how all function areas were to work in "lock-step" to accomplish Trilogy UAC goals and objectives.
- Contractor did not appear to have a strong team (from both leadership and management perspectives) assigned to the Trilogy UAC Task Order.

Because of the above noted concerns and problem areas, the Government considered the following Contractual "Options-to-Proceed:"

**Termination for Convenience – Option NOT Exercised**

The Government did not view this as a viable option due to justification difficulties (ie. Govt. still has a viable contract need and still has available funding).

**Termination by Default – Option NOT Exercised**

The Government did not view this as a viable option due to the fact that the Trilogy UAC TOR is a performance based contract. To date, the Contractor had not committed any contractual violations, and there had been no written evaluation/documentation regarding Contractor performance.

**Modify Contract to fund “Requirements Analysis” only - Option NOT Exercised**

The Government did not view this as a viable option due to the following primary issues:

- Time/Schedule delays to recompete TOR via Millennia or Millennia Lite
- Time/Schedule delays due to learning curve of a new Contractor
- Political ramifications (Congressional expectations already established on the Hill)

**Mutual Agreement to establish “ending period” with Contractor - Option NOT Exercised**

Per above (Option 3), FEDSIM CO recommended this approach, if the Government chose to “de-scope” requirements/tasking efforts. For the same reasons noted above (Option 3), the Government did not view this as a viable option.

**FIX IT (Continue with proposal negotiations) - OPTION EXERCISED**

**BOTTOM LINE**, in order to maintain a good working relationship with the Government, the Contractor needed to:

Build confidence (with the Government)

Strengthen the Team (replace applicable personnel in order to provide better management and leadership).

<b>DATE:</b>	May 13, 2002
<b>ACTION:</b>	Contractor's ECP Received
<b>IMPACT:</b>	COST (program over budget)

Total program cost of the Trilogy UAC ECP exceeded funding in FBI's allocated budget for the Trilogy UAC program.

Available funding to the FBI was approximately: \$108M  
Contractor Cost Proposal was approximately: \$149M

<b>DATE:</b>	June 24, 2002
<b>ACTION:</b>	Trilogy UAC Mod #8
<b>IMPACT:</b>	COST (ceiling increase)

On June 24, 2002 modification #8 was approved to increase CLIN 0003 ceiling.

**CLIN Ceilings**

CLIN 1 (Labor)	61,397,931.00
CLIN 2 (Long Dist. Travel)	300,000.00
CLIN 3 (ODCs)	150,000.00
CLIN 4	26,063,000.00
<b>Total Contract Value</b>	<b>87,910,931.00</b>

**DATE:** July 9, 2002  
**ACTIONS:** - FEDSIM requests revised ECP (ECP1a) from Contractor  
 - Revised/Updated Authority-to-Proceed (ATP) Issued to Contractor  
**IMPACT:** COST (budget constraints)  
 SCHEDULE (budget constraints)  
 REQUIREMENTS (budget constraints)

Revised/updated tasks via an ATP. An ATP was issued in lieu of a modification because Enterprise Solution requirements had not yet been identified in full.

As noted earlier, the FBI did not have sufficient funding allocated to fund the Trilogy UAC program in its entirety, at this time. In order to best assist the FBI, FEDSIM requested a revised ECP (ECP01a for work through November 30, 2002). It was/is also the desire of the government to award additional ECP(s), as needed, to continue performance beyond November 30, 2002, dependent upon the FBI's available budget.

On July 9, 2002, FEDSIM requested a revised technical and cost proposal, ECP01a, (from the original ECP01, received on May 13, 2002) and provided a revised/updated ATP for work performed, prior to execution of a modification incorporating the negotiated ECP01a.

The ECP01a proposal deadline was set for July 26, 2002.

**DATE:** July 26, 2002  
**ACTION:** Contractor's ECP1a Received  
**IMPACT:** COST  
 SCHEDULE  
 REQUIREMENTS

Contractor provided ECP1a to the Government which was a revision of the ECP proposal received on May 13, 2002. However the cost and technical proposal now reflected a period-of-performance (PoP) through November 30, 2002 only (not entire duration of anticipated PoP).

Contractor Cost Proposal was approximately: \$67M (6/5/01 - 11/30/02)

**DATE:** August, 2002 - October 10, 2002  
**ACTION:** Award Fee Negotiations  
**IMPACT:** CONTRACTOR PERFORMANCE  
 COST (fee negotiated/invalid performance criteria)  
 SCHEDULE (ECP1a Mod Delayed)

Award Fee had to be negotiated due to invalid performance criteria for periods 1 and 2 (resulting from 9-11 terrorist attacks).

ECP1a could not be implemented contractually (via modification), until all parties (FBI, FEDSIM and the Contractor) completed/reached concurrence on negotiations for the Trilogy UAC Award Fee distribution/plan. Mutual agreement was reached on October 10, 2002 by all parties on the following points (with a proposed revision of the Award Fee Determination Plan to be forwarded by the FBI):

- \$1,267,000 negotiated fee amount for the 1st and 2nd award fee periods.
- 3% base fee and 7.5% award fee pool for period 3 (end date of November 30, 2002)
- ECP01b delivery 1 award fee will be allocated as follows:
  - 3% base fee and 7.5% award fee pool if delivery 1 occurs on or before December 12, 2003.
  - 3% base fee and 8.5% award fee pool if delivery 1 occurs on or before November 12, 2003.
  - 3% base fee and 9.5% award fee pool if delivery 1 occurs on or before October 12, 2003

If the options are exercised, the same award fee structure will apply for deliveries 2 and 3. In the ECP01b award fee period, the contractor may earn all, part, or none of the award fee allocated to the applicable evaluation periods. If the award fee rating is 80 or higher, then any unearned award fee will automatically roll over into a subsequent award fee period. For award fee ratings below 80, the AFDO reserves the right to make a determination as to the amount of unearned award fee, if any, to be rolled over into a subsequent period.

<b>DATE:</b>	October 10, 2002
<b>ACTION:</b>	FEDSIM Requests ECP1b from Contractor
<b>IMPACT:</b>	COST SCHEDULE REQUIREMENTS

FEDSIM requested ECP01b which would provide cost/schedule for the Trilogy UAC program in its entirety (projected to end August, 2004).

The ECP01b proposal deadline was set for October 30, 2002.

<b>DATE:</b>	November 4, 2002
<b>ACTION:</b>	Contractor's ECP01b Received
<b>IMPACT:</b>	COST (program still over approved budget) SCHEDULE REQUIREMENTS

Contractor provided a cost and technical proposal for the Trilogy UAC program in its entirety (projected to end August, 2004). Total program cost of the Trilogy UAC ECP01b still exceeds FBI's allocated budget for the Trilogy UAC program. However, the FBI was confident that additional funding would be secured.

Contractor Cost Proposal is approximately: \$141M (6/5/01 - 8/2004)

<b>DATE:</b>	December 5, 2002
<b>ACTION:</b>	Trilogy UAC Task Order Mod #12 (ECP1a Complete)
<b>IMPACT:</b>	COST SCHEDULE REQUIREMENTS

SAIC's proposal dated May 13, 2002 (ECP), as revised on July 26, 2002 (ECP01a) and October 17, 2002 (ECP01a) is incorporated by this modification. The proposal iteration dated October 17, 2002, covers anticipated costs from date of award through December 6, 2002 (in lieu of through November 30, 2002 as captured in the July 26, 2002 proposal). The December 6 date represents the end date for Award Fee period 3.

SAIC's letter dated December 4, 2002, is incorporated by reference and this modification authorizes work to be performed IAW with that letter. Funding currently obligated under the

Task Order covers costs incurred to date, as well as anticipated expenditures to be incurred IAW the December 4<sup>th</sup> letter through December 31, 2002.

**Section C was modified to reflect the following:**

- Delete the WEB enabling tasks
- Add Section 508 requirements
- Add requirements to re-engineer the data and business processes
- Create a single physical database
- Build custom applications and software around user requirements
- Overhaul the security and access control mechanisms

**Section F was modified to do the following:**

- Extend the period of performance from June 2004 to August 2004 and to specify the delivery date for delivery 1 deployment to be December 12, 2003
- Modify the milestone schedule for additional planned completion dates for deliverables and activities planned to date
- Modify the specifications for the Trilogy UAC master plan

**Section J was modified to re-define the Award Fee Determination Plan and to add accessibility standards IAW 508.**

<b>DATE:</b>	April 7, 2003
<b>ACTION:</b>	Authority-To-Proceed on ECP1b Options 1 and 2
<b>IMPACT:</b>	COST SCHEDULE REQUIREMENTS (redirect in approach) *VISION/APPROACH CHANGE (as proposed by SAIC/agreed to by Gov)
The previous ATP issued in conjunction with ECP01a, Mod #12, on December 5, 2002, anticipated an earlier ECP01b contract modification timeline.	
*This could be considered a key data point where the vision/approach of the VCF program shifts from clear cut integration and replacement of the five major existing (legacy)	

**Schedule Concerns:** Actual timeline (as opposed to anticipated timeline) necessitated a need to update ATP activities in order to preserve schedule, since the previous ATP issuance did not reflect start up activities on Options 1 and 2 of the ECP01b proposal.

**Budget Concerns:** A modification could not be issued at this time because the total program cost of the Trilogy UAC program (as proposed in ECP01b) still exceeded funding in FBI's allocated budget. Additional Trilogy UAC reprogramming dollars had not yet been approved by Congress.

**VCF Vision:** This ATP letter also recognized a new product management approach (as proposed by SAIC/agreed to by the Government). As the vision of the VCF emerged, the VCF team began to recognize the implications of this new enterprise system and how the FBI will do business in the future. The plan to simply migrate three more systems into the VCF environment does not acknowledge that the previously envisioned "target" system has changed dramatically since the Delivery 2 and 3 plan was originally developed. FEDSIM and the FBI agreed with



SAIC that a product management approach for developing the VCF as well as other enterprise-level applications should be considered.

<b>DATE:</b>	May 16, 2003
<b>ACTION:</b>	GSA/FEDSIM issues Award Fee amount for Period 3
<b>IMPACT:</b>	AWARD FEE/COST CONTRACTOR PERFORMANCE (87% final rating – out of possible 100%)

- Final award fee performance evaluation report and determination amount for period 3 was forwarded to SAIC. This resulted in a 87% performance rating (out of 100% possible rating).
- SAIC awarded 87% of the monies available for Trilogy UAC award fee period three (06/22/02 – 12/06/02).
- SAIC awarded a fee of \$932,758.00, and all of the unearned fee of \$139,378.00 was rolled forward from the third award fee period to the fourth award fee period.

<b>DATE:</b>	June 20 – June 24, 2003
<b>ACTION:</b>	ALPHA Sessions – Revisited for ECP1b
<b>IMPACT:</b>	COST (BOE justification discussions) SCHEDULE (justification discussions) REQUIREMENTS (definition discussions)

Alpha pricing sessions were again conducted with the Contractor to revisit the basis of estimates (BOEs) for the ECP1b cost proposal. This proposal had not changed since submission on November 4, 2002 and due to delay in issuance it was deemed necessary by the Government to revisit this proposal. Technical requirements were also discussed in the context of the required technical skills and level of effort required to accomplish the tasks required by the statement of work. Any inconsistencies found in the BOEs (regarding current status gameplan as to what was proposed in November of 2002) were resolved during these sessions.

Only changes from ECP1b proposal were:

- Multi Media Station Training
- BOE – 1.6.6 (Data Engineering)
  - SAIC update (re: task description w/ 4,193 hrs)
  - SAIC replaced Nov 02 BOE (1.6.6 & 1.6.7) with Feb 03 replan (new 1.6.6)
- BOE 1.10 (Training)
  - SAIC struck training hours as identified in ECP01b BOE notebook (pg. 454)
  - SAIC updated training materials and delivery of training

<b>DATE:</b>	July 18, 2003
<b>ACTION:</b>	Contractor at Risk (Start Date)
<b>IMPACT:</b>	COST

The Contractor was now working at risk because the Trilogy UAC program had reached the ceiling level on CLIN 0001 - Labor (\$61M). FEDSIM could not increase the ceiling (via a modification incorporating ECP01b) because Congress had still not approved additional Trilogy reprogramming dollars.

Contractor performed "at risk" (July 17, '03 - Sept. 4 '03) during this period even though future funding for the Trilogy UAC program was still unknown/unapproved.

<b>DATE:</b>	July 31, 2003
<b>ACTION:</b>	Senate approves Trilogy Reprogramming Dollars
<b>IMPACT:</b>	COST

On 7/31/03 the Senate approved \$110M out of the \$138M Trilogy reprogramming dollars sought/requested by the FBI.

<b>DATE:</b>	September 2, 2003
<b>ACTION:</b>	FEDSIM Receives Trilogy Reprogramming Dollars
<b>IMPACT:</b>	COST

The Treasury Department forwarded approved funding to the FBI on August 29, '03. FEDSIM received \$53.1M of FBI funding to obligate on Trilogy UAC on September 2, 2003.

Contractor was still at risk (since July 18, '03).

<b>DATE:</b>	September 4, 2003
<b>ACTION:</b>	Trilogy UAC Mod #22 (ECP1b Complete)
<b>IMPACT:</b>	COST (ceiling increase) SCHEDULE REQUIREMENTS

Modification #22 incorporated by reference SAIC Engineering Change Proposal (ECP) No. 01b into this Task Order. ECP 01b consists of Part I (Cost Proposal), Part II (Technical Proposal) and Part III (Basis of Estimate) dated 4 November 2002, revised July 2003, and approved/accepted by the Government on July 25, 2003.

Modification #22 increased, as well as funded Trilogy UAC CLINs 1, 2 and 3 in their entirety.

**CLIN Cellings**

CLIN 1 (Labor)	113,035,239.00
CLIN 2 (Long Dist. Travel)	542,115.00
CLIN 3 (ODCs)	916,218.00
CLIN 4	27,264,000.00
<b>Total Contract Value</b>	<b>141,757,572.00</b>

<b>DATE:</b>	September 21, 2003
<b>ACTION:</b>	Award Fee Period 4 - Interim Performance Evaluation #1
<b>IMPACT:</b>	AWARD FEE CONTRACTOR PERFORMANCE (75% interim rating - out of possible 100%)

Award Fee Evaluation Report (number 1) for period 4 was forwarded to the contractor. This report served as a "checkpoint" to clarify the Government's current position of the Contractor's performance rating/score for award fee period 4.

- **Contractor Performance Points: 75 (out of 100 possible)**
- **Contractor Rating Adjective: Standard** (Award Fee Point Range ~ 70 to 79)
- **Standard is defined as:** *Performance meets Task Order requirements. Non-conformances are minor, but Government resources are required to assure that timely corrective actions are taken. Customer satisfaction is at risk.*

CRITERIA	Rating Adjective	Points	Weight (%)	Category Total
Technical	Standard	74	40%	30
- Test	- Marginal	- 62	- 10%	
- Training	- Standard	- 70	- 10%	
- System Design	- Standard	- 73	- 10%	
- System Support	- Good	- 90	- 10%	
Schedule	Standard	75	40%	30
Cost	Standard	75	20%	15
<b>GRADE</b>	<b>Standard</b>			<b>75</b>
<b>Award Fee</b>				<b>N/A for now</b>
<b>Roll Over</b>				<b>N/A for now</b>

<b>DATE:</b>	<b>December 2, 2003</b>
<b>ACTION:</b>	<b>Award Fee Period 4 – Interim Performance Evaluation #2</b>
<b>IMPACT:</b>	<b>AWARD FEE</b>
	<b>CONTRACTOR PERFORMANCE (69% interim rating – out of possible 100%)</b>

Award Fee Evaluation Report (number 2) for period 4 was forwarded to the contractor. This report served as a "checkpoint" to clarify the Government's current position of the Contractor's performance rating/score for award fee period 4.

- **Contractor Performance Points: 69 (out of 100 possible)**
- **Contractor Rating Adjective: Marginal** (Award Fee Point Range – 61 to 69)
- **Marginal is defined as:** *Nonconformances are serious, and extra Government resources are required to assure that corrective actions are taken. Few achievements are made. Contractor is not proactive. Corrective actions are not timely or effective. Customer is not satisfied.*

CRITERIA	Rating Adjective	Points	Weight (%)	Category Total
Technical	Marginal	67	40%	27
- Test	- Unsatisfactory	- 42	- 10%	
- Training	- Standard	- 79	- 10%	
- System Design	- Unsatisfactory	- 56	- 10%	
- System Support	- Good	- 90	- 10%	
Schedule	Standard	70	40%	28
Cost	Standard	70	20%	14
<b>GRADE</b>	<b>Marginal</b>			<b>69</b>
<b>Award Fee</b>				<b>N/A for now</b>

EFF Section 215-406

Roll Over

N/A for now

<b>DATE:</b>	December 3, 2003
<b>ACTION:</b>	Trilogy UAC Mod #24
<b>IMPACT:</b>	COST (ceiling increase) REQUIREMENTS

Modification #24 authorized an increase in the number of facilitated instructors for Virtual Case File (VCF) training from 25 to 60. The reason for this increase is to ensure there is enough training coverage to send facilitators to all field offices (FOs) and resident agencies (RAs). This change request (CR-0308) was approved through SAIC's Engineering Review Board (ERB), the SAIC Configuration Control Board (CCB) and the FBI.

**CLIN Ceilings**

CLIN 1 (Labor)	114,033,095.00
CLIN 2 (Long Dist. Travel)	1,167,217.00
CLIN 3 (ODCs)	916,218.00
CLIN 4	27,264,000.00
<b>Total Contract Value</b>	<b>143,380,530.00</b>

<b>DATE:</b>	December 11, 2003
<b>ACTION:</b>	Arbitration Process Meeting
<b>IMPACT:</b>	COST (increase labor CLIN ceiling vs. bill against labor CLIN ceiling) REQUIREMENTS (FEDSIM to arbitrate disputes)

The growing number of new Change Requests (CRs) that were impacting cost now required 3<sup>rd</sup> party intervention to deem applicable CRs as either a CHANGE (NEW Requirement) OR a FIX.

- A **FIX** is a change designed to bring the system into compliance with a specified set of functional (or physical) requirements.
- **CHANGES** are those related to improving performance, or capabilities, beyond the minimum requirements stated in the specification.

Changes with associated cost impact are treated as a new requirement (new cost/increase in ceiling) and fixes are billed against the "current" ceiling.

All parties (FBI, FEDSIM and SAIC) agreed to implement an arbitration process to solve disputes over interpretation of changes vs. fixes within the VCF program. One primary POC was appointed from each party (FBI, FEDSIM and SAIC) in this arbitration process. FEDSIM has final ruling authority on those issues that do not reach agreement/concurrence between the FBI and SAIC. This process is held independently from the current CR and Software Problem Reports (SPR) processes.

<b>DATE:</b>	December 12, 2003
<b>ACTION:</b>	VCF Deployment Date Not Met
<b>IMPACT:</b>	COST SCHEDULE REQUIREMENTS

EFF Section 215-407

The contractor failed to deploy the VCF system upon the agreed deployment date of December 12, 2003.

<b>DATE:</b>	December 17, 2003
<b>ACTION:</b>	VCF System Delivered (NOT Deployed) to the Government
<b>IMPACT:</b>	SCHEDULE REQUIREMENTS

VCF System was delivered (NOT deployed) to the Government on Wednesday, Dec. 17, 2003.

<b>DATE:</b>	January 21, 2004
<b>ACTIONS:</b>	- FEDSIM rejects 12-17-03 VCF delivery - Gov cites 17 VCF deficiencies - Gov request: When will VCF be delivered for inspection/acceptance? - Gov request: Will SAIC complete program at or under cost, within PoP?
<b>IMPACT:</b>	COST SCHEDULE REQUIREMENTS (VCF rejected)

A "draft" VCF system had not been recognized as a contractual Section F deliverable by the Government.

- FEDSIM issued written correspondence to inform SAIC that the Virtual Case File as delivered on December 17, 2003 was not acceptable (in accordance with FAR 52.246-5, Inspection of Services – Cost Reimbursement).
- In accordance with Millennium Contract GS00T99ALD0210, Section E 3.3, the Government also provided written notification citing 17 deficiencies addressing why the VCF system/deliverable was not considered acceptable.
- SAIC was authorized to perform activities necessary to address the 17 deficiencies.
- SAIC was requested to provide written notification of when they anticipated VCF to be delivered for inspection/acceptance.
- Finally, SAIC was requested to provide written response if SAIC expected to complete Delivery 1, Release 2 and Release 3 within the current Period of Performance (June 5, 2001 – August 2, 2004) at or under the current contract ceiling of \$143,380,530.

<b>DATE:</b>	January 23, 2004
<b>ACTIONS:</b>	- SAIC deems 12-17-03 VCF delivery a DRAFT submission - SAIC responds to 17 deficiencies - SAIC provides acceptance date for VCF - SAIC provides VCF completion date/cost/schedule
<b>IMPACT:</b>	COST SCHEDULE REQUIREMENTS

- SAIC responded to FEDSIM via written correspondence indicating the VCF delivery of December 17, 2003 was a draft submission, not final.
- In regards to the 17 deficiencies, SAIC indicated that they believed a number of the items within the list were changes to the specification and not deficiencies.
  - FEDSIM would work independently (as agreed to via the Dec. 11 2003 Arbitration Process meeting) to review all 17 issues (and sub-issues) and make a determination for final ruling that would deem each item as either a change/new requirement OR a fix. In parallel, SAIC would move forward to complete necessary design activities that addressed all 17 identified issues (and sub-issues).

- SAIC developed/submitted a schedule that estimated the following major acceptance milestones as follows:
  - Complete System Test – April 26, 2004
  - Complete preparations for Acceptance Test – May 10, 2004
  - Ready for Acceptance Test – May 11, 2004
- SAIC updated the resource-loaded network (RLN) which now indicated ~~axpected~~ **completion date of October 29, 2004 for all project activities.**
- In regards to cost, SAIC indicated that they did not anticipate exceeding the current task order ceiling of \$143M. However, SAIC did estimate that CLIN 0001 (Labor) would exceed the current CLIN ceiling by \$14.2M (exclusive of base and award fee) and that CLIN 0004 (Tools) would under-run current CLIN ceiling by \$25M.
- SAIC estimates only addressed work scope authorized under the task order as currently modified. Outstanding Change Requests (CRs) for the Production Performance Test and the Training Environment were not considered in these cost and schedule estimates. In addition, unauthorized or undefinitized activities, still under consideration by FEDSIM and the FBI, had not been included in this estimate. Some of these activities included Section 508 implementation, Instructor-led training (ILT) activity, changes to the Training Environment, User Acceptance, Beta Testing, additional TNC/IPC integration testing, and Records Management Application (RMA) changes.

<b>DATE:</b>	February 9, 2004
<b>ACTIONS:</b>	<ul style="list-style-type: none"> <li>- FEDSIM again confirms rejection of 12-17-03 VCF delivery</li> <li>- FEDSIM does not recognize "draft" VCF system as a deliverable</li> <li>- Gov deems VCF delay unjustified</li> <li>- Gov requests Estimate-To-Complete (ETC) for D1 and R2/R3</li> <li>- Gov captures 16 items for scope clarification</li> </ul>
<b>IMPACT:</b>	<ul style="list-style-type: none"> <li>COST</li> <li>SCHEDULE (delay unjustified)</li> <li>REQUIREMENTS (contractual validity of VCF draft)</li> </ul>

- FEDSIM informed SAIC via written correspondence that per the ECP01b modification agreement of September 4, 2003, the VCF system was proposed to be delivered to the Government on December 12, 2003, for deployment. The VCF was not delivered in a state ready to be deployed, and had not been provided to the Government for User Acceptance and Testing in accordance with SAIC's proposed schedule on October 20, 2003. Therefore, the VCF as delivered on December 17, 2003 was not acceptable.
- FEDSIM communicated the Government's position that the delayed availability of TNC/IPC did not prevent SAIC from completing development and initial application testing of the VCF. Because there were no dependencies on the TNC/IPC schedule for development and "delivery" of the VCF, the Government did not find acceptable justification for an excusable delay.
- The Government requested SAIC to provide an Estimate to Complete (ETC) for Delivery 1, Release 2 and Release 3, in accordance with ECP01(b).
- The ETC deadline was set for February 13, 2004.
- 16 activities were noted for inclusion with this ETC direction. The 16 Activities captured were:
  1. Records Management Application (RMA)
  2. Security

3. Interface Testing
4. Data Engineering
5. Acceptance Test Criteria
6. IPC/TNC task order visibility
7. Acacia document needs
8. Training Delivery Approach
9. Performance testing using the production system infrastructure
10. Operations and Maintenance approach
11. ArcSight
12. Section 508
13. Implementation of CISP/Intelplus functions and data migration
14. VCF maintenance releases
15. EOC Support
16. Improvement in SAIC Test Cases

<b>DATE:</b>	February 10, 2004
<b>ACTIONS:</b>	<ul style="list-style-type: none"> <li>- SAIC again defends 12-17-03 VCF delivery as a DRAFT submission</li> <li>- SAIC defends Mgt. practices in communicating VCF schedule slippage</li> <li>- SAIC requests face-to-face discussions for ETC scope clarification</li> <li>- SAIC cites 28 outstanding CRs (w/cost impacts) for ETC clarification</li> </ul>
<b>IMPACT:</b>	<p><b>COST</b></p> <p><b>SCHEDULE</b> (communication of slippage)</p> <p><b>REQUIREMENTS</b> (contractual validity of VCF draft)</p>

- SAIC's correspondence again defends VCF delivery of December 17, 2003 as a draft deliverable and also defends SAIC's management practices regarding the communication to the Government on VCF schedule status (re: slippage).
- SAIC requests face-to-face discussions in order to reach agreement on full scope/clarification of all ETC related activities.
- SAIC recognized 28 Change Requests (CRs) that had been jointly reviewed and approved by the FBI via the Configuration Control Board (CCB) that still required cost/schedule impact proposals for modification.

<b>DATE:</b>	February 12, 2004 – March 22, 2004
<b>ACTION:</b>	ETC Scope Clarification Activities/Discussions
<b>IMPACT:</b>	<p><b>COST</b></p> <p><b>SCHEDULE</b></p> <p><b>REQUIREMENTS</b> (define ETC)</p>

ETC scope clarification discussions were kicked off at the SAIC Vienna facility on February 12 (all day event). Over 100 items were captured/discussed that required attention for ETC clarification purposes.

Closure processes for all recorded activities that required clarification for ETC issuance would take the VCF program through March 22, 2004 (date of revised ETC issuance from FEDSIM).

<b>DATE:</b>	February 13, 2004
<b>ACTIONS:</b>	<ul style="list-style-type: none"> <li>- Gov descopes IntelPlus requirement</li> <li>- Gov suspends R2/R3 activities</li> </ul>
<b>IMPACT:</b>	<p><b>COST</b></p> <p><b>SCHEDULE</b></p> <p><b>REQUIREMENTS</b> (descop/stop work)</p>

- The Government requested SAIC to continue development of Delivery One with the exception of the IntelPlus application functionality and data migration. SAIC was now to provide only an interface to the IntelPlus legacy application as part of Delivery 1.
- The Government also requested SAIC to suspend all development and related activities for Releases 2 and 3. The only exception to this directive was the Evidence Program Audit Inventory Software (EPAIS), which the Government requested to include as part of Delivery 1.

**DATE:** March 12, 2004  
**ACTION:** Award Fee Period 4 – Final Evaluation and Award Fee Determination  
**IMPACT:** AWARD FEE/COST  
**CONTRACTOR PERFORMANCE**  
 (34% final period rating–of possible 100% )

Final award fee performance evaluation report and determination amount for period 4 was forwarded to SAIC. This resulted in a 34% performance rating (out of a possible 100%), \$0.00 earned in award fee, with 100% roll over for period 4.

- **Contractor Performance Points: 34 (out of 100 possible)**
- **Contractor Rating Adjective: Unsatisfactory (Award Fee Point Range – 0 to 60)**
- **Unsatisfactory is defined as:** *Nonconformances are serious, and extra Government resources are required to assure that corrective actions are taken. Few achievements are made. Contractor is not proactive. Corrective actions are not timely or effective. Customer is not satisfied.*

CRITERIA	Rating Adjective	Points	Weight (%)	Category Total
Technical	Unsatisfactory	44	40%	18
- Test	- Unsatisfactory	- 30	- 10%	
- Training	- Unsatisfactory	- 60	- 10%	
- System Design	- Unsatisfactory	- 28	- 10%	
- System Support	- Unsatisfactory	- 57	- 10%	
Schedule	Unsatisfactory	20	40%	8
Cost	Unsatisfactory	40	20%	8
<b>GRADE</b>	<b>Unsatisfactory</b>			<b>34</b>
<b>Award Fee</b>				<b>\$0.00</b>
<b>Roll Over</b>				<b>100% roll over</b>

**DATE:** March 12, 2004  
**ACTION:** FEDSIM Issues Final Determination Ruling on 17 VCF "Deficiencies" Modification PS25 incorporates this understanding  
**IMPACT:** COST (increase ceiling OR bill against ceiling) REQUIREMENTS ("deficient" OR "new work")

FEDSIM completed independent review to resolve SAIC/FBI dispute over each party's position (change OR fix) on the 17 issues cited in the Government's January 21, 2004 correspondence regarding VCF acceptance.

FEDSIM issued the final ruling to all parties, defining each issue as a change or fix, with applicable justification. Final results captured the following break-down of the 17 issues (and applicable sub-issues under each of the 17, totaling 59 items in all):



- Changes 19
- Fixes 40

<b>DATE:</b>	March 22, 2004
<b>ACTION:</b>	FEDSIM issues Second Request for ETC (per post ETC definition activities/discussions) from Contractor
<b>IMPACT:</b>	COST SCHEDULE REQUIREMENTS (ETC definition discussions closed)

Parties reached closure on ETC activities that required clarification/definition.

FEDSIM requested an ETC from SAIC which would provide cost/schedule for Delivery 1, Release 2 and Release 3, as agreed to in ECP01b for the User Application Component (UAC).

The ETC deadline was set for April 2, 2004.

<b>DATE:</b>	March 22 – April 1, 2004
<b>ACTION:</b>	VCF Functional Review Sessions
<b>IMPACT:</b>	REQUIREMENTS (functional validation)

VCF Functional review sessions ran in parallel with ETC costing and scheduling activities (as opposed to completing PRIOR to ETC activities). Due to time constraints, all parties recognized, agreed to, and accepted the risk involved with this parallel approach (all parties understood that results of these sessions could significantly impact SAIC's ETC submittal package).

SAIC conducted 8 separate VCF Functional Review sessions during this time period with intent to demonstrate to the Government how the VCF system would fulfill the functionality needed to support the FBI's business. Processes included SAIC to walk the Government through predetermined investigative business scenarios/transactions as conducted using the VCF system. Approximately 400 issues were captured for further Government review/direction during this 2 week functional review period.

**Gameplan for NEXT STEPs beyond VCF Functional-Review included:**

1. SAIC review of the 400 issues and to identify FIXES (as opposed to changes/new requirements)
2. FBI review of the 400 issues to cite concurrence or non-concurrence on FIXES identified by SAIC
3. FBI review of the 400 issues to identify SHOWSTOPPERS for D1 ("must haves")
4. FBI review of the 400 issues to identify which issues would be included for future maintenance releases (follow-on from D1)
5. **DESCOPE:** Per ETC cost and schedule, FBI to review 400 issues to identify what could be deferred/must be deferred from D1

<b>DATE:</b>	March 23, 2004
<b>ACTION:</b>	FEDSIM Extends ETC Deadline
<b>IMPACT:</b>	COST SCHEDULE REQUIREMENTS

The ETC deadline was extended to April 7, 2004.

FEDERAL BUREAU OF INVESTIGATION  
FOIPA  
DELETED PAGE INFORMATION SHEET

No Duplication Fees are charged for Deleted Page Information Sheet(s).

Total Deleted Page(s) ~ 41

Page 14 ~ Duplicate

Page 15 ~ Duplicate

Page 16 ~ Duplicate

Page 17 ~ Duplicate

Page 18 ~ Duplicate

Page 19 ~ Duplicate

Page 20 ~ Duplicate

Page 21 ~ Duplicate

Page 22 ~ Duplicate

Page 23 ~ Duplicate

Page 24 ~ Duplicate

Page 25 ~ Duplicate

Page 26 ~ Duplicate

Page 27 ~ Duplicate

Page 29 ~ Outside the Scope

Page 30 ~ Outside the Scope

Page 33 ~ Outside the Scope

Page 34 ~ Outside the Scope

Page 43 ~ Outside the Scope

Page 47 ~ b5

Page 48 ~ b5

Page 50 ~ b5

Page 51 ~ b5

Page 52 ~ b5

Page 53 ~ b5

Page 54 ~ b5

Page 55 ~ b5

Page 56 ~ b5

Page 57 ~ b5

Page 58 ~ b5

Page 59 ~ b5

Page 60 ~ b5

Page 61 ~ b5

Page 62 ~ b5

Page 63 ~ b5

Page 64 ~ b5

Page 65 ~ b5

Page 66 ~ b5

Page 67 ~ b5

Page 68 ~ b5

Page 69 ~ b5