



U.S. Department of Justice

Office of Legislative Affairs

---

Office of the Assistant Attorney General

Washington, D.C. 20530

November 30, 2006

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 2, 2006. The subject of the Committee's hearing was "Oversight of the Federal Bureau of Investigation." The FBI submitted these responses for clearance on July 10, 2006. We hope this information is helpful to the Committee.

The Office of Management and Budget has advised us that from the perspective of the Administration's program, there is no objection to the submission of these responses. If we may be of additional assistance in connection with this or any other matter, we trust that you will not hesitate to call upon us.

Sincerely,

A handwritten signature in cursive script, reading "James H. Clinger".

James H. Clinger  
Acting Assistant Attorney General

Enclosure

cc: The Honorable Patrick J. Leahy  
Ranking Minority Member

**Responses of the Federal Bureau of Investigation  
Based Upon the May 2, 2006 Hearing Before the  
Senate Committee on the Judiciary  
Regarding FBI Oversight**

**Questions Posed by Senator Specter**

**FBI Classified Information Questions**

**1. What is the FBI doing to prevent leaks of classified information from within its own ranks?**

**Response:**

All new FBI employees receive briefings on the importance of protecting classified information, the protocols of addressing FBI issues with external contacts, and administrative measures which the Bureau takes against those who mishandle classified material. In addition, new employees sign a Classified Information Non-Disclosure Agreement before they come in contact with any classified information. For employees who are already on board, the FBI also presents security awareness training and mandatory information security training on a regular basis.

Throughout employment with the FBI, all employees undergoes a Periodic Reinvestigation every five years which may include a Personnel Security Polygraph (PSP) examination. The PSP focuses on counterintelligence issues, to include unauthorized disclosures. The PSP is used not only to identify any potential unauthorized disclosures of classified information that may have occurred, but also to serve as a deterrent to unauthorized disclosures by FBI personnel.

**2. On April 30, 2006, The New York Times reported that the Bush Administration is attempting to prosecute publication of classified information by reporters under the Espionage Act of 1917, citing justification given in Justice White's dissenting opinion of *U.S. v. New York Times* (the Pentagon Papers case). Given the FBI's recent attempt to seize Jack Anderson's papers, does the FBI agree that reporters are vulnerable to prosecution under this act?**

**Response:**

Please refer to the 6/6/06 testimony before this Committee of Matthew W. Friedrich, Chief of Staff and Principal Deputy Assistant Attorney General of the

Department of Justice (DOJ) Criminal Division, regarding the application of the Espionage Act of 1917 to the prosecution of reporters.

**3. The FBI has stated that under the law, no private person may possess classified documents that were illegally provided to them by unidentified sources, and that such classified documents remain the property of the US government? Specifically, under which law?**

**Response:**

Numerous mechanisms are available to protect the government's property interest and right to possess and control the dissemination of classified information. Pursuant to 18 U.S.C. § 793, whoever is in unauthorized possession of documents or information related to the national defense and willfully retains the same, and fails to deliver this material to the officer or employee of the United States entitled to receive it, is subject to imprisonment and fine. In addition, 18 U.S.C. § 3663(b)(1) provides that, when sentencing a defendant convicted of a Title 18 offense, the court may order restitution, including the return of stolen property. Executive Order 12958, as amended, establishes that information remains classified and must be protected from unauthorized disclosure until it is officially declassified. This Executive Order further requires that classified information remain under the control of the originating agency and specifies storage and distribution restrictions. Under common law, the owners of stolen property generally retain ownership of the property, even if it is passed to an innocent third party.

**4. Do you agree with the 1971 Supreme Court decision in *U.S. v. New York Times* in which the court stated that a newspaper could be "vulnerable to prosecution"?**

**Response:**

Please see the response to Question 2, above.

**5. A recent *New York Times* article (Liptak, 04/30/06) reported that the FBI recently made efforts to reclaim classified documents allegedly in the personal files of the late columnist Jack Anderson. The FBI has stated no private person may possess classified documents that were illegally provided to them by unidentified sources, and that such classified documents remain the property of the United States government. The *Times* article refers to two Federal statutes in the Espionage Act which prohibits: (1) anyone with unauthorized access to documents or information concerning the national defense from telling others (18 U.S.C. § 793); and (2) the publication of government codes and other "communication intelligence activities" (18 U.S.C. § 798). What is your interpretation of these statutes as they relate to the issue at hand? What is your interpretation of the**

**following statutes, which might also be relevant to the issue at hand: 50 U.S.C. § 421; 42 U.S.C. § 2277; 50 U.S.C. § 783?**

**Response:**

This question requests a legal opinion concerning the interpretation of the specified statutes. The FBI defers to DOJ's longstanding policy of declining to render legal opinions to Congress (except comments on proposed legislation) and others outside the Executive Branch. *See* Request of the Senate for an Opinion, 39 Op. Att'y Gen. 343, 344, 347 (1939).

**6. In your opinion, did Congress intend 18 USC § 798 and 50 USC § 421 to apply to the dissemination of classified information to newspapers and reporters? How about the other statutes mentioned above?**

**Response:**

The referenced statutory provisions identify the classes of persons and the conduct to which they apply. The FBI is not aware of any class of persons, covered by a particular statutory provision, that is generally immune from prosecution under that provision.

**7. How have these three statutes been applied in the past? Who has been prosecuted under these statutes?**

**Response:**

Computerized FBI statistical accomplishment records do not reflect prosecutions occurring under 50 U.S.C. § 421 or 42 U.S.C. § 2277. Two subjects were charged under 50 U.S.C. § 783. Thomas Joseph Dolce, a weapons analyst at the Aberdeen Proving Ground in Maryland, pled guilty to passing classified defense information to the South African government and was sentenced in Federal Court on 04/19/89 to 10 years' incarceration and fined \$5,000. Douglas Simon Tsou, an FBI Language Specialist in the Houston Division, was convicted of passing classified defense information to representatives of the government of Taiwan and sentenced on 01/22/1992 to 10 years in federal prison. Sharon M. Scranage pled guilty to violation of 50 U.S.C. § 421 in 1985 and was sentenced to 5 years' imprisonment, which was ultimately reduced to two years. Lawrence Anthony Franklin pled guilty in January 2006 to violations of 18 U.S.C. §§ 793 and 371 (conspiracy to violate 50 U.S.C. § 783) and was sentenced to 12.5 years in prison. Frederick C. Hamilton pled guilty in 1993 to two counts under 50 U.S.C. § 783(b) and was sentenced to 3 years and one month of imprisonment.

**8. Under which statute do you seek to reclaim the Jack Anderson documents?**

**Response:**

The FBI met with the Anderson family in an effort to review the files with their consent. At this time the FBI is not seeking to reclaim any documents.

**9. In your testimony, you note that it is imperative to protect the nation's security while still preserving our civil liberties. Do you agree that prosecuting reporters under the Espionage Act would protect the nation without unduly burdening freedom of the press?**

**Response:**

DOJ has never in its history prosecuted a member of the press under Section 793, 798, or any other section of the Espionage Act of 1917 for the publication of classified information, even while recognizing that such a prosecution is possible under the law. DOJ's policy in this regard is published at 28 C.F.R. § 50.10, which requires that the Attorney General approve not only prosecutions of members of the press but also investigative steps aimed at the press, even in cases where the press is not itself the target of the investigation. This policy - voluntarily adopted by DOJ - ensures that any decision to initiate criminal proceedings against the press is made at the very highest Departmental level and only after all relevant facts and circumstances have been considered and other options have been exhausted. The Attorney General has stated that DOJ's "primary focus" is on the leakers of classified information, as opposed to the press, and that the country's national security interests and First Amendment interests are not mutually exclusive and can both be accommodated. The FBI fully acknowledges that freedom of the press is vital to our nation and protected by the First Amendment to the Constitution.

**10. What papers is the FBI attempting to seize from Jack Anderson, and why is it trying to take them? Considering that Anderson stopped writing his column in the mid-1980's, at best these papers are twenty years old, and they should have little to do with current issues. There have been allegations that the FBI is interested in them because Anderson discovered certain things about J. Edgar Hoover's personal life; is this true? Or do these papers concern the recent court case against two former AIPAC lobbyists, Steven J. Rosen and Keith Weissman? Feel free to answer this question in a classified session, if you so wish.**

**Response:**

The FBI contacted the Anderson family to seek their consent for an FBI review of files in their possession. Through discussions with the family and others, the FBI confirmed that the files contained documents marked as classified and that the

papers were being reviewed for purposes of making them publicly available. Consistent with our obligations under existing law and Executive Orders, we sought to review the papers to determine, among other things, whether public disclosure of any of them would cause a risk to national security. Access was not sought because Anderson allegedly had information regarding former Director Hoover's personal life.

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

#### FBI TRILOGY Questions

**11. At least \$7.6 million worth of equipment purchased for Trilogy is unaccounted for in a GAO report entitled “Weak Controls over Trilogy Project Led to Payment of Questionable Contractor Costs and Missing Assets” from February 2006. What steps have been taken to locate these assets? Are the Trilogy contractors required to reimburse the FBI for equipment losses? What is being done to ensure that the same missteps are not repeated during the Sentinel or subsequent purchasing projects?**

#### Response:

To provide context for the Report's findings regarding property controls, the FBI notes that more than 44,000 pieces of accountable property were successfully deployed and tracked in the FBI's property management system during Trilogy's development. The Government Accountability Office (GAO) report initially identified 1,404 items (approximately 3% of the total) of unaccounted for or improperly documented property. As of April 2006, the FBI had accounted for more than 1,200 of these items, and we are continuing our efforts to locate or document the remaining Trilogy assets.

It was always the intent of both the FBI and the General Services Administration's (GSA) Federal Systems Integration and Management (FEDSIM) Center to have the Defense Contract Audit Agency (DCAA) conduct final close-out audits to assess final costs, including direct and indirect labor costs. This is the appropriate means of identifying and addressing any potential overpayments to contractors. Close-out audits are designed to disclose and resolve questionable costs of the type GAO reported, as well as costs deemed unallowable under the contract. The initiation of the close-out audits has been delayed until final rates for both the prime contractors and all subcontractors have been approved by DCAA and final reconciliation is completed by both prime contractors. At that time both prime contractors will be able to submit their final invoices and DCAA will be able to complete the final closeout audit. While the prime contractors are reconciling their subcontractor costs and waiting for DCAA approval of their final rates,

GSA/FEDSIM is finalizing negotiations with the GSA Deputy Assistant Inspector General (IG) for Auditing, FBI, and DCAA to have DCAA conduct an overall program audit of both task orders. The scope of the program audit will include the costs identified by GAO as potentially questionable. Upon completion of the program audit, DCAA will conduct the final closeout audit of both task orders. GSA and the FBI will monitor the progress of the close-out audits and will ensure all areas of concern cited in the Report, including the direct labor rates charged by the contractors and their subcontractors, are thoroughly reviewed and resolved.

In preparing for Sentinel, the FBI has taken care to lay the groundwork for a successful major investment. We have created a strong program management office (PMO) with clear reporting lines to the Chief Information Officer (CIO) and the FBI Director. We have staffed the PMO's Office with highly skilled technical, programmatic, business management, and administrative subject matter experts. The FBI will augment that staff with audit support from the FBI's Finance Division to review invoicing, as well as an independent verification and validation (IV&V) contractor to review the accuracy of the development contractor and the PMO, ensuring proper execution and delivery of the Sentinel system.

The GAO and Department of Justice (DOJ) IG are both performing audits of the Sentinel program throughout its development to provide assessments concerning the PMO's progress in delivering and implementing the Sentinel system. The DOJ CIO, Deputy Attorney General (DAG), Office of the Director of National Intelligence (ODNI), and Office of Management and Budget (OMB) are all meeting with the Sentinel Program Manager and senior managers in the Office of the CIO (OCIO) and the Finance Division in various forums to ensure the Sentinel program is proceeding as planned and the contracted system will be delivered to the users on time, within cost, and with the required capabilities.

In accordance with the FBI's Life Cycle Management Directive (LCMD), the Sentinel program is required to present its programmatic, architectural, technical implementation, and operational readiness updates to several enterprise level control boards in order to ensure the end product of the development activity meets the criteria for investment alignment with the FBI's strategic planning, enterprise architecture, systems engineering standards, and operation and maintenance policies and practices. Finally, the contract vehicle is structured so that the contractor has clear reporting requirements, deliverables, and milestones.

**12. GAO reports over 1200 pieces of equipment, worth \$7.6 million, is unaccounted for from the Trilogy project. Additionally, 30 pieces of equipment worth almost \$167,000 were reported as being lost or stolen. Does it concern you that assets that may be sensitive in**

**nature are not only missing from FBI warehouses but may also have been stolen? Can you describe the protocols the FBI uses to track its assets?**

**Response:**

Any loss or theft of property is a concern, and the FBI took immediate action to locate those items listed as unaccounted for by the Report that, if lost, would have posed a potential security breach.

The FBI tracks assets, from acquisition through disposal, consistent with the Federal Management Regulation (41 C.F.R. § 102), the DOJ Property Management Regulations (41 C.F.R. § 128), and applicable Federal property management regulations promulgated by GSA and OMB. This includes maintaining inventory, upon receipt, for all accountable property in the system of record. Accountable property includes all hardware with an acquisition cost of \$1,000 and greater, all software with an acquisition cost of \$500,000 and greater, and - regardless of cost - all firearms, COMSEC equipment, laptop computers, jewelry, and central processing units. These five classes of property are considered controlled personal property, or sensitive property, which are subject to a high probability of theft or misuse due to their inherent attractiveness and/or portability. Property valued at \$25,000 or more is a capital asset. Property management is decentralized in the FBI, with accountability assigned to an Accountable Property Officer in each Division, Field Office, or Legal Attaché. The Finance Division exercises centralized oversight of property management through annual inventory of capital assets and sensitive property, biannual inventory of all accountable property, semi-annual reviews of orders and transfers, and periodic reviews and audits of sensitive and accountable property.

The agreement with the Trilogy contractor resulted in modified property management procedures. In its discussion of control over Trilogy assets, the Report notes the FBI did not require compliance with its normal procedures for documentation of shipments from contractors. In discussions with GAO staff and in materials provided to GAO, the FBI explained that the normal policy was modified in order to maintain the contractor's control of the shipments until the contractor completed the installation process. In effect, while the FBI received the shipments, we did not accept delivery until the contractor processed the contents of those shipments. This modification for the Trilogy program should not be construed as a systemic lapse in the FBI's property management policies.

The FBI is focused on improving property management, reinforcing existing policies and instituting stronger reporting and accountability across the FBI. KPMG, the independent auditor cited in the Report and contracted by the DOJ IG to check the health and accuracy of the FBI's financial statements, recently



changed the FBI's property and equipment grade from a material weakness to a reportable condition, stating, "During fiscal year 2005, the FBI showed progress in resolving several of the issues noted in prior year audits, and has worked towards implementing effective and routine controls."

#### FBI Sentinel Questions

**13. A *U.S. News and World Report* article entitled "High tech's High Stakes at the FBI" (U.S. News & World Report, 4/17/06), states "Some executives believe the bureau's computer upgrades (i.e. Sentinel) could ultimately total a billion dollars--double the projected costs ... at the bureau, tensions are rising as many officials stew over what they view as imprudent across-the-board cost cutting to hide Sentinel's *real* price tag from Congress and spare Mueller further ignominy." Including the costs of transferable assets from VCF, what is the total cost of Sentinel?**

#### Response:

The total value of the contract with Lockheed Martin is \$305 million over 6 years, including both development and Operations and Maintenance (O&M). The FBI estimates that the total cost of the Sentinel Program, including program management, systems development, O&M, and IV&V, will be \$425 million over 6 years. Sentinel's total cost is depicted in the below tables. (The first table breaks the costs out by activity, while the second table depicts costs by phase.) The assets developed in the course of the Trilogy project, including Virtual Case File (VCF), were reinvested in the FBI's overall enterprise network before award of the Sentinel contract and are, therefore, not appropriately attributable to Sentinel.

ACTIVITY	COST
Pre-Award	\$ 4.3M
Program Management Operations	74.8M
IV&V	6.0M
Risk Management	35.0M
Development Contract	232.4M
Operations and Maintenance	72.7M
<b>TOTAL</b>	<b>\$425.2M</b>

PHASE	COST
Pre-Award	\$ 4.34M
Phase 1	97.0M
Phase 2 (+Pre-FOC O&M)	150.3M
Phase 3 (+Pre-FOC O&M)	51.7M
Phase 4 (+Pre-FOC O&M)	79.8M
O&M Years 1 and 2	42.1M
<b>TOTAL</b>	<b>\$ 425.24M</b>

**14. At our last FBI Oversight hearing in July 2005, we discussed the timing of completion of the Sentinel project and how that might impair the effective coordination of intelligence efforts against current terrorist threats. Now that you have more concrete plans as to when Sentinel will be completed, do you anticipate this being a problem?**

**Response:**

No, we do not anticipate this being a problem. With the development of both the Case Management Line of Business and the National Information Exchange Model (NIEM) to improve intelligence efforts, the timing of the Sentinel project is good, since the Sentinel efforts can assist in guiding both.

**FBI Translation Problems Questions**

**15. In your written responses from last July's hearing, over 3,000 employees and contractors are reported to be certified in language proficiency at or above the working proficiency level. What is the turnover rate among these employees and contractors?**

**Response:**

For the past 5 years, annual language analyst attrition has ranged between 5 and 8%, and contract linguist attrition has been between 9 and 11%. Competition for high-quality language services in the public and private sectors is fierce, and others are willing to pay steep premiums for resources already vetted by the FBI. Many departing employees have cited the lure of the higher salaries offered in the private sector as the primary reason for their separation. Despite these factors, however, Foreign Language Program attrition remains relatively low. Innovative retention programs, such as a Foreign Language Proficiency Pay Program, are currently under consideration within the FBI. These programs, partnered with other career-enhancing opportunities now being afforded to linguists, are expected to reduce attrition even further.

**16. According to IG Glenn Fine, the FBI's counterterrorism audio backlog was 4,086 hours as of April 2004 and in a follow up review, has doubled to 8,354 hours. What is the current amount of unheard audio? What have you done to remedy this problem?**

**Response:**

Of the several hundred thousand hours of audio materials and almost two million pages of text collected in connection with counterterrorism investigations over the last 4 years, only 1.35% of all audio (7,028 hours out of 519,217 hours collected), 0.48% of all electronic data files (26,518 files out of 5,508,217 files collected), and less than 0.0001% of all text (62 pages out of 1,847,497 pages collected) were backlogged as of February 2006.

Of the accrued backlog, 31.23% is attributable to elongated "white noise" microphone recordings resulting from certain techniques not expected to yield intelligence of tactically high value (2,195 hours of open microphone recording out of the total audio backlog of 7,028 hours). Another 46.1% (3,240 hours out of the total audio backlog of 7,028 hours) is audio from very obscure languages and dialects. The FBI is currently recruiting the linguists necessary to address this backlog.

The FBI now possesses sufficient translation capability to promptly address all of the highest priority counterterrorism intelligence, often within 24 hours. The FBI's prioritization and triage processes are helping to reduce the accrued backlog. The FBI continues to hire as many linguists as can be cleared, and we are hiring them in field offices where traditionally there were none. The FBI currently has 1,379 linguists, with the capability of translating in approximately 100 languages, a 76% increase in the overall number of linguists since 9/11/01, with the number of linguists in certain high priority languages (e.g., Middle Eastern and North African languages) increasing by 200% and more. In addition, the FBI is obtaining qualified and cleared linguist support from other available sources (including from within the United States Intelligence Community (IC)) through the National Virtual Translation Center, as well as from the language programs of allied intelligence agencies.

**17. According to FBI statistics, it takes approximately 13 to 14 months to hire a contract linguist. Has improvement been made in this area?**

**Response:**

During the past 18 months, the FBI has worked to implement re-engineered procedures that will increase the efficiency of the processing lifecycle of contract linguist applicants. Through a contractor-based partnership, the FBI is designing

an applicant communication and management system, called the Contract Linguist Automated Support System (CLASS), for all contract linguist applicants.

This initiative was based on a business process improvement study, the purpose of which was to identify, document, and provide solutions for bottlenecks, inefficiencies, outdated technologies, and underlying environmental and cultural factors that contribute to the lengthy contract linguist applicant process. The study generated recommendations that will enhance many of the processing steps, including prescreening, language proficiency testing, suitability determinations, contract issuance, and invoice payments.

The contractor has gathered nearly all the information necessary for the design and development of CLASS. The FBI's robust LCMD ensures this system will meet the criteria established by our Records Management, Information Technology (IT) Operations, and Security Divisions, as well as by the FBI's Office of the General Counsel (OGC). With an anticipated rollout in the summer of 2007, CLASS is expected to reduce contract linguist application cycles by as much as five months.

**18. It has been alleged in an article that despite a shortage of Arabic translators, the FBI turned down applications for linguist jobs from nearly 100 Arabic-speaking Jews in New York following the World Trade Center attacks. (Sperry, 10/09/03) Is this true? It has further been alleged that "the FBI was concerned that many of the applicants were "too close to Israel," and might lack the objectivity to accurately translate the Arabic recordings and writings of Muslim terrorist suspects under investigation. Indeed, some worked for the Israeli military." Why were all of these individuals turned down? Are non-Jewish Arabs similarly evaluated as to potential biases?**

**Response:**

These unsubstantiated allegations relate to a meeting between our New York Field Office (NYFO) and Sephardic Bikur Holim (SBH), a New York-based charity, after 9/11/01 to discuss how the charity's membership could assist the FBI. During this meeting, NYFO representatives explained that generally only United States citizens can be considered for the FBI's contract linguist positions because of the requirement for a "Top Secret" security clearance. Executive Order (EO) 12968, "Access to Classified Information," Section 3.1(B), provides that, with certain limited exceptions, "access to classified information shall be granted only to employees who are United States citizens." (While the EO does permit an agency to grant limited access to foreign nationals under some circumstances, both the scope of the work required and the restrictions placed on that access militated against the exercise of that authority in this case.)

After this meeting, an SBH representative provided NYFO with the names and telephone numbers of possible candidates and NYFO personnel immediately contacted them. Because many of these individuals reported that they were not United States citizens, we did not invite them to apply for contract linguist positions. However, we did encourage individuals who were United States citizens to submit applications.

The SBH list included 55 type-written names and 4 illegible handwritten names. Of the 55, 32 did not apply for positions, 3 submitted applications but were discontinued because we were unable to contact them using the information provided in their applications, and 2 withdrew from processing before proficiency testing. 18 of the listed individuals submitted to the first phase of the application process: language proficiency testing. Of these:

- 15 applicants were discontinued because they failed to pass language proficiency tests;
- 1 applicant was considered for a language specialist position in 1999, but was discontinued during the course of the background investigation based on a lack of candor;
- 1 applicant passed language proficiency tests but was discontinued because the polygraph examination indicated deception; and
- 1 applicant successfully completed each stage of processing and was approved as a contract linguist in October 2003.

All SBH members who applied for contract linguist positions were processed in a manner fully consistent with FBI rules and procedures. One of these applicants successfully completed the vetting process and is now making a valuable contribution to the FBI as a contract linguist assigned to NYFO. These results are not inconsistent with our normal rate of successful contract linguist applications.

#### FBI Seaport Security Questions

**19. A recent IG report, “FBI’s Efforts to Protect the Nations Seaports,” indicates that unless agreements are reached for incident command and other coordination issues, the overlapping responsibilities of the Coast Guard and the FBI could result in confusion in the event of a maritime incident. What is the FBI doing to reach these agreements? When will these agreements be finalized?**

**Response:**

The FBI is actively working with the United States Coast Guard (USCG) to resolve coordination issues in advance of actual threats and incidents in the maritime domain. The FBI's efforts are conducted in accordance with the Maritime Operational Threat Response (MOTR) Plan, which was approved by the President and is one of eight supporting plans under the National Strategy for Maritime Security as required by National Security Presidential Directive 41/Homeland Security Presidential Directive (HSPD) 13. The MOTR Plan was developed under the joint leadership of the Department of Homeland Security (DHS) and the Department of Defense (DoD), with DOJ and FBI participation. The current MOTR Plan is an interim plan that was approved by the President in October 2005. This interim plan is currently being revised, and we anticipate that the final plan will be approved by the President by late 2006. The final MOTR Plan will recommend protocols for each agency and will provide guidance for interagency coordination in response to maritime threats and incidents. After the final MOTR Plan is adopted, the FBI and USCG will address the need for an MOU, if any.

The MOTR Plan provides a framework for interagency communication and coordination in response to maritime threats and incidents. MOTR conference calls, made through the existing network of federal command centers, have been used to successfully resolve several real-world incidents over the past few months. The FBI and USCG agree that these coordination mechanisms have dramatically improved the operational response to maritime threats and incidents, and we have jointly briefed the MOTR Plan to interagency audiences.

The FBI has taken several additional steps to ensure a coordinated response to an incident of maritime terrorism. In July 2005, the FBI initiated the Maritime Security Program (MSP), the mission of which is to prevent, disrupt, and defeat criminal acts of terrorism directed against maritime assets and to provide counterterrorism preparedness leadership and assistance to Federal, state, and local agencies responsible for maritime security. The MSP will complement the efforts of other United States Government entities, focusing on core FBI competencies that include the establishment of a human intelligence (HUMINT) base, the collection and distribution of relevant information and intelligence, the preparation of threat and vulnerability analyses, and the provision of investigative support. The MSP emphasizes the importance of its liaison relationships with the USCG and other agencies, participating with the Coast Guard Investigative Service (CGIS) and others in formal and informal interagency working groups. Recently, both the USCG and Naval Criminal Investigative Service (NCIS) have assigned full time representatives to the MSP.

The MSP also provides guidance to approximately 80 Maritime Liaison Agents (MLAs), who are assigned to the FBI's Joint Terrorism Task Forces (JTTFs) throughout the United States. MLAs include FBI Special Agents (SAs) as well as JTTF Officers from the CGIS, NCIS, state and local port authorities and police departments, and others. The FBI recently hosted an MLA training conference that included representatives and presentations from the FBI, DOJ, USCG Headquarters, USCG field operations, CGIS, NCIS, and other Federal and local law enforcement agencies. Conference training included the authorities and capabilities of these agencies as well as best practices and guidelines for operational responses to maritime terrorism threats and incidents.

The FBI and the USCG train together to ensure coordination and interoperability in response to maritime terrorism threats and incidents. Fifteen of the FBI's Special Weapons and Tactics (SWAT) teams are Enhanced Maritime SWAT Teams with specialized training and equipment. These enhanced teams are available to conduct joint exercises with the USCG. In addition, the USCG has invited representatives of the FBI's Hostage Rescue Team and Weapons of Mass Destruction Operations Unit to act as observers and to provide feedback during an upcoming exercise.

**20. This same IG report also states that the FBI is concentrating its intelligence efforts on a narrow group of attack scenarios and not devoting resources to high-risk areas. For example, the FBI is concentrating significantly on attacks carried out by combat swimmers and not the smuggling of a weapon of mass destruction being shipped in a cargo container. What is the FBI doing to address this concern?**

**Response:**

The FBI is responsible for acting on maritime threats that may have a nexus to terrorist or criminal acts directed against the United States or its interests and, for this reason, it does not concentrate intelligence efforts solely on a narrow group of attack scenarios. To ensure the FBI is positioned to efficiently and effectively execute its maritime responsibilities, the FBI initiated the MSP, which has the full-time participation of both the NCIS and USCG in order to provide MSP management at the national level. Through the MSP, the FBI, NCIS, and USCG jointly and collaboratively address all identified maritime threats.

**21. The FBI has instituted Maritime Liaison Agents (MLA). These agents are assigned to FBI field offices and are responsible for coordinating with the agency's maritime partners including CBP and the USCG. However, the IG audit states that the FBI assigns MLA's indiscriminately, without assessing the threat and risk of terrorists attacking each port. This has led to irrational decisions, such as assigning only one MLA to the New Orleans field office, which has six significant ports in its territory, while assigning five MLA's to the**

**Louisville field office, which has no strategic ports in its area. Is the FBI preparing to implement a threat assessment plan for the positioning of MLA's? And if not, why not?**

**Response:**

In July 2004, the FBI established a requirement that Field Offices having maritime liaison responsibilities in connection with oceans, rivers, or large lakes identify field personnel to be assigned to the MLA Program as a collateral duty. Other than the requirement to establish the MLA position, how maritime liaison is addressed by each Field Office from a resource standpoint is left to the discretion of the Special Agent in Charge (SAC). For example, the Louisville, Kentucky, Field Office has 11 "resident agencies" dispersed throughout the state. The Louisville SAC determined that maritime liaison activities could best be managed in his Field Office by assigning MLA collateral duty to five SAs stationed in that Division's resident agencies because those SAs are most familiar with the maritime activities and venues and with the Federal, state, and local resources and personnel in their assigned areas. By contrast, the New Orleans Field Office includes a significantly different maritime venue, and that SAC's assessment led to a different approach. In the New Orleans Division, two JTTF officers are assigned as MLAs and have this role as their primary responsibility. In addition, because of the prevalence in southern Louisiana of maritime resources and personnel from the USCG, Customs and Border Protection, and state and local law enforcement agencies, the FBI is able to leverage these resources in the New Orleans Division, which is not necessarily possible in other areas.

**22. The FBI does not have a method of tracking the amount of time its agents spend preventing or investigating maritime terrorism. Currently, under the FBI's case classification system, most MLA activities are designated as "Counterterrorism Preparedness - Other." This classification is not specific enough to allow managers of the FBI's maritime efforts to determine the amount of resources the FBI is spending maritime issues, which prevents the implementation of a risk-based counterterrorism program. Is the FBI planning on changing its classification system to solve this problem? If not, why not?**

**Response:**

Because of the establishment of the MSP and the requirement to designate MLAs in all FBI Field Offices, the FBI's focused maritime security work has increased considerably. This increase has demonstrated a need to review our classification system to determine if changes are warranted. This review is ongoing.



## Random Questions

**23. Several times, the FBI has refused to produce its agents for interviews with the Judiciary Committee. Each time, they have claimed that existing DOJ policy bars them from producing these agents, citing a letter, originally sent out in 2000, written by then Assistant Attorney General Robert Raben. However, the DOJ/FBI's reasoning behind this policy is not a correct reading of the law and/or history. (see CRS Report "Investigative Oversight" by Rosenberg, 1995) Does the FBI support this policy of impeding Congressional oversight? If so, will they be willing to produce more supportive evidence for this policy? If not, are they willing to go on record as opposing this policy?**

### Response:

The FBI is committed to complying with Congressional oversight requests to the fullest extent consistent with the constitutional and statutory obligations of the Executive Branch and to making every effort to accommodate the needs of the legislative branch to perform its oversight function. We support DOJ's policy of protecting the independent judgment of line SAs by ensuring that the supervisory personnel who serve as decisionmakers are the ones who answer to Congress for those decisions. Please note that the January 27, 2000 letter from Assistant Attorney General Robert Raben cites case law, formal DOJ legal opinions, and correspondence from members of the United States Senate and House of Representatives in support of its policy for responding to Congressional oversight requests.

**24. Glenn Fine, the Justice Department's Inspector General, said in a February 17, 2006 briefing that the FBI email system automatically deletes messages that are 60 days old unless an affirmative action is taken to archive emails by the user. Do you believe this system is conducive to appropriate oversight of the FBI? Are there any problems that could arise if a message has been automatically deleted that may be necessary after the 60-day window?**

### Response:

The FBI's Exchange email system has three locations for message storage. The first location is an enterprise repository that stores a copy of every email message created and sent. Messages remain in the enterprise repository for 90 days. Messages older than 90 days are automatically deleted from the repository pursuant to Records Management Division (RMD) policy.

Messages are also stored in personal mailboxes. Every FBI employee has a personal mailbox, and each employee is responsible for managing that personal mailbox (deleting and archiving messages, organizing messages within files, etc).

Messages stored in a user's personal mailbox are not deleted after 90 days. Only the user can delete messages from the personal mailbox.

The third location in which mail messages are stored is the personal archive file (PST file). Users can move mail out of their personal mailboxes and into PST files. The movement of files from a user's personal mailbox to a PST file is controlled by the user, as is the deletion of files from a user's PST file. PST files have no set retention time. Messages within a PST file are deleted only if the user takes action to delete them.

**25. Committee staff was briefed by the Foreign Terrorist Tracking Task Force (FTTTF) that 2 terrorists a week are detected in the United States and those leads are forwarded to the Joint Terrorism Task Force (JTTF). We know from the FTTTF representative who briefed our staff that 2 of the 9/11 hijackers were on the terror watch list, but the information was not communicated to the JTTF. Have you identified the cause of the breakdown, and taken steps to avoid its reoccurrence?**

**Response:**

Before the attacks of 9/11/01, multiple terrorist watchlists were maintained by various Federal agencies without review by or coordination with other agencies. The two 9/11 hijackers referenced in the question were on the Department of State (DOS) watchlist referred to as TIPOFF at the time of the attacks, but the FBI was not aware of this. Following the 9/11 attacks, HSPD 6 (9/16/03) mandated the creation of the Foreign Terrorist Tracking Task Force (FTTTF) and the Terrorist Screening Center (TSC) to ensure watchlists and terrorist tracking efforts are coordinated throughout the Federal government.

The TSC was created to systematize the Government's approach to terrorist screening and to the maintenance of secure, consolidated terrorist identity information. The TSC shares watchlist information with Federal, state, local, territorial, and tribal law enforcement agencies and with others in the IC.

The FTTTF was created to provide information that helps to keep foreign terrorists and their supporters out of the United States or that leads to their location, detention, removal, prosecution, or other appropriate action. The FTTTF uses innovative techniques to provide the information necessary to fill gaps relating to the location of known or suspected terrorists and terrorism supporters. Like the TSC, the FTTTF shares this information with Federal, state, local, territorial, and tribal law enforcement agencies and with others in the IC.

**26. A June 2005 OIG report entitled “A review of the Terrorist Screening Center” found that the watch list could be missing names, some names might be designated at inappropriate threat levels and that the FBI hasn’t given other agencies full access to its watch list. Is this still a problem?**

**Response:**

The TSC is charged with developing an accurate watchlist of known and suspected terrorists. These identities and the derogatory information describing their specific nexus to terrorism are passed to the TSC through the watchlist nomination process by either the National Counterterrorism Center (NCTC) (for international terrorism subjects) or the FBI (for domestic terrorism subjects).

Upon the receipt of an NCTC or FBI nomination, the TSC conducts an individual review of the available information, including the derogatory information on which the nomination is based. If this information supports placement on the watchlist, the identity is included on all watchlists for which it qualifies, including the Violent Gang and Terrorist Organization File (VGTOF), the Transportation Security Administration (TSA) Selectee and No Fly lists, DHS' Interagency Border Inspection System, the DOS Consular Lookout and Support System, as well as to the Canadian and Australian governments through programs called TUSCAN and TACTICS, respectively. Each of these lists has specific minimum criteria for inclusion. For example, inclusion on TSA's No Fly list requires that the nomination contain a full date of birth in addition to other specific derogatory information, and citizenship status affects inclusion in TUSCAN and TACTICS.

The FBI requires that all subjects of domestic terrorism full investigations be watchlisted and that all subjects of international terrorism preliminary or full investigations be nominated for watchlisting (watchlisting the subjects of domestic terrorism preliminary investigations is at the discretion of the field office involved). Consequently, these identities will also be included in the other watchlists for which the subject qualifies. From these lists, other agencies have access to information regarding FBI subjects.

**27. In a recent article, Judge Richard Posner stated, “We would probably be better off with a different reorganization (of intelligence) with ... a domestic intelligence agency separate from the FBI.” (Posner, 04/11/06.) Do you disagree with this assessment? Why do you disagree with him?**

**Response:**

The FBI believes there is no reason to separate the functions of law enforcement and domestic intelligence. On the contrary, combining law enforcement and

intelligence affords us ready access to every weapon in the government's arsenal against terrorists, allowing us to make strategic and tactical choices between the use of information for law enforcement purposes (arrest and incarceration) or intelligence purposes (surveillance and source development).

The benefits of this approach have been clearly borne out. Since 9/11/01, the FBI has identified, disrupted, and neutralized numerous terrorist threats and cells, and we have done so in ways an intelligence-only agency like the United Kingdom's MI-5 cannot.

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

- A worldwide network of highly trained and dedicated SAs;
- Intelligence tools to collect and analyze information on threats to national security;
- Law enforcement tools to act against and neutralize those threats;
- Expertise in investigations and in the recruitment and cultivation of human sources of information;
- Longstanding and improving relationships with those in state and local law enforcement, who are the intelligence gatherers closest to the information we seek from these communities; and
- Nearly a century of experience working within the bounds of the United States Constitution.

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

Experience has taught the FBI that there are no neat dividing lines distinguishing criminal, terrorist, and foreign intelligence activities. Criminal, terrorist, and foreign intelligence organizations and activities are often interrelated or interdependent. FBI files contain numerous examples of investigations in which information sharing between counterterrorism, counterintelligence, and criminal intelligence efforts and investigations was essential to the FBI's ability to protect the United States from terrorists, foreign intelligence activities, and criminal efforts. Some cases that begin as criminal cases become counterterrorism cases,

and vice versa. The FBI must sometimes initiate parallel criminal and counterterrorism or counterintelligence cases to maximize the FBI's ability to identify, investigate, and address threats to the United States. The success of these cases is entirely dependent on the free flow of information between the respective investigations, investigators, and analysts.

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

In arguing that a separate domestic intelligence agency should be created, Judge Posner asserts that "the bureau's conception of intelligence is of information that can be used to obtain a criminal conviction." We emphatically disagree with this assertion. In the nearly 4½ years since the attacks of 9/11/01, the FBI has undergone a dramatic transformation from a law enforcement agency focused on investigating crimes after the fact into an intelligence and law enforcement organization focused largely on preventing terrorist attacks. We have entered an era of unprecedented information sharing among the law enforcement and intelligence communities and we are continuing to build on our success in strengthening our intelligence capabilities.

The most recent step in the FBI's evolution is the establishment of its National Security Branch (NSB), which combines the capabilities, resources, and missions of the Counterterrorism Division (CTD), the Counterintelligence Division (CD), and the Directorate of Intelligence (DI) under one leadership umbrella. The NSB will build on the FBI's strengths, ensure the integration of national security intelligence and investigations, promote the development of a national security workforce, and facilitate a new level of coordination with others in the IC.

Three major assessments of the FBI's intelligence capabilities have agreed that the FBI should retain its domestic intelligence responsibilities: the report of the National Commission on Terrorist Attacks Upon the United States (9/11 Commission), the assessment by the National Academy of Public Administration (NAPA) of the FBI's transformation, and the report of The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction (WMD Commission). In its March 2005 report, "Transforming the FBI: Progress and Challenges," the NAPA Panel on FBI Reorganization wrote:

"This Panel, like the 9/11 Commission, is convinced that the FBI is making substantial progress in transforming itself into a strong domestic intelligence entity, and has the will and many of the competencies required to accomplish it. That Panel recommended that the FBI continue to be the key domestic intelligence agency responsible for such national security concerns as terrorism, counter-intelligence, cyber, and transnational criminal activity."

The WMD Commission also examined the FBI's intelligence program and concluded in March 2005 that it had been significantly improved since 9/11/01. The commission rejected the need for a separate agency devoted to internal security without any law enforcement powers, recognizing that the FBI's hybrid intelligence and investigative nature is one of its greatest strengths and emphasizing the importance of the ongoing effort to integrate intelligence and investigative operations. At the same time, the commission noted that the FBI's structure did not sufficiently ensure that intelligence activities were coordinated with the rest of the IC. Accordingly, the commission recommended the creation of a "National Security Service." In response to the President's directive endorsing that recommendation, the FBI created the NSB.

**28. It has been alleged that some of the new FBI analysts were administrative assistants at the FBI who were promoted to the analyst position, without an actual change in their job positions or responsibilities. Is this allegation true?**

**Response:**

This is not true. The FBI is hiring Intelligence Analysts (IAs) who possess critical skills and meet both educational and professional qualifications. The FBI's internal applicants for IA positions must meet the same qualifications as external candidates. FBI metrics indicate that qualification standards for IAs have steadily increased in terms of both education and critical skills. More than 90% of all FBI IAs hired within the last 2 to 5 years have bachelors' degrees and more than 48% have advanced degrees. New FBI IAs also possess critical skills in such areas as Islamic studies, international banking, analytical studies, and computer science.

**29. Given Choicepoint's substantial history of compromised databases, why has the FBI chosen to contract out information analysis to them?**

**Response:**

The FBI awarded a 5-year, fixed-price contract to i2, Inc., a subsidiary of ChoicePoint, on 12/1/05. ChoicePoint issued a press release announcing this contract on 4/3/06, which created some confusion as to whether the contract was for ChoicePoint data services or for i2 analytical tools. In fact, this contract is

solely for i2's software applications and analytical tools, and not for ChoicePoint data services. These i2 applications and tools include software licenses, software upgrades, technical support for i2's primary product, the "Analyst's Notebook," a scaled-down version of i2's "Visual Notebook," and related tools. The "Analyst's Notebook" is a link-node analysis tool that has proven highly useful in counterintelligence, counterterrorism, and criminal investigations that involve large volumes of data.

The FBI also continues to use ChoicePoint's data services, and we are committed to continuing to use this information responsibly. In pursuit of our national security and criminal investigative missions, FBI SAs and analysts must have access to the same types of information, with appropriate safeguards, to which an average private investigator or paralegal can subscribe. Commercial databases such as ChoicePoint contain public information (which includes information obtained from public sources) as well as proprietary information that is privately owned and commercially available at the discretion of the owner. This information is available to the FBI from the same sources that provide it to the commercial databases. What commercial databases offer their customers, including the FBI, by contract is a consolidation of this information so that, rather than going to multiple databases for this information, it can be obtained through one or two searches.

The FBI's contracts with commercial databases do not, in any respect, undermine the FBI's obligation to comply with all federal laws that protect an individual's privacy including, among others, the Privacy Act, the Right to Financial Privacy Act, and applicable provisions of the federal tax code. In other words, the FBI can only collect and retain data available from commercial databases in compliance with applicable federal law.

The United States Constitution and the United States Congress, through legislation, carefully delineate acceptable conduct in law enforcement investigations and intelligence activities. The FBI has an unwavering commitment to adhere to those requirements, as well as those mandated by federal regulations and the Attorney General's Guidelines. Whether the work is performed manually or in an automated fashion, that commitment does not change. The FBI exercises due diligence to ensure that the use of public source data is in furtherance of the FBI's mission and consistent with applicable privacy laws, regulations, and policies.

**30. The turnover rate for the position of Executive Assistant Director (EAD) for Counterterrorism and Counterintelligence has been remarkably high, with a total of six over the past five years. This month, current EAD Gary Bald announced his retirement after only six months on the job. This turnover is clearly harming the efforts of the FBI to**

**improve its counterterrorism and counterintelligence activities. Will you require the next EAD, prior to his or her promotion, to agree to stay on for at least two years, if not more? If not, why not? Will you require other potential FBI leaders to make similar agreements?**

**Response:**

We disagree that the turnover in the position of Executive Assistant Director (EAD) for Counterterrorism and Counterintelligence has harmed the efforts of the FBI to improve those programs. The success of the FBI's national security programs is not dependent upon a single person. The leadership teams in both CTD and CD have decades of operational experience and have successfully developed effective programs at Headquarters and throughout the field offices. With regard to the promotion of future executives, minimum time commitments may be discussed but are not enforceable.

**31. The FBI is perhaps the only law-enforcement agency in the country that doesn't use standardized promotional exams or any other objective criteria in selecting managers for advancement. Why not?**

**Response:**

The FBI does, in fact, use standardized promotional assessments in selecting managers for advancement. The FBI has recently implemented a new, three-phased standardized and professionally validated promotion system, called the SA Mid-Level Management Selection System (SAMMSS). This promotion system, which was recently implemented as part of a settlement agreement (Johnson et al v. Ashcroft, Civ. No. 93-0206 (DDC)), emphasizes the managerial and leadership skills required to lead others in the execution of the FBI's National Security and Law Enforcement Mission. These managerial and leadership skills were established as essential for all GS-14 and GS-15 SA mid-level managerial positions through three separate job analyses conducted in conformance with professional and legal guidelines, including the 1978 Equal Employment Opportunity Commission Uniform Guidelines on Employee Selection Procedures. The FBI especially wanted to emphasize the importance of leadership and management in its managerial cadre; therefore, the promotion system focuses on both the technical knowledge and the managerial and leadership skills required to perform any managerial job. The eight core managerial competencies identified through the three job analyses upon which the promotion system is based include: leadership, interpersonal ability, liaison, planning and organizing, problem solving, flexibility and adaptability, initiative, and communication. These competencies are measured and evaluated in a standardized manner throughout the different phases of the SAMMSS.



**32. The FBI's Office of Professional Responsibility (OPR) and the Internal Investigations Section (IIS) of the FBI Inspections Division seem to be having problems doing their jobs. Twice recently, in cases involving 1) the murder of Assistant US Attorney Jonathan Luna and 2) potential retaliation against FBI agent Mike German, the OPR and the IIS mischaracterized these cases as involving only "performance issues" rather than "misconduct issues," only to have the Department of Justice's Inspector General contradict them. Why is this happening? How many times in the last five years has the IG reached opposite conclusions than an FBI investigative unit? If the FBI is unable to police itself, do you feel that this task should be taken away from it and given to the IG?**

**Response:**

Director Mueller commissioned a comprehensive review of the FBI's internal disciplinary process in May 2003 to be led by former United States Attorney General and Federal Judge Griffin B. Bell and by former FBI Associate Director Dr. Lee Colwell. The Bell Colwell study looked at all aspects of the FBI's internal disciplinary process, including its structure, responsibilities, standards, and processes. A final report was provided to the FBI in February 2004 and its recommendations were adopted. Organizational changes included the April 2004 transfer of the Internal Investigations Section (IIS) from the FBI's Office of Professional Responsibility (OPR) to its Inspection Division. Other changes, including policy directing that an OPR matter will not be discontinued or closed when the subject retires or resigns during the pendency of an investigation if necessary to protect the FBI's institutional interests, became effective in November 2004. The cases cited in the question were investigated and adjudicated before implementation of the Bell Colwell recommendations.

The Inspection Division's IIS does not maintain a record of its differences with DOJ's Office of the Inspector General (OIG). It is the FBI's understanding that the OIG also does not maintain a record of these differences. Under the current structure, the IIS coordinates closely with the OIG but the FBI and the OIG generally do not investigate the same cases and, therefore, seldom have the opportunity to reach different interpretations or investigative conclusions. While longstanding DOJ policy does not permit the FBI to comment on the outcomes of such investigations, in neither of the two cases cited in the question did the OIG and the FBI examine the same conduct of the same individual and reach different conclusions. Under the current structure, the OIG reviews all allegations of misconduct by FBI personnel, chooses to investigate a small fraction of those allegations, and refers the remainder back to the IIS for independent evaluation and appropriate action. The OIG also monitors the FBI's internal investigations as appropriate and can assume responsibility for an ongoing investigation at any time. When the OIG investigates an FBI employee, the IIS and other FBI entities cooperate with the OIG and assist to the extent the OIG deems appropriate.

Because the OIG can intervene at all these points, the OIG does, in fact, "police" the FBI.

The FBI is completely able and willing to "police itself" and it cooperates fully in OIG investigations of FBI personnel. The FBI maintains an entire Section dedicated solely to internal investigations, and that Section can and does draw on others in the FBI to support its mission, including Supervisory Special Agents (SSAs), Assistant Special Agents in Charge (ASACs), Unit Chiefs, and even Senior Executive Service (SES) officials. The FBI's OPR is dedicated solely to the independent adjudication of internal investigation results. When appropriate, other FBI Divisions conduct criminal investigations of FBI personnel. For decades, whether a matter was as relatively minor as the inadvertent loss of identity documentation or as significant as espionage, the FBI has "policed itself" with a total commitment to professionalism, thoroughness, and objectivity.

**33. The Department of Justice Reauthorization Act of 2005 directs the FBI to establish a task force to combat organized retail theft. Since this bill's passage, the FBI has seemingly done little to implement this task force. Is there a reason for the FBI's inaction?**

**Response:**

The FBI has been actively engaged in establishing a task force to combat organized retail theft. Section 1105 of the Violence Against Women and DOJ Reauthorization Act of 2005, Pub. L. No. 109-162, 119 Stat. 2960, 3092 (1/5/06), directs the Attorney General (AG) and the FBI, in consultation with the retail community, to "provide expertise to the retail community for the establishment of a national database or clearinghouse housed and maintained in the private sector to track and identify where organized retail theft type crimes are being committed in the United States."

The FBI has engaged in a number of specific actions in satisfaction of this requirement. Upon enactment of the legislation, the FBI formed a working group with the National Retail Federation and consulted with members of the retail community to ensure the specific needs of the retail community shaped the design of the national clearinghouse and the composition of the task force. The FBI working group identified two existing private databases, each vying to be the "national database" used by the industry and law enforcement. One database, the Retail Loss Prevention Intelligence Network, was launched in December 2005 by the National Retail Federation, which developed the database in conjunction with the FBI's Major Theft Unit. DOJ and the FBI's OGC, Budget Unit, and Major Theft Unit continue to conduct research to determine the eventual structure of the "national database", the composition of the task force, and the specific

requirements for accessing and utilizing funds appropriated for Fiscal Years (FY) 2006-2009.

**34. To facilitate CALEA implementation, Congress appropriated \$500 million to reimburse carriers for the direct costs of modifying systems installed or deployed on or before January 1, 1995. (CALEA is the Communications Assistance for Law Enforcement Act, which was passed in 1994 at the request of the FBI to enable law enforcement to conduct electronic surveillance on the new technologies and wireless services then in existence.) Approximately 90% of this money has been spent already; there is only \$45 million remaining. However, according to the IG, the FBI is determined to spend the remaining \$45 million, even though the IG feels that is no longer appropriate or effective. Does the FBI believe that this money should be spent? If so, why? Does the FBI feel that CALEA has been successful overall?**

**Response:**

Electronic surveillance forms the foundation for many of the FBI's criminal and terrorism-related investigations. In October 1994, Congress passed the Communications Assistance for Law Enforcement Act (CALEA) to protect national security and public safety by ensuring that changes in telecommunications technology would not compromise law enforcement's ability to conduct authorized electronic surveillance. Pursuant to CALEA the FBI balances three key goals: 1) preserving a narrowly focused ability to conduct authorized intercepts; 2) protecting privacy in light of increasingly powerful technologies; and 3) avoiding impediments to the development of new communications services and technologies.

In its March 2006 audit report regarding CALEA's implementation, DOJ's OIG recommends that the FBI re-examine *how* it plans to expend the remaining funds. While the report does not comment on either the appropriateness or effectiveness of spending the remaining funding, it does offer a list of factors the FBI should consider in determining how to spend the remaining funds. Understandably, the OIG's primary concern is that these expenditures fund efficient and effective technical solutions.

CALEA allows the reimbursement of industry costs for retrofitting existing equipment. Challenging and complex negotiations, coupled with a novel payment structure, resulted in the FBI's expenditure of approximately \$450 million to cover costs originally estimated by the industry to be well over \$4 billion. The FBI has managed the reimbursement process carefully, and will continue this careful stewardship of CALEA funds, expending the remaining resources to ensure the greatest possible benefit to law enforcement while honoring CALEA's reimbursement eligibility constraints.

For the first time, the most extensively deployed telecommunications services (traditional circuit-switched land line and wireless services) comply with technical standards that meet the electronic surveillance needs of law enforcement. The FBI worked with Federal, state, and local law enforcement to identify the capabilities required to intercept modern telephone services, and developed from that information standards that address the capabilities required by CALEA. The FBI continues this coordination and works with the relevant services to ensure these standards work with new and emerging communications services. For example, these standards have allowed law enforcement to address: the migration of criminal users to wireless telephones; the shift in the vast majority of Title III intercepts to wireless telephones; and the advent of new Voice over Internet Protocol and broadband access services. Additional technical standards, currently in various stages of development, will address voice services over cable, wireless data access services, and wireline Internet Protocol network access services. Both the existing and the developing standards have required extraordinary liaison and interaction among a diverse group of law enforcement agencies, other government agencies, telecommunications carriers, and telecommunications equipment manufacturers and are clear indications of CALEA's success.

#### **Questions Posed by Senator Grassley**

**35. This March, a New York grand jury accused former Special Agent Lin DeVecchio of giving secret information to his informant, which led to the murders of four individuals in the 80s and early 90s. Following similar scandals involving mafia informants in Boston and former FBI agents John Connolly and H. Paul Rico, new informant guidelines were developed to ensure that similar problems did not recur.**

**a. Have the current informant guidelines been re-evaluated in light of the allegations against DeVecchio? If so, what additional changes may be considered in light of the allegations against DeVecchio?**

#### **Response:**

Confidential informants and other confidential human sources are critical to the FBI's ability to carry out its counterterrorism, national security, and criminal law enforcement missions. A source may have a singular piece of information we could not otherwise obtain, enabling us to prevent a terrorist act or a crime or to apprehend a fugitive. It is important that the FBI have a vigorous and effective human source program that complies with legal and Departmental requirements.

Because of the importance of this program, several months ago the FBI's DI initiated a comprehensive review and revision of our HUMINT program in

conjunction with DOJ. As one part of the re-engineering project, the FBI is working with DOJ to draft revised AG Guidelines governing source operations and to develop new internal manuals. The Validation Standards Manual details the implementation of a comprehensive, Bureau-wide validation process that has been reviewed by DOJ and complies with the standards developed by the Director of National Intelligence (DNI). In addition to requiring the validation of every source and every relationship between an SA and a source on a regular and consistent basis, the revised validation process will be streamlined and automated through a new technology application. By automating the administrative aspects of human source operations, the FBI will improve compliance with AG Guidelines and reduce human error.

**b. If the allegations against DeVecchio are proven, please explain which provisions of the current informant guidelines that were not in effect at the time of his actions might have prevented his misconduct or brought it to light earlier.**

**Response:**

The existing AG Guidelines Regarding the Use of Confidential Informants provide for substantial oversight of the FBI's use of informants, including annual internal reviews of informant files and external reviews of long-term informants by DOJ's Confidential Informant Review Committee (CIRC). These AG Guidelines expressly prohibit law enforcement agents from interfering with criminal investigations involving confidential informants and provide specific guidance concerning prohibited transactions and relationships. As indicated in response to subpart a, above, the FBI is currently re-engineering its HUMINT program. This re-engineering effort and the implementation of forthcoming validation procedures will allow for a thorough and comprehensive review of the classifications of all sources being operated in the FBI. Part of the re-engineering effort includes a review of the current CIRC process, including the current procedure under which a source can have a designated classification that would not be reviewed by the CIRC.

**c. Please provide a detailed description of the nature and extent of previous internal investigations into DeVecchio's relationship with Gregory Scarpa Sr., including (1) the origin of the allegations, (2) the factual findings of the investigations, and (3) an explanation of the basis for any conclusion to impose or not impose discipline on DeVecchio for alleged misconduct.**

**Response:**

In 1995, the United States Attorney's Office for the Eastern District of New York alleged in an ex parte court filing that SA DeVecchio had unlawfully provided

confidential law enforcement information to an informant involved in organized crime in New York. These allegations were reviewed and investigated by DOJ's Public Integrity Section and the FBI's OPR. In September 1996, the Public Integrity Section determined that prosecution of SA DeVecchio was not warranted, and the OPR investigation was closed. SA DeVecchio retired from the FBI in October 1996. At that time, FBI policy did not provide for the continuation of internal investigations after a subject retired or resigned even if continuation would protect the FBI's institutional interests. The FBI's current policy of continuing internal investigations under those circumstances is based on recommendations resulting from the Bell Colwell review of the FBI's internal disciplinary system.

**36. According to the website maintained by DeVecchio's supporters in the FBI (www.lindevocchio.com), the agents helped post a one million dollar bond to secure his release and are raising money for his legal defense. After his arraignment agents surrounded DeVecchio "in a human blanket" as he left the courtroom so that he could not be questioned by reporters. One agent wrote, "it might even be said that a few reporters received a few body checks out on the sidewalk" and that he "was never prouder to be an FBI Agent."**

**a. Is it appropriate for current and former FBI agents to cite their affiliation with the Bureau to lend credibility to a private effort to raise money for a defendant charged with murder? Please explain why or why not.**

**b. What rules, if any, govern an agent's use of affiliation with the FBI for other than official purposes?**

**Response to subparts a and b:**

It would be inappropriate for current FBI employees to use their FBI affiliation to lend credibility to their private efforts to raise money for a criminal defendant. Internal FBI regulations generally prohibit employees, except in an official capacity, from becoming involved in any matter directly or indirectly concerning an employee or non-employee who has been arrested or is otherwise in difficulty with a law enforcement agency, from attempting to mitigate the action of any arresting officer, agency, or prosecuting officer, and from trying in any way to minimize publicity concerning such incidents. When expressing their personal views or discussing matters related to the functions of the FBI, FBI employees are cautioned to make clear that they are stating their personal opinions, not those of the FBI, especially when they have been identified as FBI employees.

In addition, current FBI employees are subject to the regulations governing federal employees generally. Pursuant to these regulations, "[e]mployees shall not use

public office for private gain." (5 C.F.R. § 2635.101(b)(7).) Employees are also prohibited from using their Government position, title, or authority to induce others to provide any benefit to the employee or to another person, or in a manner that could be construed as implying that the FBI or another Government entity sanctions or endorses the employee's personal activities or those of another. (5 C.F.R. § 2635.702.) Federal employees also may not use, or allow the use of, their official titles or positions to further their personal fund raising efforts. (5 C.F.R. § 2635.808(c)(2).)

In contrast, former FBI employees who are no longer in federal service are not subject to these restrictions. While a federal statute (18 U.S.C. § 709) prohibits the use of the FBI's name to convey the impression that the FBI endorses a publication or production, it does not, by its terms, prohibit former FBI employees from referring to their former FBI positions to "lend credibility" to their own beliefs about a former colleague in soliciting donations on his behalf.

**c. If an agent boasts about assaulting members of the press, does that constitute misconduct? What action, if any, has been taken to investigate the propriety of activities on the part of active agents who are supporting Mr. DeVecchio?**

**Response:**

If the individual who boasted about "assaulting members of the press" was a former FBI employee at the time of the alleged offense, he/she would not be subject to the FBI's internal disciplinary process. If, however, a current FBI SA boasted of assaulting a member of the press, such conduct would be covered by the FBI's disciplinary process and would constitute misconduct. If an assault actually occurred, the SA might be terminated and/or criminally prosecuted. Even if no assault took place, such boasting by a current FBI employee would negatively impact the FBI's image. Conduct that disgraces, dishonors, or discredits the FBI or compromises the standing of the FBI, whether committed on- or off-duty, constitutes "unprofessional conduct" and is sanctionable. The sanction imposed would depend on the specific facts of the case, including the impact such a statement had on the public's confidence in or perception of the FBI, the demoralizing impact the statement had on other FBI employees, and the employee's prior disciplinary record. Because the types of misconduct that constitute "unprofessional conduct" are quite varied, the FBI's OPR is given wide latitude in determining the appropriate sanction for this offense, ranging from an oral reprimand to dismissal.

The DOJ OIG has not notified the FBI that it has received any allegations of misconduct by current FBI personnel who support Mr. DeVecchio, and the FBI is otherwise unaware of any such allegations. We have, consequently, not initiated

an investigation. Should the FBI's IIS become aware of such an allegation, it would provide that information immediately to the OIG for review. If the OIG were to refer the matter back to the FBI, the IIS would evaluate the information carefully and investigate the matter further, if appropriate.

**37. During the recent sentencing hearings for convicted terrorist Zacharias Moussaoui, Harry Samit, the Minneapolis FBI agent who conducted the investigation of Moussaoui testified at length about the lack of support he received from FBI supervisors during his efforts to obtain a warrant to search Moussaoui's computer and apartment. He said that he "warned higher-ups and others in the government at least 70 times that Moussaoui was a terrorist." He described the failure of FBI supervisors as "criminal negligence, obstructionism, and careerism." This is amazing testimony from a sitting agent in one of the most important cases in FBI history.**

**a. What steps have you taken to ensure that Agent Samit will not face retaliation for his recent testimony?**

**Response:**

Director Mueller is committed to ensuring the protection of FBI employees who report organizational wrongdoing and has issued multiple communications reiterating his position that reprisals will not be tolerated, nor will attempts to prevent employees from making protected disclosures. Employees who engage in reprisals or intimidation against individuals who make protected disclosures can expect appropriate disciplinary sanctions, including dismissal from the rolls of the FBI, where warranted.

While Special Agent Samit's concerns have only recently been made public as a result of the Moussaoui sentencing hearing, they have received considerable review by numerous internal and external entities since 9/11/01, including the Joint Inquiry of the House and Senate Intelligence Committees, the 9/11 Commission, and the DOJ OIG. These reviews have resulted in findings and recommendations that have been incorporated into the FBI's ongoing transformation.

**b. The chapter on the Moussaoui case in the Inspector General's report on the FBI's handling of intelligence information before 9/11 was not released at the same time as the rest of the report because the criminal case against Moussaoui was still pending at the time. Now that Moussaoui has been sentenced, do you support the release of a declassified version of that chapter, so that the American public can understand better what happened?**



**c. What action, if any, is required by the FBI before the chapter can be released?**

**d. When do you expect that chapter to be released publicly?**

**Response to subparts b-d:**

The DOJ OIG issued its completed report in November 2004. The full report, classified at the Top Secret/Sensitive Compartmented Information (SCI) level, was provided to the FBI, DOJ, Central Intelligence Agency (CIA), National Security Agency (NSA), 9/11 Commission, and Congress. At the request of members of Congress, the OIG created an unclassified version of the report. In June 2005, consistent with the rules of the United States District Court for the Eastern District of Virginia, the Court gave the OIG permission to release the sections of the unclassified report that did not discuss the FBI's investigation of Zacarias Moussaoui. The Moussaoui case concluded on 5/4/06, and on 6/19/06 the OIG released the full version of the unclassified report, which includes the Moussaoui chapter (chapter 4) and other references to Moussaoui throughout the report.

**38. Agent Harry Samit's testimony provides at least some reason to believe that the horrific events of 9/11 might have been averted if FBI supervisors had listened to and supported their field agents. It also raises the question of whether too many supervisors operate by the principle that some agents describe as, "Big cases equal big problems. Little cases equal little problems. No cases equal no problems."**

**a. How do you identify which supervisors regularly fail to support the investigative efforts of their field agents?**

**Response:**

FBI supervisors are subject to annual Performance Appraisals and semi-annual Progress Reviews provided by their Rating and Reviewing Officials. In addition, every three years, the FBI's Inspection Division conducts comprehensive inspections of every field office, Legal Attaché, and FBI Headquarters (FBIHQ) entity. These inspections emphasize management performance at all levels. Prior to the inspection, each employee is requested to complete an automated leadership survey regarding the two levels of management above them. The survey includes questions regarding the supervisors' competence, ethics, and support of investigations. The survey is anonymous. Every SA and 50% of all support employees are personally interviewed by the inspection staff and asked about management's support of their efforts. Investigative and source files are

reviewed, outside agency contacts are interviewed, statistical accomplishments are assessed, and a determination is made regarding each supervisor's performance.

**b. What should a field agent do when a supervisor consistently fails to reward initiative or approve investigative proposals? Is there any way to report the problem without fear of retaliation?**

**Response:**

Within a field office, an employee is free to speak to the ASAC or SAC if unable to resolve an issue with a direct supervisor. Consistent supervisory declination of investigative proposals would produce a trail of documentation, and a field SA could share this documentation with executive managers, who are encouraged to maintain "open door" policies.

The FBI's inspection process addresses supervisory effectiveness in a number of ways. A preliminary assessment of whether initiative is rewarded can be obtained through a specific inspection interrogatory that requires supervisors to list all employee awards. In addition, the pre-inspection leadership survey and employee interviews are designed to determine whether initiative and tangible results are being rewarded, whether managers' open door policies are being honored, and whether managers are otherwise effective. The file reviews conducted during field office inspections help to identify supervisors who consistently disapprove operational proposals or mismanage investigations, and field SAs have the opportunity to speak privately with inspectors during inspections.

Although the FBI can never completely eliminate an employee's fear of retaliation, factors likely to induce such fear can be reduced or eliminated. The anonymous nature of the inspection leadership survey, private interviews with the inspection staff, and executive managers who promote the proper environment all help to reduce the fear of retaliation. If an employee nonetheless believes retaliation has occurred, this may be reported to the Inspection Division's IIS or to DOJ's OIG or OPR. FBI employees are also frequently reminded through FBI-wide emails and other mechanisms that there is a procedure established under law (5 U.S.C. § 2303) and implemented by regulation (28 C.F.R. Part 27) that provides a formal avenue for an employee to seek corrective action based on a personnel action taken in reprisal for whistle blowing.

**c. How does FBI headquarters measure the productivity and performance of particular field offices? To what extent does the Bureau track metrics such as frequency of electronic surveillance, number of search warrants executed, and numbers of active confidential informants as well as numbers of arrests, indictments, and convictions?**

**Response:**

Field office performance and productivity is continuously tracked and evaluated. The recently implemented COMPASS database placed a wide variety of performance metrics on the computer desktop of every field Executive Manager and many FBIHQ Executive Managers. COMPASS enables production of reports on statistical accomplishments, resource utilization by program, confidential informant and asset data, and many other performance metrics. Regular reports are generated that enable managers to track progress in specific areas over selected time frames, compare offices of similar size, monitor resource utilization by squad, program and office, and measure source development against specific targets. Each of the operational divisions at FBIHQ maintains data specific to field office performance in particular programs. During on-site inspections the Inspection Division compiles and analyzes all available metrics including the utilization of sophisticated investigative techniques, seizures and forfeitures, indictments and convictions, national security accomplishments, and others. This data helps form the basis of an inspection determination as to the effectiveness and efficiency of an office's investigative programs and the performance of its managers.

**39. Please identify and describe any and all agent surveys or questionnaires conducted by the FBI, outside consultants, or independent entities within the last 15 years.**

**Response:**

The FBI does not track the circulation of surveys or questionnaires to its employees. If the Committee is interested in a particular survey or questionnaire, we will make every effort to locate it.

**40. The Inspector General recently completed his report on allegations by former ICE/SAC Houston, Joseph Webber that the FBI inappropriately delayed a wiretap request on a criminal suspect in a terrorist financing case. The report has been classified secret. Mr. Webber, who reviewed a draft of the report, has told my office that passages critical of certain FBI officials were originally marked "unclassified," but had later been changed to "secret" even though they contain no information that would reveal sources or methods of gathering intelligence.**

**a. The Inspector General provided a copy of the draft report to FBI headquarters for classification and sensitivity review prior to seeking FBI comment on the substance of the report. Please describe the process that the FBI followed in this case to make classification decisions about the IG report and identify any instance where the procedure differed from that followed in the review of other IG reports.**

**Response:**

The classification and sensitivity review process for this draft report was consistent with the process for other draft reports. The FBI received the original draft from the OIG as a classified document. Upon receipt, the draft report was electronically scanned. This electronic copy was distributed to RMD's Classification Unit to perform the classification review. Additionally, the technical/subject matter experts in CTD, OGC, and other relevant parties were tasked to review the draft for factual accuracy and sensitivity issues. All parties concurrently reviewed the report and provided comments and corrections, if any, to the External Audit Management Unit, Audit, Evaluation and Analysis Section, Inspection Division. The Classification Unit compiled and reviewed the sensitivity comments and content concerns for comparison to the classification issues identified in its initial review of the draft document. CTD was consulted on items where clarification was needed to complete the classification review. The final sensitivity and classification review comments, as well as technical/factual accuracy concerns, were forwarded to OGC, and the Special Counsel to the Director for final review prior to release to the OIG. The Assistant Director of the Inspection Division reviewed and signed the formal response. Inspection Division personnel transmitted the response to the OIG.

**b. Are such reports reviewed solely by a classification unit in headquarters or is it disseminated to the subjects mentioned in the report? Please describe who typically participates in the classification decision, and identify who is ultimately responsible for the final classification decision.**

**Response:**

The report was distributed to RMD's Classification Unit, the technical/subject matter experts in CTD, OGC, and other relevant parties. Final, official classification authority rests with the Classification Unit, and sensitivity concerns, as well as factual accuracy and technical issues, are the responsibility of the technical/subject matter experts in the affected division -- in this case, CTD. The Classification Unit may make recommendations or express concerns to the affected division concerning law enforcement sensitive content, references to or including information from other agencies, etc., but the Classification Unit primarily reviews OIG drafts and proposed FBI responses for classification pursuant to Executive Order 12958, as amended, and in accordance with FBI and DOJ policies.

**c. Do you believe that it would present an inappropriate conflict of interest to give FBI officials who are the subject of criticisms in an IG report the ability to censor the public version of that report? Please explain why or why not.**

**Response:**

Neither with regard to this report nor any other OIG product did the FBI "censor the public version of the report." We agree that information should not be marked SECRET to protect individuals or the FBI from criticism or embarrassment. Classification reviews are conducted to ensure compliance with Executive Order 12958, as amended, and FBI and DOJ policies. These reviews are professional and objective.

**d. Were any FBI officials mentioned in this report allowed to make decisions, directly or indirectly, about which portions would be classified?**

**Response:**

Although parties named in the report were allowed to review the draft and provide comments on sensitivity and technical/factual accuracy, official classification decisions were made by the Classification Unit.

**e. Please list all of the FBI officials who reviewed the report for classification purposes and when each review occurred.**

**Response:**

Pursuant to the release of the draft by the OIG on January 27, 2006, the Classification Unit performed the official classification review in February 2006 (reported on 02/07/06). The Acting Unit Chief and her supervisor oversaw the classification review and approved the classification.

**41. Earlier this year, the Inspector General completed his report into the allegations for former FBI Special Agent Michael German. The Inspector General found that after he wrote an internal whistleblower letter about the mismanagement of an undercover operation in Tampa, he was retaliated against. FBI Undercover Unit Chief Jorge Martinez vowed that German would never work another undercover case and blocked German from continuing to teach other agents at FBI training sessions. The IG also found that some unknown FBI official altered official records with correction fluid in order to undercut German's claims.**

**a. What steps has the FBI taken to identify the individual who altered official records with correction fluid?**

**Response:**

The DOJ OIG referred its findings to the FBI's OPR, where they are being adjudicated. We do not anticipate undertaking additional investigative steps in response to the OIG's referral.

**b. What are the maximum consequences that Unit Chief Martinez may face for retaliating against German?**

**Response:**

Under the FBI's adjudicative guidelines, the maximum penalty for an employee who is found to have retaliated against a whistleblower is dismissal.

**c. Please list all FBI personnel who have been disciplined for whistleblower retaliation and provide a brief description of each case, including a description of the punishment imposed.**

**Response:**

Since the promulgation of regulations governing whistleblower protection for FBI employees in November 1999, one employee has been disciplined for whistleblower retaliation. That employee, an ASAC, was found to have retaliated against an SA based on the SA's protected disclosure. Investigation of this matter was initiated by DOJ's OPR in June 2003 and it was adjudicated by the FBI's OPR in February 2005 under the disciplinary system in place before implementation of the Bell Colwell recommendations based on the precedent relied upon at that time. The ASAC exercised his right to appeal, and the FBI's Appellate Unit vacated the 3-day suspension. The FBI's OGC has since opined that the Appellate Unit's analysis of DOJ's whistleblower regulation was flawed, but there is no vehicle for reversing an appellate determination under these circumstances. Under the present penalty table, the violation would have resulted in a penalty ranging from a 10-day suspension to dismissal.

**d. When do you expect a final decision to be made about punishment for Martinez and will you please notify the Committee about what action is taken when that occurs?**

**Response:**

The FBI's OPR is currently adjudicating the matters referred to it by DOJ's OIG. The FBI does not routinely provide information concerning the outcome of

individual personnel matters. We are willing to discuss other methods of accommodating the Committee's legitimate oversight requests.

**e. On February 3, 2006, I joined with Senator Specter and Senator Leahy in sending a letter requesting copies of documents relating to the Michael German matter. We are still waiting for a complete response from the FBI. Why has the request been delayed so long and when will we receive copies of the documents we requested?**

**Response:**

The Committee's 2/3/06 letter requesting documents concerning the Michael German matter was addressed to the DOJ OIG, which referred the request for FBI documents to the FBI. On 4/28/06, the FBI made an initial release of material to the Committee and advised that we would supplement that production when our review of the remaining material was complete. The FBI completed its response by letter to the Committee dated 7/27/06.

**42. During the investigation of the death of Assistant U.S. Attorney Jonathon Luna, agents in the Baltimore FBI office aggressively questioned one of its own female field agents who knew Luna. The agent later complained about the nature of the questioning and claimed that her laptop computer was searched without her consent. During an internal investigation of the complaint, FBI agents reportedly gave contradictory statements about the interrogation and unauthorized search. However, the FBI closed the matter as merely a "performance issue." The IG reviewed that decision and determined that it should have been treated as a misconduct issue and that the allegations against Smith-Love should have been referred to the Office of Professional Responsibility (OPR).**

**a. There has apparently been no criminal investigation to determine whether any FBI agents gave false statements during their interviews by the Internal Investigations Section. Why not? Isn't it crucial that the FBI get to the bottom of issues that call into question the truthfulness of its agents?**

**Response:**

The FBI remains committed to fairly and impartially investigating allegations that call into question the candor and truthfulness of all FBI employees; however, we do not believe that differences in witness statements necessarily raise issues of candor or truthfulness.

The DOJ OIG review of the FBI's complaint investigation resulted in a recommendation that the underlying investigation be forwarded to the FBI's OPR for adjudication. The FBI adopted this recommendation, and the results of the original investigation as well as the OIG report of investigation were forwarded to

OPR for adjudication. The OIG found the facts of the matter sufficiently established for adjudication and did not recommend that additional investigation of the underlying matter be conducted. Following issuance of the OIG report, the original complainant, as well as one of the subjects of the underlying internal inquiry, made a number of allegations, including that the other had made false statements in the underlying inquiry. Inasmuch as at least one of the employees claimed "whistle blower" status, consistent with FBI policy, their letters were referred by the FBI to the DOJ OPR and DOJ OIG for handling. The DOJ OPR deferred to the DOJ OIG for consideration of the matter. The OIG responded to the FBI advising that the core allegations raised in the employees' letters involved issues that had already been investigated by IIS and/or the OIG and were ready for review and adjudication by OPR. Accordingly, no further investigation of the underlying matter was conducted.

**b. After the IG intervened to ensure that OPR reviewed the matter as a potential misconduct issue, OPR reportedly determined that there was no misconduct. Please provide a detailed explanation of the basis for OPR's conclusion that no misconduct occurred in this case.**

**Response:**

OPR substantiates allegations of misconduct based on a preponderance of the evidence. To reach a finding of misconduct, OPR must determine that a policy, law, or regulation has been violated. In this instance, OPR reviewed witness statements and other evidence contained in the investigative files and determined that the preponderance of the evidence did not support a finding of misconduct, including false statements or lack of candor.

**c. What is Jennifer Smith-Love's current position with the FBI? When was she promoted to that position?**

**Response:**

Ms. Love's current position with the FBI is Section Chief in CTD. She was promoted into that position, which is within the SES program, effective 01/03/05.

**d. Please describe FBI policy with regard to promotions of employees with pending misconduct allegations?**

**Response:**

The general policy regarding promotion of an FBI employee into or within any mid-management or SES position requires an administrative review of records by



the FBI's Office of Equal Employment Opportunity Affairs, Security Division, Inspection Division, and OPR, and by the DOJ OIG. In addition, for SES positions, record checks are conducted by DOJ's OPR and Criminal Division. These checks span the employee's entire FBI career for SES candidates and the previous 3 years for non-SES positions. Prior to any selection, the results of these record checks are considered by the relevant career board and the Director. The Director retains the authority to make final selections.

**e. Did Smith-Love receive a promotion before the complaint against her was properly resolved? Please explain.**

**Response:**

As is typically done before promotion to the SES, an administrative records check was conducted before Ms. Love was promoted to the position of CTD Section Chief. That check revealed that DOJ OIG and FBI OPR inquiries were then pending related to the Luna investigation. Director Mueller was made aware of this and approved Ms. Love's promotion, which was effective 1/3/05. Several months thereafter, it was alleged that Ms. Love had made inconsistent statements in the context of the administrative reviews of the Luna investigation. Ultimately, the FBI's OPR determined that the preponderance of the evidence did not support a finding of any misconduct, including false statements or lack of candor.

**43. Cecilia Woods retired from the FBI last year after being subjected to a succession of disciplinary suspensions and unwanted transfers. These followed her reporting gross misconduct by her supervisor, including that he had engaged in a sexual relationship with a paid FBI informant. After reporting these egregious acts of misconduct by her supervisor, Agent Woods alleges that she was treated as if she were the problem instead of him. Her supervisor is still employed with the FBI even though, according to Woods, he admitted to the misconduct after initially denying it to Bureau investigators.**

**a. According to the FBI's disciplinary guidelines, the standard penalty for an "improper personal relationship" with an informant is a seven day suspension, although it can range from a mere censure to dismissal, depending on the circumstances. Why is it appropriate for such a serious violation to have such a broad range of potential penalties?**

**Response:**

Improper personal relationships take many forms, ranging from non-romantic, social relationships to romantic and intimate sexual relationships. Moreover, merely creating the impression that an improper relationship exists can subject an employee to discipline. Because violations vary greatly in substance and consequence, there is a need for a broad range of potential penalties. For

example, if an SA were to regularly play golf with an informant but the conduct had no effect on the prosecution of a case, such behavior would be far less serious than an SA's involvement in a romantic relationship with an informant in which the informant's credibility was destroyed and the underpinnings of the criminal case irreparably compromised. A broad range of disciplinary options must be available to accommodate the many-faceted forms of this disciplinary infraction.

**b. Please explain why the FBI should not have a zero-tolerance policy with regard to agents engaging in sexual activity with informants. Would you consider implementing such a policy?**

**Response:**

The FBI does not tolerate SAs engaging in sexual activity with informants. The FBI's disciplinary code prohibits SAs from engaging in social, romantic, or intimate relationships with sources. It further provides that an employee will be disciplined for: (1) engaging in an improper personal relationship, or, (2) without authorization, engaging in conduct that would cause the reasonably prudent person to believe that there is an improper relationship. The sanctions available for engaging in sexual activity with informants include substantial periods of suspension and termination.

**c. Please provide a detailed description of the investigations, conclusions, and actions taken against Cecilia Woods' former supervisor.**

**Response:**

In 2000, the FBI opened an administrative inquiry pertaining to Ms. Woods' former supervisor. That administrative review substantiated allegations that the former supervisor had engaged in misconduct and he received a 14-day suspension. Before OPR concluded its adjudication of the matter, the supervisor was removed from his GS-15 position and reassigned to a GS-13 position. OPR's final adjudication letter refers to his reassignment.

**d. Have any of those conclusions been re-examined in light of her former supervisor's deposition testimony in her EEOC case, in which Woods alleges he admitted to sexual activity with an individual who was a paid informant and a foreign national?**

**Response:**

The FBI is a party in a pending administrative proceeding relating to the allegations raised by Ms. Woods. Given the pending status of this proceeding, it

would be inappropriate to comment on information developed through this confidential process.

**44. The FBI recently announced the retirement of Gary Bald, head of the FBI's National Security Service. Mr. Bald had only been in this position for only eight months. The FBI's previous Director of Intelligence held that position for less than two years. The 9/11 Commission identified high turnover in key management positions as a major problem with our counterterrorism efforts.**

**a. Did you know when you chose Gary Bald for the position last summer that he would be retiring so soon?**

**Response:**

Director Mueller became aware of Mr. Bald's decision to retire just prior to the public announcement on April 27, 2006.

**b. Did you or anyone else involved in the decision to appoint Gary Bald as head of the National Security Service have any communications with him about his retirement plans prior to his appointment? If so, please describe the communications in detail.**

**Response:**

Director Mueller's appointment of Gary Bald as EAD of the NSB was subject to the concurrence of the DNI and the AG. We do not believe it would be appropriate to disclose internal personnel discussions that may have occurred regarding this appointment.

**c. On what date was Gary Bald first eligible to retire with full benefits?**

**Response:**

Mr. Bald was eligible to retire with full benefits on 02/24/04.

**d. On what date would he have been subject to mandatory retirement?**

**Response:**

Mr. Bald would be subject to mandatory retirement on 02/28/11.

**e. How will you ensure that the next candidate for this critical position stays long enough to provide some consistent, long-term leadership?**

**Response:**

The FBI is presently developing succession planning initiatives targeting the SES ranks. Initiatives include inventorying the SES population's knowledge, skills, and abilities (KSAs), as well as identifying the job requirements for each SES position. This will allow the FBI to identify gaps in the SES population's KSAs to fill particular positions. With the gaps identified, the FBI can pro-actively develop a pool of qualified candidates to fill particular SES positions through training and developmental assignments. By identifying larger pools of qualified candidates, Executive Management will have greater choice from which to make selections. The FBI recruits qualified candidates for senior executive positions from all appropriate sources consistent with merit system principles.

**45. In your testimony, you described the Investigative Data Warehouse (IDW), an FBI technology initiative with over 560 million FBI and other agency documents from previously stove-piped systems, accessible to almost 12,000 users.**

**a. How many data sources are consolidated for unified searching through IDW and how many agencies contribute data to the IDW? Please list all of the data sources and the agencies providing them.**

**b. Please describe the extent to which the IDW currently allows searching data contained in the information systems maintained by the Drug Enforcement Administration.**

**c. Please describe the extent to which the IDW currently allows searching data contained in the information systems maintained by the U.S. Secret Service.**

**d. Please describe the extent to which the IDW currently allows searching data contained in the information systems maintained by the U.S. State Department (other than information on lost or stolen passports).**

**e. Please describe the extent to which the IDW currently allows searching data contained in the information systems maintained by the Bureau of Alcohol, Tobacco and Firearms.**

**f. Which law enforcement organizations contribute data from their information systems to IDW other than the FBI, Immigration and Customs Enforcement, and the Financial Crimes Enforcement Network?**

**g. What steps are you taking to encourage other law enforcement entities to contribute data from their systems?**

- h. What percentage of FBI agents currently has access to IDW?**
- i. What percentage of FBI analysts has access to IDW?**
- j. What percentage of agents and what percentage of analysts with access to IDW would constitute full deployment?**
- k. When do you expect to reach full deployment?**
- l. How much would full deployment cost and how much of the total cost is covered by existing budget requests?**
- m. How many non-FBI law enforcement agents have access to IDW? How many of those serve on Joint Terrorism Task Forces (JTTFs)? How many do not? Please explain whether and to what extent non-FBI law enforcement agents will be granted access to IDW, including the ability to search ACS (or future FBI case-management systems) both inside and outside the JTTF-context.**
- n. What level of access by non-FBI law enforcement agents would constitute full deployment of IDW?**

**Responses to subparts a-n:**

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

**46. In February, 2006, the Government Accountability Office (GAO) released a report of a study of the FBI's management of the Trilogy Project, finding over \$10 million in questionable or undocumented costs. The GAO report singled out two Trilogy contractors, Computer Sciences Corporation and CACI International, Inc., for inflated spending and inadequate documentation. On March 18, 2006, the *Washington Post* published an article reporting that those same two contractors will be working on Project Sentinel as subcontractors for the general contractor, Lockheed Martin Corporation.**

**a. What assurances can you provide to taxpayers that any money that these contractors may owe to the government due to problems identified by GAO will be repaid before more taxpayer funds are disbursed to them under the Sentinel project?**

**Response:**

Two vendors are common to both Trilogy and Sentinel - Computer Science Corporation (CSC) and CACI. The division of CSC that worked on Trilogy (and actually a separate firm at the time of its Trilogy work, acquired by CSC

thereafter) will not be working on Sentinel, so we anticipate little or no overlap of services or personnel. We have contracted with CACI to provide training for Sentinel, which was also the purpose of the Trilogy contract.

The FBI has strengthened its internal controls to avoid a repeat of the issues cited by the auditors with respect to all vendors. Among other things, we have improved our contract oversight in two major ways. First, the Sentinel contract has clear reporting requirements and severable deliverables. In other words, we can stop work if we are not satisfied with a contractor's progress. Second, we have structured our contract management with clearly defined roles and responsibilities, so accountable personnel are reviewing all documentation and expenses. That process will be supplemented by internal audits of our financial management, as well as by oversight from Congress and the Administration.

GSA/FEDSIM is finalizing negotiations with the GSA Deputy Assistant Inspector General (IG) for Auditing, FBI, and DCAA to have DCAA conduct an overall program audit of both task orders. The scope of the program audit will include the costs identified by GAO as potentially questionable. Upon completion of the program audit, DCAA will conduct the final closeout audit of both task orders. GSA/FEDSIM and the FBI will pursue reimbursement of any improper charges identified by that audit.

**b. The GAO recommended that the FBI employ an independent third party to conduct a more complete audit of the Trilogy project. Will the FBI be implementing that recommendation? If not, why not. If so, please explain.**

**Response:**

As noted in response to Question 11, above, it was always the intent of both the FBI and the General Services Administration's (GSA) Federal Systems Integration and Management (FEDSIM) Center to have the Defense Contract Audit Agency (DCAA) conduct final close-out audits to assess final costs, including direct and indirect labor costs. This is the appropriate means of identifying and addressing any potential overpayments to contractors. Close-out audits are designed to disclose and resolve questionable costs of the type GAO reported, as well as costs deemed unallowable under the contract. The initiation of the close-out audits has been delayed until final rates for both the prime contractors and all subcontractors have been approved by DCAA and final reconciliation is completed by both prime contractors. At that time both prime contractors will be able to submit their final invoices and DCAA will be able to complete the final closeout audit. While the prime contractors are reconciling their subcontractor costs and waiting for DCAA approval of their final rates, GSA/FEDSIM is finalizing negotiations with the GSA Deputy Assistant Inspector General (IG) for Auditing, FBI, and DCAA to

have DCAA conduct an overall program audit of both task orders. The scope of the program audit will include the costs identified by GAO as potentially questionable. Upon completion of the program audit, DCAA will conduct the final closeout audit of both task orders. GSA and the FBI will monitor the progress of the close-out audits and will ensure all areas of concern cited in the Report, including the direct labor rates charged by the contractors and their subcontractors, are thoroughly reviewed and resolved.

**47. According to documents obtained by FBI agent Bassem Youssef in the course of his civil suit against the FBI, several senior FBI personnel had approved a directed transfer of Youssef to the International Terrorist Operations Section (ITOS), as late as two days before he met with you and his congressman to express concerns about the under-utilization of his native Arabic language skills and counterterrorism expertise. After that meeting, the transfer was never completed, and there has been no explanation of why not. This sequence of events presents an appearance of whistleblower retaliation. Senior FBI officials openly complained about the meeting in deposition testimony, suggesting they thought Youssef's protected disclosures to you were inappropriate. What steps are you taking to ensure that this matter receives a thorough and independent review? How can the public have confidence that no retaliation occurred in this instance?**

**Response:**

We believe the meeting to which the question refers occurred in June 2002. At that time, the FBI was undergoing reorganization and the CTD was being restructured based on needs revealed by the 9/11/01 attacks. Among other things, a Document Exploitation project had been initiated in support of CTD's International Terrorist Operations Section (ITOS), but the project had not yet been assigned formally to CTD because the reorganization had not yet been authorized by Congress.

As indicated in public documents related to the case of Bassem Youssef v. Alberto Gonzales, et al., SSA Youssef's transfer from CD to CTD, planned before the referenced meeting, was not rescinded after that meeting. In March 2002, SSA Youssef was assigned to CD but was detailed to CTD as the manager of the Document Exploitation project, which was designed to exploit and extract information of investigative and intelligence value from foreign electronic and written media following the 9/11/01 attacks. The Document Exploitation project's main purpose was to analyze media for potential leads in the 9/11 investigation in order to prevent future terrorist attacks and to funnel relevant information to CTD's ITOS. SSA Youssef's Arabic language ability was a significant factor in his assignment to this project.

Rather than continuing his detail to CTD, the FBI planned to transfer SSA Youssef permanently to the position of CTD project manager but, in April 2002, the Document Exploitation project was in bureaucratic limbo because of CTD's ongoing reorganization. Because Document Exploitation directly supported ITOS, SSA Youssef's transfer from CD to ITOS, CTD, was the only logical designation available for the transfer to CTD at that time. The intent was that SSA Youssef would continue to perform the duties he had been performing since his assignment to the Document Exploitation project, but he would be officially assigned to CTD.

There was no action to rescind SSA Youssef's transfer or to otherwise retaliate against him after the meeting with Congressman Wolf. Because there was a legitimate business reason for the personnel action taken with respect to SSA Youssef, which was the same action contemplated before and implemented after the meeting, there is no basis for additional review.

**48. According to a May 1, 2006, *Washington Post* article:**

**Many researchers and defense attorneys say [polygraph] technology is prone to a high number of false results that have stalled or derailed hundreds of careers and have prevented many qualified applicants from joining the fight against terrorism. At the FBI, for example, about 25 percent of applicants fail a polygraph exam each year, according to the bureau's security director."**

**The article also cites "a comprehensive 2002 review by a federal panel of distinguished scientists" which found that "if polygraphs were administered to a group of 10,000 people that included 10 spies, nearly 1,600 innocent people would fail the test[.]"**

**a. Has the FBI conducted, commissioned, or reviewed scientific studies of the accuracy and effectiveness of polygraph examinations? If so, please describe them in detail. If not, why not?**

**Response:**

For clarification, the FBI's Assistant Director for Security's comments to the reporter indicated that about 25% of applicants are disqualified as a result of the polygraph test. These results usually include admissions of information or activities that lead to a disqualification decision.

The FBI does not independently conduct or specifically commission polygraph research but it works with other federal agencies to improve polygraph techniques



and has participated in research studies with the DoD Polygraph Institute (DoDPI) which is charged with conducting research for the federal polygraph community. All DoDPI research is available directly from DoDPI.

**b. What is the FBI's estimated rate of false results on polygraphs used for employment screening?**

**Response:**

Because scientists are unable to conduct field studies under ideal (laboratory) conditions, and the absolute truth is not always available to validate the results of polygraph examinations in actual cases, known error rates remain elusive. Although error rates can be estimated, the estimates depend upon the testing situation, the issues being tested, and the persons being tested. Empirical studies cannot be used to generalize rates of error because different polygraph examiners and examination situations will produce different error rates. A major reason why scientific debate over polygraph validity yields conflicting conclusions is that the validity of such a complex procedure is very difficult to assess and may vary widely from one application to another. The accuracy obtained in one situation or research study may not generalize to different situations or to different types of persons being tested. Scientifically accepted research on polygraph testing is hard to design and conduct as evidenced by the depth of studies conducted by academic laboratories. The FBI would welcome and encourage broader research in this area.

We would offer a noteworthy data point concerning FBI internal testing of employees. Since the inception of the PSP Program in 2001, approximately 7500 counterintelligence-focused examinations have been conducted with a Deception Indicated rate of less than 1%. This result is significantly lower than the *Washington Post's* predicted 16% failure rate.

**c. Given the high rate of false results, should a "failed" polygraph alone be the basis for a negative employment decision or personnel action? How many times per year is a polygraph result the primary reason for a negative employment decision or personnel action?**

**Response:**

We do not believe that FBI is experiencing a high rate of false positive results. Throughout the Federal polygraph community, the polygraph is considered to be an effective and acceptable screening tool and is a strong contributor in conjunction with the entire applicant process which examines the prospective employee from several standpoints. These include field investigations, records

checks and polygraph examinations. As noted earlier, polygraph results, including statements and admissions, account for about 25% of applicant disapprovals. With regard to on-board employees, a “failed” polygraph is never used as the sole basis for an adverse personnel decision. Anomalies are addressed through additional interviews and investigative work. The polygraph program does not make determinations on negative employment issues or personnel actions.

**d. What steps has the FBI taken to identify more reliable alternatives to polygraph tests for ensuring the trustworthiness of current and prospective employees?**

**Response:**

The FBI supports DoDPI research through a cooperative agreement and currently has two SAs assigned to DODPI. Later this year, DoDPI will host a summit sponsored by the interagency Technical Support Working Group and DoD's Counterintelligence Field Activity. The purpose of assembling these experts is to develop a research plan for the next 5-10 years for means to assist in determining truth of statement.

**49. In response to a previous question for the record regarding the New York Police Department (NYPD), you indicated that during a meeting to explore cooperation with the NYPD's translation and analysis program, the NYPD indicated that it did not want its officers and translation staff to undergo FBI polygraph testing as a condition of being granted access to “FBI information.” The response further stated, “we understand that the CIA and Pentagon have found a means of ensuring trustworthiness without the use of polygraph examinations.”**

**a. Please describe the alternative method of ensuring trustworthiness to which that response refers.**

**b. The previous response also stated, “We will work with both organizations to learn more about this process and will evaluate our ability to do the same.” Please explain what progress has been made toward implementing this polygraph alternative.**

**Response to subparts a and b:**

We have established a program where NYPD translators work on unclassified IC materials through the National Virtual Translation Center (NVTC). The FBI is also providing the NYPD with romanization training, teaching the IC's standard for transliterating foreign scripts into the Roman alphabet. Although we contacted our sister agencies to discuss their internal policies in this regard, we were pleased

to find the NVTC to be a suitable vehicle through which we could fully use the NYPD's available translator resources.

### **Questions Posed by Senator Kyl**

**50. I know that, for good reasons, you are not able to discuss operational details of the NSA's terrorist surveillance program. However, I was hoping that you could tell Committee whether, from your perspective, this program has made a significant contribution to your ability to prevent terrorist attacks against the United States homeland. Do you believe that the defunding or suspension of this program would make America more vulnerable to catastrophic terrorism?**

#### **Response:**

The Terrorist Surveillance Program (TSP) has been valuable to the FBI in a number of terrorism investigations. We have received information from the TSP that has assisted the FBI in discovering individuals who are terrorists or are associated with terrorists. To the extent that suspension of this program could deprive our agents of this sort of information in the future, it would be cause for concern.

**51. Alternative bills before the committee would require that the NSA surveillance program be briefed, in one proposal, to the Intelligence Committee alone and, in other proposal, to both the Intelligence and the Judiciary Committee. From your perspective as someone who is fighting terrorism on a daily basis, would it be desirable to keep both the full Intelligence and Judiciary Committees read into the program, or would it be better to restrict that access to the Intelligence Committee, which is accustomed to handling highly classified information on a routine basis?**

#### **Response:**

Under Executive Order 12958, access to Special Access Programs (SAPs) is determined by the agency that creates the SAP. The FBI did not create the SAP referenced in the question and we would, therefore, defer to the NSA for response.

### **Questions Posed by Senator DeWine**

**52. Although there has been an increase in the overall number of agents at the FBI since 9/11, most, if not all, of those agents have gone directly to the Counterterrorism, Counterintelligence and Computer Intrusion Programs. In addition, between 9/11 and**

**FY06, there has been a reduction of 661 agents assigned to all Criminal Programs with another 300 slated to be eliminated by the President's Budget in FY07. This amounts to a reduction of between 10 and 15% of agents focusing on criminal matters. This has no doubt limited the number of criminal cases the Bureau has been able to investigate - - has it decreased effectiveness of the Bureau in fighting crime? How much of a priority is law enforcement? How have you compensated for the decrease in criminal agents?**

**Response:**

The Funded Staffing Level for FBI criminal case agents has decreased by 994 agents, or 18%, since the attacks of 9/11. Despite the loss of those agent positions, protecting the nation's citizens from traditional criminal offenses has always remained a core function of the FBI, and 48% of all FBI agents remain allocated to these criminal matters.

To compensate for the decrease in criminal agents, the FBI has made difficult choices in determining how to most effectively use the available agents. In 2002, the FBI established as its criminal program priorities: public corruption, civil rights, transnational and national criminal enterprises (which include violent gangs and the MS-13 initiative), white collar crimes (which include corporate fraud and health care fraud), and violent crimes (which include crimes against children).

Since public corruption was designated as the top criminal priority, over 260 additional agents were shifted from other criminal duties to address corruption cases. The FBI is singularly situated to conduct these difficult investigations, and our effectiveness is demonstrated by the conviction of more than 1,000 corrupt government employees in the past two years.

The FBI has also maintained a steady commitment to addressing civil rights matters, and the number of these cases has remained fairly constant even as the complexity of the cases has increased. For example, the number of complex human trafficking cases has increased by almost 200% from 2001 to 2005, and the resolution of these cases has generally required both more time and more agents than the average non-human trafficking case.

The FBI has addressed violent street gang matters through its Violent Gang Safe Streets Task Force (VGSSTF) program, which leverages Federal, state, and local law enforcement resources to investigate violent gangs in urban and suburban communities. There are currently 128 VGSSTFs in 54 FBI field offices, composed of 561 FBI SAs, 76 other Federal agents, and 924 state/local law enforcement officers. The number of FBI SAs addressing gangs has increased,

with a decrease in the number of SAs addressing bank robberies, although the FBI still addresses violent and serial bank robberies.

Although the FBI has had to reduce the number of SAs working Governmental fraud matters since 9/11/01, FBI agents still respond to serious crime problems, as exemplified by the FBI's current initiatives to address hurricane-related fraud and Iraq contract fraud. The FBI does not currently open Governmental fraud cases unless the loss exceeds \$1 million.

The FBI also prioritizes investigations within its White Collar Crime Program, emphasizing corporate/securities fraud and health care fraud. The corporate fraud cases, in particular, are very labor intensive, but they are a priority for the FBI because so many represent the private industry equivalent of public corruption, where the dishonest actions of a few people in leadership positions cause tremendous monetary losses and undermine investor confidence, both of which can threaten economic stability.

The FBI has also compensated for the decrease in SAs addressing traditional criminal matters by leveraging resources through the Organized Crime Drug Enforcement Task Force and High Intensity Drug Trafficking Area initiatives. In addition, the FBI has shifted criminal resources to implement the Child Prostitution and Violent Crime Task Force initiatives. The child prostitution initiative is a coordinated national effort to combat child prostitution through joint investigations and task forces that include FBI, state and local law enforcement, and juvenile probation agencies. This initiative has resulted in more than 500 child prostitution arrests (local and federal combined), 101 indictments, 67 convictions, and the identification, location, and/or recovery of 200 children. To address violent crime, the FBI has partnered with other state and local law enforcement agencies to create 24 Violent Crime Task Forces throughout the U.S. The FBI also funds and operates 18 Safe Trails Task Forces to address violent crime in Indian Country.

In addition to the above initiatives, the FBI has continuously worked to use technology, intelligence analysis, and enhanced response capability to leverage criminal program resources. In October 2005, the National Crime Information Center (NCIC) fugitive data base was integrated with the Department of State passport application system, resulting in automatic notification when fugitives apply for United States passports. In December 2005, eight Child Abduction Rapid Deployment Teams were established in four regions of the United States. These teams are available to augment field office resources during the crucial initial stages of a child abduction. The FBI is currently developing a means of integrating sex offender registries and other public data bases to better identify sex

offenders in the vicinities of child abductions and to "flag" sex offenders who have changed locations without satisfying registration requirements.

**53. As you know, when individuals wish to naturalize and adjust their status, the US Citizenship and Immigration Services requests name checks from the FBI. We have had a number of cases in Ohio where the FBI backlog is creating very long delays which are harming the people who are requesting citizenship or waiting to have their names cleared for sensitive work. For example, my office has heard about long-term lawful permanent residents from Ohio who are applying to become U.S. citizens, and applied for name checks as far back as October of 2003, with no results yet. Some of these people are losing benefits that they would be entitled to, and which they rely on, if their names were cleared, yet they can't seem to get an answer from the FBI. Another Ohio resident will lose his job this week at Wright-Patterson AFB because his name check, submitted in August 2003, has not yet cleared.**

**Of course, it goes without saying that we need to take the time to make sure that applications for citizenship and clearances are thoroughly screened, but it is critically important that we do it in a timely way, both for security purposes and also to avoid the great hardships that these delays are imposing on many innocent and deserving applicants. I'm told that over a quarter-million cases have been pending for several years, which seems to be an unacceptably large backlog. What resources are being provided to address this problem, and when do you think the backlog will be cleared?**

**Response:**

The FBI is sensitive to the impact of the delays in processing name check requests and is doing all it can to streamline the current, labor-intensive, manual process. Prior to 9/11/01, annual incoming workload averaged 2,500,000 name checks requests per year. The National Name Check Program (NNCP) is experiencing a post 9/11 spike in incoming work that peaked in 2003 at 6,309,346. The current workload averages 3,500,000 name checks per year. After 9/11, the FBI and United States Citizenship and Immigration Services (USCIS) agreed to enhanced search criteria and initiated a re-processing of 2,700,000 name checks. Of these, 15,088 remain pending final processing. Currently, the USCIS Name Check backlog is 302,016 name check requests.

Below is a summary of the initiatives the FBI is undertaking to address the backlog:

- The Name Check program is moving toward automating a primarily manual process by scanning paper files to provide machine-readable documents to build an Electronic Records System to allow for future automation of the process, which will reduce time spent locating files. At

this time, the FBI is scanning all paper files required for the Name Check process.

- The FBI is making enhancements to its Dissemination Database that will promote a paperless process within the next two or three months and provide a platform for commercial off-the-shelf products to greatly enhance search capability, improving tracking and workflow management.
- The FBI is collaborating with customer Agencies to enhance Name Check staffing by providing temporarily assigned employees and contractors to assist in the name check process.
- The FBI is in receipt of a custom Employee Training Program to significantly reduce new employee development time.
- The FBI is aggressively pursuing ways to better customer relations. Name Check staff and USCIS staff interact on a daily basis regarding Name Check Issues. In March and April 2006, Name Check and USCIS staff jointly briefed Congressional staffers on name check and immigration issues.
- The FBI is pursuing a Fee Study to ascertain the cost of providing a name check to customer agencies. This will allow appropriate adjustment to fees charged thereby providing increased income needed to adequately resource the NNCP.
- The FBI is working with internal IT resources to improve search techniques with existing technology to increase quality of searches.
- RMD's NNCP is initiating technology upgrades in FY 2008 with a \$4.2 million budget request.
- The RMD has initiated contracts to procure contractors to assist in processing name checks.

It is difficult to pinpoint a time when the backlog will be cleared because of the continuous incoming volume of name check requests versus the currently static limited resources of the NNCP. Additionally, the length of time a name check is pending depends on a number of factors that are case specific, such as the number of files an analyst must obtain (which is dictated by the number of "hits" on a name), the location and availability of those files, and the amount of information contained in a file that must be individually reviewed by an analyst. The steps

referenced above should allow the NNCP to accelerate its productivity in the near future allowing for a significant reduction on the backlog.

**54. We have spoken before about the need for FBI Field Offices to have so-called SCIFs – Secure Compartmented Information Facilities -- where agents and prosecutors can examine classified information safely and securely. Obviously, this is a critical issue -- if we don't have enough space for our people to examine classified materials and enough classified computers and phone lines, we just can't fight terrorism effectively. In other words, if we don't have enough SCIF space, FBI agents will not be able to fight terrorism to the best of their ability. Despite the importance of this issue, I hear that many FBI field offices throughout the country still have inadequate SCIFs.**

- a. What, if any, plans does the FBI have to upgrade or expand its SCIF facilities?**
- b. What is delaying the deployment of adequate SCIF facilities?**
- c. What is your time-line for resolving the problems with SCIF facilities?**

**Response to subparts a-c:**

SCIFs are being constructed on two tracks: (1) the first track includes those offices scheduled for standard renewal or relocations projects; (2) the second track includes those offices where new or expanded SCIFs are being constructed according to identified need, based primarily on a risk assessment.

In FY 2005, 5 Field Division offices, about 25 Resident Agencies, and 4 FBIHQ off-sites were undergoing standard renewal/relocation projects on the regular cycle, and some of these are still in the construction phase. As part of this cycle, 9 Field Division offices, 25 Resident Agencies, and 5 FBIHQ offsite projects are planned for each of the following years (FY 2006 and FY 2007).

Within the NSB, the Secure Work Environment Working Group has ranked the top 100 facilities for non-routine construction, based on a risk assessment. The FY 2006/2007 Secure Work Environment SCIF construction program will address these top 100 facilities (based on risk), in an effort to bring their capability in line with their mission.

The Secure Work Environment SCIF construction program is budgeted at \$40,500,000 for FY 2006 (a \$20 million enhancement on top of the \$20.5 million dollar base). The President's budget for FY 2007 includes approximately \$63,700,000 for SCIF construction (\$30,500,000 in the base).



**55. The FBI's computer system has been woefully ineffective and outdated for years, and it is critical that the new Sentinel computer system be implemented quickly and fully.**

**a. You mentioned in your written testimony that Sentinel will be rolled out over four years and in four phases. What are they, and what is the timeline for each phase?**

**Response:**

Phase 1, scheduled for completion in April 2007, introduces the new Sentinel portal that provides access to legacy data, the case management workbox, and infrastructure components. The portal will initially provide access to legacy system data and will support future access to the new investigative case management system. The portal will employ web services technologies and provide users with browser access to investigative data without requiring them to understand the changes taking place in the system design. The first phase establishes a single point of entry for case management; improves the current web-based ACS capabilities by summarizing a user's workload on his dashboard, rather than requiring him to perform a series of queries to discover it. Furthermore, to simplify data entry into the FBI's Universal Index (UNI), a new entity extraction tool will identify persons, places, and things for automated indexing. Finally, core infrastructure components will be selected, and these may include an Enterprise Service Bus and foundation services.

Phase 2, scheduled for completion in May 2008, will begin the transition to paperless case records and electronic records management. Phase 2 will provide the information assurance and records management foundation upon which all future application services can be built. We will begin the replacement of legacy case management applications by integrating a commercial off-the-shelf database management system that will serve as the case document management repository, replacing the Electronic Case File portion of ACS. A workflow tool will support the flow of electronic case documents through the review and approval cycles. This phase will address the VCF Initial Operational Capability users' concerns that a paperless environment is necessary to obtain the benefits of automated workflow. A new security framework will be implemented to enhance system access authorization, role-based access controls, auditing, and Public Key Infrastructure-based electronic signatures.

During Phase 3, scheduled for completion in February 2009, the new global index database will replace UNI in ACS. The Sentinel global index will incorporate functional enhancements to overcome UNI's limitations. Sentinel will provide the ability to create and store index entries at both document and case levels, unlike UNI, which does not correlate index entries to documents. Sentinel index entry

types (i.e., persons, organizations, locations, incidents, property, and communication accounts) will support a wider range of attributes than currently offered by UNI. Furthermore, to improve the quality and completeness of index information, Sentinel will automate the extraction of index entries from the content of case documents. All index information within Sentinel will be searchable by leveraging the advanced searching capabilities that will have been integrated into Sentinel in Phase 2.

Phase 4, scheduled for completion in December 2009, will implement new case and task management and reporting capabilities and will begin the consolidation of case management systems. At the end of this phase, legacy systems will be shut down and the remaining cases in the Electronic Case File system will be migrated. Phase 4 will involve the replacement and consolidation of the following systems: Investigative Case Management, ASSET, Criminal Informant Management System, Financial Institution Fraud, Bank Robbery Statistical Application, Integrated Statistical Reporting Analysis Application, Case Document Access Report, and Guardian Threat Tracking System. Incremental changes to the portal and other services (e.g., searching) will be needed to accommodate new features being introduced.

**b. Please elaborate as to what the FBI is doing to make sure that it is going to be done on time and at no more cost than what was contracted for?**

**Response:**

Several measures have been initiated to tighten accountability in the execution of FBI contracts. Among other measures, all contracting officers will receive updated training with respect to the contract process that outlines current policy, regulatory changes, and new initiatives. In addition, the FBI's Finance Division has been reorganized to create a new unit responsible for coordinating acquisition planning, tracking, and reporting requirements for major programs. This unit will coordinate the development of an acquisition plan that clearly defines and documents the roles and responsibilities of key personnel, including the contracting officer, contracting officer's technical representative (COTR), program manager, property manager, and financial manager. These measures are designed to address the issues raised in the report by the GAO, including the need to establish clear lines of authority and accountability.

In the specific case of the Sentinel contract, the FBI has taken care to lay the groundwork for a successful major investment. The FBI has already implemented steps to ensure that all costs are authorized in advance, verified when products are delivered, and validated when invoiced. The Sentinel PMO includes both a dedicated contracting officer and a Business Management Unit (consisting of a

government business manager, budget analyst, Earned Value Management (EVM) analyst, cost estimator, and full-time COTR), which will track, monitor, and control all program and developmental costs.

Additionally, a separate, dedicated cost code for Sentinel has been established by the FBI's Chief Financial Officer (CFO) within the OCIO, allowing Sentinel, OCIO budget administration, and CFO teams to jointly track and control Sentinel costs through the Budgetary Evaluation and Analysis Reporting System and the oversight process. The FBI will augment this staff with audit support from the Finance Division to review invoicing and with the addition of an IV&V contractor, who will review the activities of the development contractor and the PMO to ensure the proper execution and delivery of the Sentinel system.

The FBI has conveyed to Sentinel's contractor, Lockheed Martin, the importance of detailed cost tracking and adherence to established policies and protocols based on the recent reviews by the GAO and the DOJ IG. Lockheed Martin understands our concerns and has assured us they will implement appropriate policies and procedures. Lockheed Martin's President and Chief Executive Officer, Robert Stevens, has stated that the Sentinel effort is one of his top six priorities. He will receive monthly updates on the status of the program from his leadership team. The President of Lockheed Martin Information Technology, Linda Gooden, stated during the 3/16/06 press event announcing award of the Sentinel contract: "Success is not an option; it is a mandate." The contract vehicle is structured so the contractor has clear reporting requirements, deliverables, and milestones. Although we do not anticipate Lockheed Martin will fall short in contract performance, the FBI has established managerial and contractual mechanisms to assess contractor performance throughout the process.

**c. You have said that the contract can be terminated in whole or in part upon identification of poor performance. If that were to happen, what is the alternative? In other words, is termination a credible threat to maintain performance quality?**

**Response:**

The FBI intends to succeed on this project and has dedicated considerable Program Management resources to ensure that any required corrective action is identified early enough to minimize poor performance. Nonetheless, the FBI is fully prepared to terminate the contract if warranted. We believe the termination of such a highly visible contract is a credible threat to a company such as Lockheed Martin.

**d. You mentioned the Independent Validation and Verification of the monthly Earned Value Management Reports. Beyond that, to what extent will outside experts monitor the progress of the creation and implementation of Sentinel?**

**Response:**

Several external agencies/groups will monitor or consult on Sentinel's development and implementation, including the following.

- Both GAO and the DOJ IG will audit the Sentinel program's developmental phase to assess the PMO's progress on Sentinel implementation.
- DOJ's Department Investment Review Board (DIRB) provides stewardship of DOJ's major IT investments and ensures they are aligned with the Department's mission and fiduciary obligations. The quarterly board is chaired by the DAG and vice-chaired by the DOJ CIO. That board has a disciplined agenda focused on program risks and risk management, budget and spending, and return on investment. After each program briefing, the board evaluates the program and "grades" the program's status. The DIRB also determines what areas require further review (action items).

The Sentinel Program Manager presented the Sentinel Program to DOJ's DIRB in early January 2006, receiving conditional approval to continue the Sentinel program along with a few follow-up action items. The Program Manager responded to those issues, in writing, in mid-February 2006, and the DIRB gave the program "passing" marks. The Sentinel Program Manager formally addressed action items and the status of the program during the DIRB's presentation in early May 2006. At that time, the DIRB rated the program as "green" (acceptable) for program management readiness and "yellow" (moderate risk, needing periodic reviews) for the program itself. Although briefings are provided at the request of the board, the Program Manager has been briefing the DIRB on a quarterly basis and responding to any follow-on questions or required actions in a timely manner. We anticipate participating in future presentations to the DIRB.

- The FBI receives the volunteer assistance of several advisory groups comprised of well-regarded individuals from various private, corporate, and academic fields. For example, the Director's Advisory Board focuses at the strategic level, suggesting and assessing organizational strategies. This board meets quarterly and is chaired by Arthur Money, former Assistant Secretary of Defense for Command, Control, Communications,

and Information. Other members of this board include Lee H. Hamilton, Charles S. Robb, Richard L. Thornburgh, and James Q. Wilson. Other advisory boards include the CIO IT Advisory Council and the Markle Foundation. Sentinel also receives oversight from NAPA and the Surveys and Investigations Staff of the House Committee on Appropriations.

- Representatives of OMB, the ODNI, the DAG, and DOJ's CIO also meet periodically with the Sentinel Program Manager and senior managers in the FBI's OCIO and Finance Division for updates on various facets of the program.

### **Questions Posed by Senator Leahy**

#### **DOMESTIC SURVEILLANCE OF PEACE GROUPS**

**56. In February, the *Seattle Post-Intelligencer* reported that Federal Government antiterrorism agencies, including the FBI, conducted surveillance of local peace groups during recent Peace Fleet protests at Seattle's Seafair festival. Was the FBI involved in such surveillance and, if so, please explain the circumstances surrounding such surveillance.**

#### **Response:**

The FBI did not participate in the surveillance of any local peace groups during Seattle's Seafair festival, which was the site of recent peace fleet protests.

**57. At the hearing, we discussed the FBI's surveillance of the Thomas Merton Center (TMC), a Catholic peace organization in Pittsburgh. An FBI memo dated November 29, 2002, and titled "IT Matters" states that FBI agents photographed TMC leaflet distributors at a public anti-war event on November 29, 2002. You testified that the agents "were attempting to identify an individual who happened to be, we believed, in attendance at that rally." Please provide copies of *earlier* investigative memos that document the basis for the agents' belief that a person of interest in an International Terrorism Matter would be present during TMC leafleting activities on November 29, 2002.**

#### **Response:**

The investigation of the individual whose presence at the rally was anticipated is still ongoing. Consequently, we are not able to discuss this investigation further. In addition, as noted in response to Question 59, below, these matters are pending review by DOJ's OIG.

**58. Another FBI memo dated February 26, 2003, suggests that the FBI's surveillance of the Thomas Merton Center on November 29, 2002, was not an isolated incident. The memo, also titled "International Terrorism Matters," states that an investigation by the Pittsburgh Division Joint Terrorism Task Force (JTTF) revealed that TMC "has been determined to be an organization which is opposed to the United States' war with Iraq." The memo goes on to describe the anti-war messages on TMC's website, and also discusses anti-war protests that had taken place earlier in the month in Pittsburgh and across the country. When the FBI released this document in March 2006, it issued a Press Response stating that the memo "was actually a draft which was never finalized – nor made a part of an FBI file." That is heartening, but it is not a complete explanation.**

- a. What was the nature of the JTTF investigation documented in this memo?**
- b. How many investigators were involved?**
- c. Was the investigation approved by a supervisory agent?**
- d. What does it mean to say that the memo was never "made a part of an FBI file"? If it could be retrieved in response to a FOIA request regarding TMC, could it not also be retrieved for other purposes?**

**Response to subparts a-d:**

In response to the FOIA request, the FBI conducted a manual search beyond its record system for all information responsive to the request. The 2/26/03 document was discovered during the search of a stenographer's computer hard drive for responsive information. This document identifies no author or file number and contains no markings indicating supervisory approval for entering into any FBI record keeping system. The Pittsburgh Division, where the document was located, was unable to identify the actual author or locate a file associated with this document. The document could possibly have been a draft that was never approved for filing. As a "loose" document, it could be retrieved only by someone with access to the computer on which it had been saved.

**59. At the hearing, you said you would have the Inspector General look into this matter regarding the Thomas Merton Center. Have you referred this matter to the Inspector General and, if not, do you still intend to do so and when?**

**Response:**

The FBI has referred this matter to the DOJ OIG and has been informed that the OIG will conduct a preliminary inquiry into the Thomas Merton Center issue to determine whether it is appropriate to formally open a case.

## INTELLIGENCE VIOLATIONS

**60. According to a recent report by the Office of the Inspector General, the FBI reported more than 100 possible intelligence violations to the President's Intelligence Oversight Board over the past two years. These violations included incidents where FBI agents intercepted communications outside of the scope of the order from the FISA court, and incidents where FBI agents continued investigative activities after their authority expired. What steps is the FBI taking to reduce the incidence of these types of intelligence violations?**

### Response:

The report by the IG referred to in this question included the results of the IG's examination of the FBI's process for reporting to the Intelligence Oversight Board (IOB) possible violations involving intelligence activities. The FBI takes all reports of possible IOB violations seriously and has a comprehensive process for conducting legal reviews of possible violations and referring them to the appropriate entities. Our internal process encourages the over-reporting of possible violations involving intelligence activities.

The IG has found no examples of willful disregard for the law or for court orders by the FBI. As the IG report notes, when possible violations are discovered, the FBI acts quickly to correct the error. In instances in which the violation involves over-collections or overruns involving the FBI's use of FISA authorities, the unauthorized collection is sealed and sequestered from the investigation. The possible violation is also then reported to the appropriate oversight entities.

Over the past four years, the FBI has realigned its investigative resources to balance the prevention of terrorism and foreign intelligence threats, but not at the cost of violating civil rights or civil liberties. FBI Special Agents are held to a very high standard in complying with the procedures currently in place to protect civil liberties and constitutional rights when using the legal tools appropriate for national security investigations.

## TRILOGY AND SENTINEL

**61. The Inspector General's March 2006 audit report on the FBI's planning for Sentinel identified several ongoing concerns about the project, including the FBI's ability to reprogram funds to pay for Sentinel without hurting other mission-critical operations. What steps are you taking to ensure that other critical FBI programs will not be hurt because of the \$425 million price tag for Sentinel?**

### Response:

The FBI has determined that no reprogramming will be required for FY 2006 Sentinel operations. The funding requested in the President's FY 2007 budget will fund O&M for Phase 1 and most of the system development, training, and program management costs for Phase 2. If there are additional Phase 2 costs beyond the \$100 million in the President's budget, the FBI will work with DOJ, OMB, and Congress to redirect existing funds where available or request additional funding as needed. Funding for Phases 3 and 4 and for the remainder of O&M for all Phases will be requested in future budget submissions. As noted in the response to the IG, the FBI evaluates the operational impact of any proposed reprogramming and takes that impact into consideration in all reprogramming decisions. The FBI routinely provides this impact assessment and other relevant information to DOJ, OMB, and Congress.

**62. The Inspector General's report noted that, as of January 31, 2006, the FBI's Program Management Office (PMO) for Sentinel had only 51 of the planned full staffing level of 76 employees and contractors on board. The report cautioned that without full staffing during the first phase of the project, "the FBI runs the risk of not being able to oversee adequately Sentinel's aggressive delivery schedule." When do you expect to have fully staffed the PMO with qualified personnel?**

**Response:**

The Sentinel PMO currently has funding for 77 positions, including 19 employees and 58 contractors. Currently, 58 of the 77 employees are on board (13 employees and 45 contractors). Six of the employees are on temporary duty or detail to the PMO from other offices.

The PMO had deferred hiring for some positions until the contract was awarded because filling those positions was unnecessary until that point. We are currently recruiting to fill five positions; those candidates will be selected within the next few months. The PMO will also begin active recruitment to fill an additional six positions (four employee and two contractor positions) within the next few months. The start dates for those in these six positions will vary depending on whether they are hired internally or externally, due to a number of factors including their security clearances and the time required for their background investigations.

Eight positions are currently vacant. Filling those positions has been deferred until we are closer to Phase 2 because they will support either O&M functions or Phase 2 development. We anticipate recruiting for these positions near the end of 2006.



**63. The Inspector General's report expresses concern that although the FBI has considered its own internal needs when developing Sentinel's design requirements, it has not yet adequately examined Sentinel's ability to connect with external systems in other Justice Department components, the Department of Homeland Security, and other agencies. The report warns, "If such connectivity is not built into Sentinel's design, other agencies could be forced into costly and time-consuming modifications to their systems to allow information sharing with the Sentinel system." What steps is the FBI taking to prevent this scenario and ensure Sentinel's ability to share information with other intelligence and law enforcement agencies?**

**Response:**

The Sentinel System Requirements Specification mandates the use of the open data exchange standards and protocols recently identified by DOJ for the exchange of law enforcement information and by other government agencies for the exchange of intelligence information. The Sentinel PMO has identified the legacy-supported law enforcement and intelligence systems with which Sentinel will interface initially and has developed the "as-is" (current) Interface Control Documents (ICD). The PMO will also analyze existing interfaces and develop the "to-be" (future) ICD necessary for additional information sharing. Sentinel is being developed to be compatible with the Extensible Markup Language (XML) standards used for data tagging and marking in both DOJ and the IC. The DOJ and IC standards will eventually merge to form the NIEM for metadata, with which Sentinel will also be compatible. The NIEM is managed by DOJ and DHS and is aligned with ODNI work. The NIEM will, therefore, provide a common standard for sharing information among law enforcement (Federal, state, tribal, and local), IC, and homeland security agencies.

As part of the Sentinel PMO's life-cycle management system, capacity for access by other law enforcement and IC agencies will be designed, assessed, reviewed, and approved as part of each Sentinel phase's preliminary design and design reviews. Sentinel's Test and Evaluation Master Plan calls for early interface testing to ensure compatibility and specifies interface monitoring and debugging tools to support verification and troubleshooting. The Sentinel PM provides monthly status briefings to OMB, ODNI, and DOJ on how these entities will use the national information sharing environment architecture, and there is additional close coordination with DHS regarding information sharing. Sentinel's PMO architects have also met with a number of other intelligence and law enforcement agencies through participation in Federal information sharing initiatives that include the NIEM, the Law Enforcement Information Sharing Program (LEISP), and the Law Enforcement Exchange Standard (LEXS). More than 30 government agencies participate in these initiatives and will conform to the information sharing specifications they establish.

The Sentinel PMO's work with outside agencies to improve information sharing capabilities includes the following.

- Sentinel architects have met on three occasions with DOJ's Chief Enterprise Architect to continue dialogs on the subjects of NIEM, the Global Justice XML Data Model (GJXDM), and LEISP. The FBI and DOJ are working together to harmonize information sharing initiatives and pursue a common interface to external systems.
- Sentinel architects have met with DOJ's Chief Data Architect to continue discussion of LEXS 2.0, particularly as it relates to the FBI's case file interface to our Regional Data Exchange (R-DEx) system. The R-DEx system is currently managed and maintained by the FBI's Office of IT Program Management, which also oversees the Sentinel Program. Further meetings are scheduled to examine revised interface requirements between R-DEx, the National Data Exchange (N-DEx), and Sentinel.
- Sentinel architects have worked extensively with DHS since the inception of the NIEM initiative. In addition, a representative of DHS Immigration and Customs Enforcement is now co-located with the Sentinel PMO and has attended Requirements Clarification Reviews with the Sentinel team.
- Sentinel architects have worked with ODNI's chief architect for more than two years. Meetings are scheduled to further discuss the NIEM initiative and the methods with which IC Metadata Working Group (ICMWG) artifacts are being harmonized with NIEM. The Sentinel architect has worked with the Terrorist Watchlist Person Data Exchange Standard (TWPDES) for almost two years and is familiar with the exchange standards envisioned by the TSC and the NCTC.
- Sentinel architects have reviewed the Common Information Sharing Standards (CISS) promulgated by the PM for the Information Sharing Environment (ISE), and much of the work needed to harmonize the FBI data model to these standards has already been done. The FBI will continue to work with Ambassador McNamara's staff and will move forward on their recommendations once the ISE PM's Concept of Operations has been finalized. Extensive feedback on the Concept of Operations has been provided to the FBI's Office of IT Policy and Planning for incorporation into the overall FBI response on CISS.

The Sentinel PMO's approach to information sharing concentrates on the standardization efforts promulgated by other agencies within the Federal Government. Work on the technical committees and with PMOs for the NIEM,

GJXDM, TWPDES, ICMWG, ISE PM, ODNI OCIO, DOJ Enterprise Architecture Unit, and others gives the Sentinel PMO access to virtually every concerned government agency, with all of whom we share the common goal of sharing terrorism data in a near real-time environment. The Sentinel PMO will continue to interact and collaborate with all external system owners.

**64. Inspector General Fine testified at the hearing that potential weaknesses in cost controls remain a continuing project risk for Sentinel. What are you doing to address this concern, so that the already high cost of the Sentinel program will not get out of control?**

**Response:**

Please see the response to Question 55, above.

**65. GAO's report on Sentinel's predecessor, Trilogy, found that weak controls on the part of the FBI and GSA resulted in the Bureau paying more than \$10.1 million in unallowable costs and in the FBI being unable to account for more than 1,400 pieces of missing equipment, valued at approximately \$8.6 million. The GAO report further noted that, given the scope of the oversight problems on the Trilogy project, there may be additional questionable costs not reflected in the its audit report. The GAO also recommended that you and the GSA Administrator take steps to investigate and recover these funds. Has the FBI taken any steps to recoup any of the at least \$10.1 million in unallowable costs of Trilogy? If so, please state the amount of taxpayer funds that have been recovered by the FBI to date.**

**Response:**

The GAO audit did not find or quantify unallowable costs, although weaknesses in internal controls did render the FBI vulnerable to paying potentially unallowable costs. GSA/FEDSIM is finalizing negotiations with GSA Deputy Assistant Inspector General (IG) for Auditing, FBI, and DCAA to have DCAA conduct an overall program audit of both task orders. The scope of the program audit will include the costs identified by GAO as potentially questionable. Upon completion of the program audit, DCAA will conduct the final closeout audit of both task orders. GSA/FEDSIM and the FBI will pursue reimbursement of any improper costs identified by that audit.

**INFORMATION TECHNOLOGY**

**66. According to several recent press reports, some 2,000 employees of the FBI's New York Field Office will not all have access to e-mail accounts until the end of this year. The Assistant Director in charge of the New York Field Office has reportedly stated that the lack of email is a funding issue. How many FBI agents and analysts – in New York and**

**elsewhere -- currently operate without a government email account, and why? When do you expect that all FBI personnel will have email accounts?**

**Response:**

Typically, FBI personnel access the Internet through either Law Enforcement Online (which is primarily used for law enforcement purposes) or the Unclassified Network (UNet) (which is a dedicated network that serves the FBI's operational and administrative needs, providing Internet connectivity and Blackberry service).

UNet was established in 2002 as the FBI's Internet Café (I-café). Similar to a public I-café, we anticipated that the UNet would be used in a kiosk environment where FBI employees would access the Internet at clustered locations. At its inception, the program was neither envisioned nor funded to provide individual users with desktop access.

In 2004, additional funding permitted the FBI to extend UNet access. To date, FBIHQ and 52 of the FBI's 56 Field Offices have UNet access, and some Field Offices also have locally arranged Internet access. A total of 24,365 UNet accounts have been assigned to FBI employees, task force members, and contractors. By the end of FY 2006, the UNet will be able to support 25,000 accounts and Internet access will be available on an additional 5,400 desktops. As additional funding becomes available, UNet will be further expanded to include the remaining FBI Field Offices and their Resident Agencies, with the ultimate goal of providing desktop UNet access for all FBI users.

Blackberry devices were first used in the FBI as a "continuity of operations" tool in advance of the Afghan conflict. There is, however, no dedicated funding for Blackberry purchase or use, and these devices are used by FBI Divisions on a limited fee-for-service basis. Expansion beyond this use is not possible without a substantial investment in both UNet and the Blackberry program.

**INFORMATION SHARING**

**67. The GAO's most recent report on information-sharing found that more than four years after 9/11, we do not have government-wide policies and processes in place to improve the sharing of critical counter-terrorism information. What steps is the FBI undertaking to improve information-sharing with its Federal and local partners? What barriers do you see to effective information-sharing? What more can Congress do to help the Bureau improve its information-sharing capabilities?**

**Response:**

The FBI has instituted several means of improving information sharing with our Federal, state, and local partners in the law enforcement and intelligence communities. Among these is the establishment of the FBI's Information Sharing Policy Board, which is chaired by the principal officer of the FBI for information sharing policy (currently the EAD, NSB). This board brings together the FBI entities that generate and disseminate law enforcement information and intelligence and is charged with implementing the FBI's goal of sharing by rule and withholding by exception. The FBI is also actively participating in the interagency effort to establish a terrorism ISE under the Presidential guidelines issued on 12/16/05.

The National Joint Terrorism Task Force (NJTTF), staffed with representatives from 38 Federal, state, and local agencies, enhances the coordination and cooperation among these government agencies. Through the NJTTF, the FBI provides a point of fusion for terrorism intelligence and supports the JTTFs, which are also comprised of personnel from the FBI and many other Federal, state, and local agencies and are located throughout the United States. Both NJTTF and JTTF members have access to FBI information systems.

Field Intelligence Groups (FIGs) are the FBI's primary interface for receiving and disseminating intelligence information, and a FIG has been established in each FBI field office. The FIGs, which complement the JTTFs and other task forces, are expected to play a major role in ensuring that the FBI shares what we know with others in the IC and with our Federal, state, local, and tribal law enforcement partners. FIGs participate in the increasing number of State Fusion Centers and Regional Intelligence Analysis Centers.

Within the law enforcement community, the FBI's National Information Sharing Strategy (NISS) is part of DOJ's LEISP and builds upon the capabilities offered by the FBI's Criminal Justice Information Services (CJIS) Division. The TSC, which was established to provide for the appropriate and lawful use of terrorist information to screen for known and suspected terrorists, also leverages the CJIS backbone to provide real-time actionable intelligence to appropriate Federal, state, and local law enforcement. Multiple Federal agencies participate in this effort, including the FBI, DOJ, DHS, DOS, and Department of the Treasury.

In the NCTC, analysts from the FBI, CIA, DHS, and DoD work side by side to identify and analyze threats to the U.S. and our interests. NCTC analysts produce the National Threat Bulletin, the Threat Matrix, and other analytic products. FBI SAs and analysts are also detailed to numerous other Federal entities, including the CIA, NSA, National Security Council, Department of Energy, Defense

Intelligence Agency, Defense Logistics Agency, and DoD's Regional Commands, adding yet another means through which information is shared with these organizations. The FBI also operates six highly specialized Regional Computer Forensic Laboratories designed to provide forensic examinations of digital evidence. In each of these laboratories, law enforcement agencies from all levels of government train, work, and share information.

Evolving technology offers ever greater ability to share classified information in secure environments. Within the IC, the FBI has a two-level approach. For those agencies that operate at the Top Secret/SCI level, the FBI is investing in the SCI Operational Network, a secure FBI network that is linked to the DoD Joint Worldwide Intelligence Communications System network used by the CIA, NSA, and other Federal agencies. The FBI also makes national intelligence more readily available to state, tribal, and local law enforcement agencies through the Law Enforcement Online network. Infrastructure threat information is provided to the private sector through the "sensitive but unclassified" InfraGard network.

For those agencies that operate at the Secret level, we have connected the FBI's internal electronic communications system to the Intelligence Community network (Intelink-S), which serves military, intelligence, diplomatic, and law enforcement users. As a result, FBI SAs and analysts who need to communicate at the Secret-level with other agencies can do so from their desktops.

The Law Enforcement N-DEx will provide a nationwide capability to exchange data derived from incident and event reports, including names, addresses, and non-specific crime characteristics. This information will be entered into a central repository available to law enforcement officials at all levels. The N-DEx is complemented by the R-DEx, through which the FBI is able to participate with Federal, state, tribal, and local law enforcement agencies in regional full-text information sharing systems under standard technical procedures and policy agreements.

**68. The Office of the Inspector General recently released an audit report on the FBI's efforts to protect U.S. seaports from terrorism. The OIG review found that the FBI and the Coast Guard have not yet resolved issues regarding their overlapping responsibilities to handle a maritime terrorism incident. In his prepared hearing testimony, Inspector General Fine warned that, "a lack of jurisdictional clarity could hinder the FBI's and the Coast Guard's ability to coordinate an effective response to a terrorist threat or incident in the maritime domain."**

**a. In your view, what is preventing the FBI from reaching an accord with the Coast Guard regarding this crucial jurisdictional question?**

**b. Is legislative action needed to resolve this impasse?**

**Response to subparts a and b:**

Please see the response to Question 19, above.

**c. What do you think of the OIG's 18 recommendations for improving the FBI's counterterrorism efforts regarding seaport and maritime activities?**

**Response:**

The FBI responded to the OIG report by letter from CTD Assistant Director Willie Hulon to IG Fine dated 3/17/06 (Enclosure A). That letter identifies the steps the FBI has taken and is taking in response to each of the findings and recommendations identified in the OIG report. The FBI is preparing a formal reply to the report that documents these and subsequent steps taken, and this process will be repeated every 90 days until the FBI has completed its response to all report findings and recommendations.

**TERRORIST WATCHLIST**

**69. During the past year, the Terrorist Screening Center has initiated a record-by-record review of the terrorist screening database to ensure accuracy, completeness, and consistency of the records. Inspector General Fine has reported that the database currently contains more than 235,000 records and that TSC's review will take several years.**

**a. How can a list this large possibly be helpful to the FBI and its law enforcement partners in the effort to thwart terrorism?**

**Response:**

The suggestion that the "large" size of the Terrorist Screening Database (TSDB) somehow makes it less helpful is incorrect. The size of the TSDB does not adversely affect the efforts of the FBI and its law enforcement partners to thwart terrorism. Rather, the TSDB - as maintained by the TSC - now serves to link the domestic law enforcement and intelligence communities, a link that did not exist before the attacks of 9/11/01. On 9/9/01, one of the 9/11 hijackers was pulled over for speeding by a law enforcement officer in Maryland. Since there was no consolidated watchlist to alert that officer that the individual he had encountered was a known terrorist, the officer did not have a chance to give that terrorist any extra scrutiny.

The June 2005 DOJ OIG Audit Report (Report 05-27) identified the need for a consolidated terrorist watchlist and, based on that recommendation, the TSDB was developed as the U.S. Government's consolidated database of all terrorist identity information based on nominations received from the FBI and the IC. If it comes to the attention of the TSC that an identity no longer exhibits a nexus to terrorism, that identity will be removed from the TSDB. The TSC engages in an ongoing effort to maintain the most thorough, accurate, and current information possible in the TSDB.

Practically speaking, the FBI and its law enforcement partners conduct electronic NCIC queries of the TSDB, so the size of the TSDB is not a factor. If a query results in a positive or possible match, the investigator is advised to contact the TSC; these calls are resolved in approximately five minutes. Unlike the officer who encountered the 9/11 hijacker on 9/9/01, law enforcement officers today who call the TSC receive a quick response advising them whether they are dealing with a known or appropriately suspected terrorist. Armed with that information, these officers are able to ask relevant questions, conduct consensual searches, and be alert to suspicious information or possible associates. Information obtained through these encounters is then fed back to the TSC and the IC for analysis, better enabling the U. S. Government to "connect the dots."

**b. How much longer will it take for the TSC to complete its review?**

**c. What impact will the delay in getting an accurate terrorist watchlist have on the FBI's counterterrorism mission?**

**Response to subparts b-c:**

As of 5/21/06, the Terrorist Screening Data Base (TSDB) contained over 491,000 records, but these records do not represent 491,000 separate individuals, since one individual may have multiple aliases or name variants or may claim multiple dates of birth, each of which is counted as a separate record.

The record-by-record review of existing TSDB records began on 4/1/05, but we cannot predict when this review will be completed because priority reviews of particular segments of information continually intervene. For example, while TSC formerly relied on the accuracy of information provided by agencies nominating individuals for inclusion in the TSDB, in March 2006 TSC began to conduct its own detailed review of each nomination to ensure all placements in the TSDB are appropriate. TSC data integrity analysts have also been asked to review the records of 4,000 frequently encountered individuals to ensure their inclusion on the No Fly list is appropriate, to review 1,383 domestic terrorist subject records to ensure the accuracy of handling codes, and to review records



marked in VGTOF as "silent hits." ("Silent hit" coding means the FBI case agent will be notified electronically of an encounter but the encountering official will not be aware of the "hit." This coding is used for several reasons, including when the subject does not pose a safety risk to local law enforcement and the investigation of the individual was opened based upon single source reporting or based upon classified information from a foreign law enforcement agency.) These high priority reviews are being conducted along with the daily average of 1,000 new nominations and requests for modification of existing records, all of which must also be rigorously reviewed and verified to avoid misidentification.

These reviews are being conducted in order to ensure that individuals who are included in the TSDB erroneously and do not pose a terrorism risk are deleted from the TSDB. Clearly, erroneous inclusion in the TSDB exerts a negative impact on the individual, such as when the person is prohibited by Customs officials from entering the United States or by the TSA from boarding a plane. While the recent review of the records of frequently encountered individuals should minimize such impacts, the FBI takes all errors seriously and is working to eliminate them. A complete record review will not, however, adversely affect our national security, because the errors this review is designed to detect are errors of excessive inclusion in the TSDB rather than omission from it. For this reason, the time required to complete this review will not impede the FBI's counterterrorism mission.

**70. The Inspector General's June 2005 audit report on the Terrorist Screening Center found that its database designates nearly 32,000 "armed and dangerous" individuals at the lowest handling code, which does not require the encountering law enforcement officer to contact the TSC or any other law enforcement agency. Has anything been done to enable the TSC to designate individuals in such a way that law enforcement encountering them would be aware of the possible danger?**

**Response:**

The premise of the question is faulty because it intermingles two separate databases that contain two different types of information. As discussed further below, the "armed and dangerous" designation is used in the NCIC database, while the "handling codes" to which the question refers are used in the VGTOF database. Consequently, it is not correct to say the TSC database "designates nearly 32,000 'armed and dangerous' individuals at the lowest handling code," because the "armed and dangerous" designation and "handling code" designations are not used in the same database.

When a law enforcement officer queries NCIC, several items of information may be obtained, including past offenses, sentences, and outstanding arrest warrants.

This information may identify the person as armed and dangerous or may otherwise alert the officer to information important to the officer's safety.

VGTOF is a component of NCIC. A subject is included in VGTOF if he or she is known or suspected to have engaged in conduct constituting, in preparation for, in aid of, or related to terrorism (as provided in HSPD 6) and certain identifying information is known to law enforcement officials, as discussed further below. Because all those associated with terrorism are potentially dangerous, all terrorism-related VGTOF entries are designated "Approach with Caution," regardless of whether the individual's terrorism-related activity has been violent. Unrelated to the individual threat that may be posed by a given VGTOF subject, all terrorism-related VGTOF entries receive one of four handling codes to reflect the nature and quality of the identifying information available on the subject and to identify the proper law enforcement response if the subject is encountered.

All four handling codes indicate "Approach with Caution" because of the inherent danger in approaching a person known or suspected to have engaged in terrorist-related activity. The VGTOF handling code is not, however, designed to alert the law enforcement officer to the threat posed by the individual, since an individual's association with terrorism does not necessarily mean the individual is personally dangerous. While other NCIC information may alert the officer to a history of violent crimes, the VGTOF handling code itself does not provide this information. The VGTOF handling code instead relates to the amount and nature of the information available about the individual and, as additional information is obtained, a handling code may be revised to reflect that fact.

Additional information regarding the handling codes and related issues was provided to the Committee in response to Question 29 following the 7/27/05 hearing.

#### NATIONAL SECURITY LETTERS

**71. The Justice Department has reported that in 2005, the FBI issued 9,245 national security letters for information on 3,501 U.S. citizens and legal residents. Let me repeat two questions I asked you at the hearing, which you were unable to answer at the time. (A) How do the 2005 numbers compare to the same numbers over the past 10 years. (B) Would you support declassifying those earlier numbers (for calendar years 1995 through 2004) and, if not, please explain why that information needs to remain classified when comparable and more current information is now publicly available.**

**Response:**

During 2005, the number of National Security Letter (NSL) requests (excluding NSLs for subscriber information) for information concerning United States persons totaled 9,254 (versus 9,245 as set forth in the question). There were 3,501 different United States persons involved in these 9,254 NSLs.

Corresponding numbers are not available for the preceding 10-year period and it is not possible to retrieve them. These numbers were calculated for the first time in 2006 to report 2005 totals in satisfaction of the new reporting requirement enacted in the USA PATRIOT Improvement and Reauthorization Act of 2005 (3/9/06). To understand these numbers, please bear in mind the following points.

First, the above numbers reflect the FBI's good-faith effort to provide the most accurate information possible. However, because these numbers could not be compiled by computer, FBI personnel personally reviewed each 2005 NSL, confirming to the extent possible that any given United States person was not reported more than once. That effort was necessary because many names appear in the NSLs in a variety of forms or styles (e.g., John Doe and Johnny Doe; Elizabeth Roe, Liz Roe, and Betty Roe) and some individuals use one or more aliases. As a result, it is possible that, despite the best efforts of FBI personnel, the number of different United States persons reported above may include circumstances in which one person is reported multiple times.

Second, four statutes authorize the FBI's use of NSLs and the FBI has traditionally tracked NSL totals separately within each of those four categories. The FBI has not historically cross-referenced those four separate databases to distinguish different United States persons, in part because of the difficulties discussed above. This effort at cross referencing may also have resulted in errors.

Third, the FBI has not previously been required to distinguish between United States persons and non-United States persons when reporting NSLs involving financial institutions and consumer reporting agencies. While the FBI has compiled these numbers with as much accuracy as possible, this was accomplished by hand count and may include some inaccuracies.

Given the recent statutory requirement to compile and publicly report these numbers annually, the statistics sought by this question should be readily available for future years. It continues to be DOJ's position, though, that NSL numbers that were classified in previous years remain classified.

## FBI EFFORTS TO SEARCH THE FILES OF JACK ANDERSON

**72. In response to questions about the FBI's efforts to review the files of the late Jack Anderson, you stated that you were unfamiliar with the details of specific actions taken by the FBI.**

**a. Is it true, as was recounted by Senator Grassley, that FBI agents first approached Mr. Anderson's son, Kevin, and that he told the agents that he would discuss the request with his family before making a decision on whether to release documents?**

### Response:

The initial contact in this matter was a telephone call between FBI SAs and Mrs. Jack Anderson. The purpose of the call was to arrange a time for an interview. Mrs. Anderson's son, Kevin, subsequently contacted the SA who set up the interview to ask the reason for it and to request that his sister be present for the interview. Mr. Anderson advised that his sister was his father's caregiver in his later years and might be able to answer the FBI's questions. The evening after the first interview of Mrs. Anderson, an FBI Agent telephoned Mrs. Anderson for clarification of the ownership status of Jack Anderson's papers. Mrs. Anderson was unsure and directed the Agent to speak with her daughter. The Agent left a message for the daughter. When Mrs. Anderson's daughter failed to return the call, the Agent called Kevin Anderson, and he explained the ownership status of the papers.

**b. Is it true that FBI agents then approached Mr. Anderson's widow and tried to "trick" her into signing a consent form that, in the words of Senator Grassley, "she did not understand"?**

### Response:

As indicated above, the FBI first spoke to Mrs. Anderson in the presence of her daughter and with knowledge of her son. After determining from Kevin Anderson that the Anderson family still owned the Jack Anderson papers, an FBI Agent called Mrs. Anderson and scheduled a second meeting at Mrs. Anderson's convenience. During this second meeting, Mrs. Anderson voluntarily signed three "Consent to Search" forms regarding the papers, for the three possible locations of the papers. The "Consent to Search" form is written in plain English, and Mrs. Anderson never indicated that she did not understand the forms or was uncomfortable in any way about signing them. It should also be noted that the FBI has not attempted to use the signed consents to gain access to the papers.

**73. You testified that the FBI had recently c[o]me into possession of “information indicating that there may be classified national security documents within Mr. Anderson’s collection.” Is the FBI or the Department of Justice currently contemplating legal action to obtain access to the files of Mr. Anderson? If so, under what statutory authority would such an action be brought?**

**Response:**

Based on information that there are classified documents within the Anderson papers, the FBI and DOJ are concerned that public access to such materials might cause damage to the national security of the United States. The FBI and the DOJ are assessing a variety of options but no legal action is currently contemplated.

**Questions Posed by Senator Kennedy**

**I. Arab & Muslim Community**

**74. At the hearing, I asked you about the FBI’s recruitment efforts in the Arab-American and Muslim communities. You indicated that there have been tangible results and that you could provide the Committee with figures. With as much specificity as possible, please tell the Committee what the results of these recruitment efforts have been. Please provide us with the figures that you mentioned in your testimony. In addition, please confirm how many new agents have been added since recruitment efforts began.**

**Response:**

Since 09/11/01:

5,964 Applicants applied on-line for the SA position with a self-proclaimed fluency in a Middle Eastern Foreign Language.

506 SA applicants who speak a Middle Eastern Foreign Language had background investigations initiated.

162 SAs have been hired who have a Middle Eastern Foreign Language fluency.

The FBI has enhanced its recruitment initiatives for persons of Middle Eastern descent in myriad ways, including the following.

**Recruitment Consultants**

- *EdVenture Partners, Inc. (EVP)*. EVP was tasked with developing partnerships and recruitment initiatives in Middle Eastern communities. These communities were an untapped resource for the recruitment of qualified applicants. The EVP contract has developed partnerships that will provide the FBI with a new vehicle to recruit qualified applicants on a national level as well as improve the FBI's relationships within the Middle Eastern community.
- *Recruitment Enhancement Services (RES)*. In FY 2005, the FBI tasked this contractor to target applicants possessing critical foreign languages via "Internet mining" strategies. RES has been contracted by the FBI to utilize an innovative approach to recruit SA applicants fluent in critical foreign languages for which the FBI has a need. It is expected RES' innovative "Internet mining" techniques will greatly enhance the probability that applicants will successfully complete the FBI's processing and hiring procedures. RES received sufficient training pertaining to the needs of the FBI in late 2005 and developed their Internet strategy which is currently being implemented.

#### Advertisements

The FBI has conducted newspaper as well as television advertising on numerous Middle Eastern mediums, including, but not limited to: Afghan Community Television, Al Offok, Al Nahar, Bridges TV advertisement, Al Arabi, Al Hureya, Ultimate Media Inc., Detroit Chaldean Times, Al Akhbar, the Al-Sahafa newspaper, Arab World, Al Nashra, Al Manassah Weekly, the Arab Voice, Aramica, Al Arab Weekly, The Beirut, Arab American Business, Language Magazine, Arab American News, the Foreign Affairs Journal, Al Sahafa Newspaper, Dandana Arabic Television, Arab American Business Journal, the Arab American Chaldean Council, and the Middle Eastern Broadcasting Network of America.

#### Middle Eastern Partnerships

- *American Arab Anti-Discrimination Committee*. The FBI met with the American Arab Anti-Discrimination Committee regarding the recruitment of persons fluent in Middle Eastern languages. New ideas were discussed and added to the FBI's recruitment strategy targeting the Middle Eastern community and included: (1) utilization of monster.com's FAST TRACK to forward e-mails to targeted students and alumni meeting designated criteria; (2) requesting all Recruiters to identify Middle Eastern-oriented support groups on college campuses; (3) establishing a partnership with students on campus as well as internship programs; (4) identifying

organizations that employ students of Middle Eastern descent and invite them to tours of FBIHQ and Quantico; and (5) identifying on-board persons fluent in critical foreign languages or knowledgeable of Middle Eastern cultures to assist with recruiting.

- *United States Copts Association.* The FBI formed a partnership with the United States Copts Association whose membership consists of Egyptian Christians. This partnership was formed to network with the various churches and to advise the membership of the FBI's need for employees with Middle Eastern language abilities in the SA and other critical skilled positions such as Language Specialist and Contract Linguists. In November 2003, representatives from FBIHQ and the Los Angeles Division attended a dinner and a civic center event and discussed the FBI's need for Middle Eastern employees and employees with Middle Eastern language abilities.

#### Middle Eastern Student Programs

- *FBI Collegiate Marketing & Recruitment Program.* In FY 2002, the FBI entered into an agreement with EVP to initiate an education focused marketing approach to target students on diverse university campuses. This allows students, via a curriculum-based peer marketing strategy, to brand the FBI and market core occupation employment opportunities. This program has proven to be a great success.
- *Middle Eastern Foreign Language Honors Internship Program.* In 2005, the FBI developed a program to hire students as interns who possess fluency in a Middle Eastern language for the summer 2006 program. This program serves as an excellent feeder program to the SA position. Graduate and Senior level students are recruited to participate in this program. There were 16 students recruited for participation in this program and after language testing, 10 were selected to undergo the background investigation. Four students have successfully passed and will enter on duty 6/5/06 (one background investigation is still pending). This will be the first year for this program.

## II. Hate Crime Statistics

**75. You also testified that, "We keep statistics of hate crimes against Muslim-Americans, Sikh-Americans, Arab-Americans, and we can get you those." The FBI's report on Hate Crime Statistics, 2004 does not include specific information on Sikh-Americans and Arab-Americans. In light of reported and confirmed hate crimes against Arab and Middle Eastern communities since 9/11, why hasn't the FBI included a specific category in its**

**annual hate-crimes report that reflects the number of hate crimes targeting these communities? As I am sure that you are well aware, some Arab Americans are Christians so the existing category for anti-Muslim attacks is [i]nsufficient. Is the FBI willing to provide more information beyond “Anti-Other Ethnicity” to at least include “Anti-Arab Crimes?”**

**Response:**

Pursuant to the Hate Crime Statistics Act of 1990, the FBI's CJIS Division, Uniform Crime Reporting (UCR) Program, collects and publishes information about hate crime incidents that have been investigated and voluntarily reported by more than 17,000 city, county, tribal, state, and federal law enforcement agencies across the nation. The Act, with its subsequent amendments, requires data be collected and published "about crimes that manifest evidence of prejudice based on race, religion, disability, sexual orientation, or ethnicity" and must not include "any information that may reveal the identity of an individual victim of a crime." The UCR Program complies with the OMB standards for federal statistics and administrative reporting with regard to Race and Ethnicity. As such, the FBI uses five categories for race (White, Black, American Indian/Alaskan Native, Asian/Pacific Islander, and Multiple Races) and two categories for ethnicity (Hispanic and Other Ethnicity/National Origin). The Anti-Arab category was originally included on the draft Hate Crime reporting form developed when collection of hate crime data began in 1990. After its review of the draft form, OMB disapproved the inclusion on the form of the Anti-Arab category pursuant to its approved information collection guidelines. CJIS discussed the possible inclusion of the Anti-Arab category with OMB again in approximately 2000, and in 2001. During this time span, OMB advised the previous information collection guidelines barring its inclusion remained in effect.

**76. Would you also be willing to provide space for reporting more specific data on attacks against transgender individuals? Would you be willing to include information on gender-based crimes which is now collected by many states? If you are unwilling or unable to provide detailed statistics, can you please provide a detailed response explaining why you object to the inclusion of such statistics?**

**Response:**

The Act does not authorize the collection of data about crimes motivated by a gender bias. Consequently, the UCR Program does not collect data about crimes motivated by gender bias.

**77. In light of the increase in youth violence associated with gang activity across the country, I'm concerned that the FBI statistics do not contain specific information on the**



**nature and extent of juvenile involvement in hate violence - either as offenders or victims. Please provide this information.**

**Response:**

The Act does not authorize the collection of data about the extent of juvenile involvement in hate violence. Consequently, UCR Program does not collect information about juvenile involvement in hate violence.

**78. You also testified that a number of hate crimes have also been prosecuted at the State and local level. Can you confirm the number of federal hate crimes prosecutions in 2004, along with details relating to each case that you are including in the statistics?**

**Response:**

The federal investigations that resulted in hate crimes prosecutions in 2004 were as follows:

Racial Discrimination involving force and/or violence:

11 Federal indictments and informations and eight convictions  
7 local indictments/informations and 28 convictions

Racial Discrimination with no force or violence:

2 federal convictions  
3 local indictments/informations and two convictions

Religious Discrimination involving force and/or violence:

1 federal indictment and conviction  
5 local convictions

Religious Discrimination with no force or violence:

1 federal indictment

Housing Discrimination:

6 federal indictments/informations and 8 convictions  
6 local convictions

Arab/Muslim/Sikh

During FY 2004, the FBI opened 77 Backlash Hate crime cases against Arab/Muslim/Sikh victims, resulting in 8 subjects being prosecuted federally and 13 subjects being charged locally.

### III. Use of Confidential Informants:

**79. As you know, a major scandal in the Boston FBI office led to important changes in FBI handling of confidential informants. Unchecked and unaccountable FBI agents in Boston failed to follow the Attorney General's Guidelines in handling such informants. These problems were not unique to Boston. A recent case in New York demonstrated that an FBI confidential informant, Greg Scarpa, was involved in several murders, yet the FBI did nothing. In fact, it was only last year that these murders were prosecuted – the District Attorney obtained the information from Congress, thirteen years after the FBI knew what had happened. In response to a question from Senator Cornyn, you also mentioned two other cases: 1) Fort Worth, Texas; and 2) the Leung Case in Los Angeles.**

**Can you please provide more detail on these three instances and describe whether the Attorney General Guidelines on confidential informants were followed in each of these cases? If not, can you please describe with specificity what steps were taken after the fact to address any failure to follow the guidelines? How have the protocols been changed? What new steps are taking place during FBI training to address these concerns?**

#### **Response:**

The cases referenced above include the Leung Case in Los Angeles and the Scarpa case in New York. We believe the statement concerning a case in Fort Worth, Texas, was made by Senator Cornyn, rather than Director Mueller, and involves another law enforcement agency. The FBI would be happy to discuss with the Senator the case he was referencing.

The Leung case involved former FBI SSA James J. Smith, who became involved in an improper relationship with one of his informants. On one occasion, when Smith stepped out of eyesight, his informant, Katrina Leung, rifled through his belongings. This incident raised issues regarding the handling of human sources and contributed to the FBI's efforts to implement a comprehensive human source validation process to better detect the mishandling of sources.

The second case involved FBI informant Gregory Scarpa, Sr. and his FBI handler, retired SA R. Lindley DeVecchio. Scarpa testified in a number of major prosecutions against New York criminal organizations. It is alleged, however, that DeVecchio reciprocated by passing to Scarpa unauthorized information. This matter is currently before the court and a determination of DeVecchio's guilt or innocence has not yet been made.

While many of the FBI's confidential human sources have criminal histories or associations with known criminals, the information provided by these individuals is our most effective law enforcement tool. Since these incidents, the FBI has

undertaken several measures to minimize the inherent risks in using these sources. Among other things, the FBI has: provided to SAs at all levels training on source administration, operation, AG Guidelines, and internal FBI policies; required every division to assign a Human Source Coordinator to its FIG to monitor source files across all programs; mandated ongoing dialogue between FBI field offices and United States Attorneys' Offices to ensure SAs comply with legal requirements; and increased inspections of the Confidential Human Source Program Bureau-wide.

The Confidential Human Source Re-engineering Project is being designed to standardize policies and processes associated with managing and validating confidential human sources and to further improve compliance with AG Guidelines. We also anticipate that the IT systems we are developing to automate the handling of the administrative aspects of sources will significantly reduce, if not eliminate, compliance errors related to AG Guidelines. While no law enforcement agency can guarantee that its agents and sources will not engage in inappropriate conduct, misconduct by SAs operating sources does, fortunately, occur infrequently in the FBI. Violations of AG Guidelines and internal FBI policies are referred to the FBI's Inspection Division and OPR for investigation and adjudication.

**80. As I mentioned at the hearing, last September, Inspector General Glen Fine reported that the FBI was not in compliance with the Attorney General's Guidelines in 87% of the FBI files examined. In nearly half of all the cases examined, the FBI did not comply with its obligation to notify state and local law enforcement about criminal activity by its confidential informants. Please describe, in detail what steps you have taken since the release of the Inspector General's report to ensure that past misuse of confidential informants will not happen again. What safeguards are in place to prevent abuses from occurring?**

**Response:**

Although the OIG found the FBI 42% noncompliant with AG Guidelines regarding unauthorized activity by human sources, it is important to note that the OIG's finding concerned the FBI's obligation to notify either a United States Attorney or the head of a DOJ litigating component of criminal activity by its confidential informants (there is no requirement that the FBI notify state and local law enforcement). Recommendation 3 in the OIG report stated that the Bureau should "institute procedures to determine whether state or local prosecuting offices have filed charges against Confidential Informants who engage in unauthorized illegal activity to determine whether notification must be provided to the US Attorney's Office in accordance with Section IV.B.1.a of the Confidential Informant Guidelines." The FBI concurs that such procedures are desirable and

will explore how to best accomplish this goal, recognizing that a field office's ability to be informed of such matters may vary widely from jurisdiction to jurisdiction and recognizing, as well, that any such policy must be consistent with operational security and the protection of the source's identity. The current AG Guidelines and FBI policy require an SAC (or the equivalent) to notify an appropriate chief federal prosecutor immediately regarding a source's unauthorized illegal activity.

Determining whether a state or local prosecutor has filed charges against a source is the responsibility of the SA handling the source. Agents conduct periodic criminal record checks, maintain contact with their sources, and conduct ongoing background investigations of their sources to determine whether they have engaged in unauthorized illegal activity.

To enhance compliance with AG Guidelines, the FBI's DI has, in coordination with DOJ, initiated a comprehensive review and revision of our HUMINT program. During the past 2 years, the FBI has been developing new policies regarding the utilization of confidential human sources through our Confidential Human Source Re-engineering Project. The DI and DOJ are collaborating to simplify and standardize administrative procedures, clarify compliance requirements, and improve compliance with AG Guidelines. This re-engineering project will include the upcoming Confidential Human Source Validation Standards Manual and the subsequent implementation of a revamped validation process that will apply to all confidential human sources. SSAs, the FIGs, FBIHQ, and DOJ will all have roles in measuring the value of a source's operation as well as managing the risks associated with using a human source. Redundancy of review will be an intentional part of the validation process, serving as a check and balance on human source activities, including authorized and any possible unauthorized criminal activities. The EAD of the NSB has approved a draft of the Validation Manual, and the FBI is moving toward implementation throughout the FBI.

**81. What measures are you implementing as a result of the Inspector General's report to improve information-sharing with state and local law enforcement?**

**Response:**

The referenced report included a recommendation that the FBI institute procedures to determine whether state or local prosecuting offices have filed charges against confidential informants who engage in unauthorized illegal activity to determine whether notification must be provided to the U.S. Attorney's Office in accordance with the Confidential Informant Guidelines. The FBI concurred with the OIG's recommendation, noting the need to explore how best to

accomplish this goal while recognizing that a field office's ability to be informed of such matters may vary widely from jurisdiction to jurisdiction. In addition, new procedures must be consistent with operational security and the protection of source identity. These efforts are included in the ongoing comprehensive FBI/DOJ project to review and revise our Confidential Human Source program. The goals of that project are to develop new policies and processes for the utilization of confidential human sources that will simplify and standardize administrative procedures, clarify compliance requirements, and improve compliance with AG Guidelines. The FBI is also actively participating in the interagency effort to establish a terrorism ISE under the Presidential guidelines issued on 12/16/05.

### **Questions Posed by Senator Feinstein**

**82. As you offered at the hearing, please provide:**

**a. A description of how many of the 2,072 FISA warrants that the FBI obtained last year were “emergency” applications, as opposed to non-emergency applications.**

**Response:**

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

**b. The average amount of time the FBI needs to file and get a FISA warrant in each of these categories.**

**Response:**

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

**83. Do you ask people you appoint to top FBI counterterrorism and counterintelligence posts to commit in advance to stay there for an agreed-upon period of time? If not, why not?**

**Response:**

Appointment to senior FBI positions are typically made following a conversation of commitment within the context of the work program plans and the personal circumstances of the individual.

**84. At the hearing, I asked you about Inspector General Fine's report and its strong language relating to port security risks. You spoke of your plan to develop a new memorandum of understanding (MOU) with the Coast Guard to replace the draft MOU under which you have been operating for several years. I appreciate your stated concern "that we reach a more formalized understanding quickly." Can you please provide me a target date by which you expect to conclude this formalized understanding? And can you send me a copy of the FBI/Customs MOU once it is completed?**

**Response:**

The interim MOTR Plan, which was approved by the President in October 2005, is currently being revised and we anticipate that the final plan will be approved by the President by late 2006. This final MOTR Plan will recommend protocols for each agency and will provide guidance for interagency coordination in response to maritime threats and incidents. After the final MOTR Plan is adopted, the FBI and USCG will address the need for an MOU, if any. The protocols established by the interim MOTR Plan and the pending final MOTR Plan have been used to guide responses to actual maritime incidents over the last several months, and the degree of interagency coordination and the speed with which joint decisions have been reached have been testaments to the effectiveness of these plans.

**FBI Transition to a Domestic Intelligence Agency**

**85. As you are aware, depositions held last Summer reveal that top FBI counterterrorism and counterintelligence officials may have had limited experience in these fields beyond the on-the-job experience they obtained since 9/11. For example, the FBI's top counterterrorism and counterintelligence official, Gary M. Bald, was reportedly unable at his deposition to explain the difference between Sunni and Shia, and suggested that top FBI counterterrorism and counterintelligence officials don't necessarily even need such subject matter experience. In your view, how important is it that your top counterterrorism and counterintelligence officials understand the substance of Islam and Muslim cultures?**

**Response:**

It is important that all investigators understand the dynamics that shape the terrorist threat facing our country. The FBI has made it a priority to ensure that our work force understands the bases of violent Islamic extremist ideologies, and has placed particular emphasis on understanding Muslim culture and the Islamic religion. This is evidenced by the counterterrorism and cultural training made available to our employees. This training teaches us to interact better with Muslim communities and to build the trust critical to effective community policing. Within the counterterrorism program, the provision to our counterterrorism workforce of the correct tools and relevant knowledge is one of

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

Since 9/11, the FBI's counterterrorism program has grown quickly and is the FBI's top investigative priority. This rapid growth has been fueled by a reallocation of our best investigators, managers, and leaders to the counterterrorism mission. We have also refocused our recruiting and hiring to attract individuals with skills critical to our counterterrorism and intelligence missions. These new recruits have included hundreds of IAs, translators, and SAs.

**86. John Gannon's written testimony describes the pre-9/11 world as one in which "[t]he terrorists knew more about our world, and how to train and operate in it, than we did about theirs – the classic recipe for an intelligence failure." Do we now know more about the terrorists' world than they do about ours? If not, is there a target date by which do you expect this goal to be accomplished?**

**Response:**

The response to this inquiry is provided separately.

**87. Please identify the number of linguists/translators that the FBI has hired in the last year – and in particular, how many of these new hires (quantified by language type) are fluent and/or proficient in the priority strategic foreign languages such as Arabic, Farsi, Chinese, etc.**

**Response:**

The response to this inquiry is provided separately.

**88. As one FBI official told the press, "If we become a terrific intelligence agency, we're one of 14 others," but "if we're the FBI, we're like none other." How does the FBI overcome this institutional barrier to elevating the importance of its domestic intelligence mission?**

**Response:**

In any organization, there are those who will resist change and seek to maintain the status quo. Since 9/11/01, FBI employees have been faced with tremendous and continuing changes. These changes are being made quickly, but there are limits to how quickly such change can be made without adverse consequences, particularly while our employees continue to accomplish the FBI's important substantive work.

To achieve the integration of investigative and intelligence operations, the FBI established the DI to manage all FBI intelligence activities and resources. The DI leverages the core strengths of the law enforcement culture, with particular attention to the pedigree of sources and fact-based analysis, while ensuring no walls exist between collectors, analysts, and those who must act upon intelligence information.

The DI consists of a dedicated headquarters staff element and embedded elements in FBIHQ and field divisions. To oversee field intelligence operations, the FBI established FIGs in each of the 56 field offices. The FIGs are composed of SAs, IAs, and language analysts, and often include officers and analysts from other intelligence and law enforcement agencies. FIGs are central to the integration of the intelligence cycle (the six-step process of developing unrefined data into polished intelligence for the use of policymakers) into field operations.

To further develop our intelligence capabilities, the FBI has consolidated its national security investigative and intelligence missions under the NSB. As the next step in the FBI's evolution, the NSB combines the missions, capabilities, and resources of the counterterrorism, counterintelligence, and intelligence elements of the FBI. Building on the success of the DI, the NSB enhances the FBI's ability to meet current and emerging national security and criminal threats by integrating the FBI's intelligence mission more fully into the broader missions of the FBI and the IC. The NSB has full authority to manage all FBI intelligence activities, from collection to dissemination, and is vested with the authority to assign, prioritize, and reallocate intelligence resources.

Since our inception, the FBI has changed and evolved in response to new threats and expectations, and it was again faced with new challenges following the attacks of 9/11/01. Never before in the FBI's history has such a transformation been undertaken, particularly in such a short time. We have made enormous progress in building an intelligence capability, but further enhancements will take time. The FBI has established and is following a strategic plan for 2004-2009 that stresses the need for continuing change.



FBI executives emphasize these themes at every opportunity they have to communicate with employees, including through speeches, meetings, the FBI intranet, and e-mail messages. Nonetheless, experts in the transformation of organizations have indicated that, in any such transformation, 30% of the employees will support the change from the outset, 30% must be persuaded, and 30% will resist the change for a variety of reasons. The FBI must and will continue to win over those who are still on the fence and ensure that our employees recognize that the world has changed and that we must change with it.

#### FBI Terrorism Prosecutions

**89. According to the Transactional Records Access Clearinghouse (TRAC), the FBI referred about 6,400 people for prosecution under anti-terrorism statutes in the first two years after the September 11 attacks. The Justice Department reported that it had obtained 184 terrorism convictions from the 6,400 cases developed mainly by the FBI. But according to TRAC, 171 of those convictions resulted either in no jail time or in sentences of less than one year – leaving only 13 with sentences of a year or more. Are these figures accurate? If not, how are they inaccurate?**

#### Response:

DOJ's Executive Office for United States Attorneys (EOUSA) advises that the United States Attorneys' case management system shows that during Fiscal Years 2002 and 2003, the FBI referred 3,967 criminal matters against 4,779 suspects to the United States Attorneys. (It should be noted that referrals are made for investigation and are not necessarily recommendations for prosecution at the time the referral is made.) These criminal matters were classified by the United States Attorneys in the international terrorism, domestic terrorism, terrorism-related hoaxes, terrorist financing, and various anti-terrorism case categories. EOUSA is not certain how TRAC derived its number of FBI referrals.

The United States Attorneys' case management system also shows that during Fiscal Years 2002 and 2003, the United States Attorneys concluded the prosecution of 411 FBI-referred terrorism or anti-terrorism defendants. Of these defendants, 352, or 86 percent, were convicted. Of the 352 convicted defendants, 207 were sentenced to prison. Of the defendants sentenced to prison, 88 were sentenced to 1-12 months in prison, 48 were sentenced to 13-24 months in prison, 12 were sentenced to 25-36 months in prison, 29 were sentenced to 37-60 months in prison, 26 were sentenced to 61+ months in prison, and 4 were sentenced to life in prison.

The sentence imposed in a given case is not necessarily an accurate measure of the significance of the case in our counterterrorism efforts. Our strategy emphasizes

prevention, and a prevention strategy requires us to engage the enemy earlier than if we waited for them to act first. We cannot wait for terrorists to strike to begin investigations and make arrests. We must use the full range of criminal offenses at our disposal to charge offenses that fit the facts before those who would do us harm put their plans into action. Thus we use non-terrorism offenses, such as false statement charges, immigration fraud, and use of fraudulent travel documents, in terrorism cases. These offenses carry lesser penalties than offenses associated with completed terrorist acts, yet the appropriate charging of such offenses is so important to our disruption of terrorist plans that the Department has urged prosecutors to undertake initiatives to increase their use of these statutes. Defendants have also been sentenced to time served and immediately deported resulting in what would appear to be short sentences, but the result is that the defendant is removed from the United States.

In January 2003, the Government Accountability Office (GAO) issued a report entitled *JUSTICE DEPARTMENT: Better Management Oversight and Internal Controls Needed to Ensure Accuracy of Terrorism-Related Statistics*. This report summarized GAO's audit of Justice Department terrorism statistics. In the report, GAO stated that a review of EOUSA's Fiscal Year 2002 statistics on defendants convicted in terrorism cases showed that 132 of 288 cases were misclassified. Although GAO stated in the report that 127 of the 132 misclassified cases fell under newly established anti-terrorism program categories, GAO made recommendations for improving data integrity nonetheless. GAO recommended that in order to improve the accuracy and reliability of terrorism-related conviction statistics in Department of Justice's annual performance reports, a formal system should be implemented to oversee and validate the accuracy of case classification and conviction data entered in the United States Attorneys' case management system.

In August 2002, EOUSA issued new program category codes so the United States Attorneys could more accurately identify their terrorism and anti-terrorism cases. Prior to that time, the three terrorism-related codes were International Terrorism, Domestic Terrorism, and Terrorism-Related Hoaxes. New codes were added for Terrorism-Related Financing and for various Anti-Terrorism categories (such as Identity Theft, Immigration, and Violent Crime) to capture activity intended to prevent or disrupt potential or actual terrorist threats where the offense conduct would not fall within one of the already-existing codes. With a few exceptions, all the FY 2002 convictions that GAO identifies as "misclassified" were ultimately determined to be convictions properly classified in one of the Anti-Terrorism categories. With the transition to a new coding scheme so close to the end of the fiscal year, United States Attorneys' Offices (USAOs) either did not have time to, or did not fully understand the need to, reclassify already closed cases.

EOUSA complied with GAO's recommendation through the completion of formal Terrorism Case Data Quality Reviews by each USAO. All USAOs were required to update their information in the case management system, if necessary, and notify EOUSA that they had completed their review and update process by the deadlines set. EOUSA and the USAOs continue to monitor the accuracy of terrorism and anti-terrorism matter and case information in the case management system as part of the review and certification process that is conducted in each USAO in April and October of each year.

United States Attorneys code terrorism matters as International Terrorism Incidents Which Impact on the U.S., Domestic Terrorism, Terrorism Related Hoaxes, and Terrorist Financing. In addition, other matters are classified as Anti-Terrorism in the following categories: Anti-Terrorism/Environmental, Anti-Terrorism/Identity Theft, Anti-Terrorism/Immigration, Anti-Terrorism/OCDETF Drugs, Anti-Terrorism/Non-OCDETF Drugs, Anti-Terrorism/Violent Crimes, and Anti-Terrorism/All Others. The Criminal Division maintains its own statistics on terrorism cases which are very different from those maintained by the USAOs.

**90. At an announcement with Attorney General Gonzales last Summer, President Bush stated that “federal terrorism investigations have resulted in charges against more than 400 suspects, and more than half of those charged have been convicted.” But the Washington Post later reported that these numbers were “misleading at best” and that only “39 people – not 200, as officials have implied – were convicted of crimes related to terrorism or national security.” And a January 2003 GAO report stated that the Justice Department “does not have sufficient management oversight and internal control standards to ensure the accuracy and reliability of its terrorism-related statistics.” In your view, how many federal criminal cases that truly involve terrorism or national security, and that have yielded convictions and prison sentences in excess of one year, have been brought by the FBI since September 11, 2001?**

**Response:**

DOJ's EOUSA advises that the numbers quoted by the President are based on statistics that represent defendants charged in terrorism or terrorism-related criminal cases with an international nexus that are tracked by DOJ's Criminal Division. The Criminal Division maintains its own statistics on terrorism cases which are based on different criteria from those maintained by the USAOs.

Cases tracked by the Criminal Division arose from investigations primarily conducted after 9/11/01, which initially appeared to have an international connection, including certain investigations conducted by the FBI's Joint Terrorism Task Forces (JTTFs) and other cases involving individuals associated with international terrorists or Foreign Terrorist Organizations. The Criminal

Division began tracking these cases during the nationwide PENTTBOM investigation of the 9/11/01 attacks; indeed, the initial cases tracked involved individuals identified and detained in the course of that investigation and subsequently charged with a criminal offense, though often not a key terrorism offense. Additional individuals have been added who, at the time of charging, appeared to have a connection to terrorism, even if they were not charged with a terrorism offense.

The Criminal Division also keeps track of all material support, terrorism financing and related cases. The material support statutes are the cornerstone of our prosecution efforts. The Criminal Division tracks a subset of cases that are reported through the case management system of the USAOs. For purposes of the USAO system, "Terrorism" investigations and cases include International Terrorism, Domestic Terrorism, Terrorist Financing, and Terrorism-Related Hoaxes; and "Anti-Terrorism" investigations and cases include Immigration, Identity Theft, OCDETF, Environmental, and Violent Crime - all in cases where the defendant is reasonably linked to terrorist activity or where the case results from activity intended to prevent or disrupt potential or actual terrorist threats.

Applicable criteria used by the Criminal Division as to which cases it tracks includes: whether a terrorism statute is charged, whether it derives from a JTTF investigation, whether the conduct involves a terrorist act or terrorist activity, whether the individual charged is associated with terrorists, a designated foreign terrorist organization, another terrorist group, or a Specially Designated Terrorist.

Proactive prosecution of terrorism-related targets on less serious charges is often an effective method of deterring and disrupting potential terrorist planning and support activities. Moreover, pleas to these less serious charges often result in defendants who cooperate and provide information to the Government - information that can lead to the detection of other terrorism-related activity.

Based on statistics maintained by the Criminal Division of terrorism and terrorism-related criminal cases with an international nexus, as of 6/22/06: 441 defendants have been charged,<sup>1</sup> resulting in 261 convictions in 45 jurisdictions,<sup>2</sup> including 218 guilty pleas, 43 convictions after trial, 150 cases remain pending,<sup>3</sup>

---

<sup>1</sup> This includes three defendants, each of whom was charged in two separate indictments; each indictment is counted as a separate case, so these three defendants are counted twice.

<sup>2</sup> Two of the defendants are counted twice here, reflecting that each was charged and convicted in two separate indictments. A third defendant has been convicted in one case and has another case pending against him.

<sup>3</sup> Pending cases include those in which the defendant is in pre-trial detention awaiting trial, or the defendant is a fugitive or is awaiting extradition; this also includes a number of cases under seal.

29 cases which have not resulted in conviction and are no longer pending,<sup>4</sup> and 1 case which resulted in mistrial and is awaiting re-trial on the same charges.

The Criminal Division does not keep comprehensive sentencing data on all terrorism cases. The sentence imposed in a given case is not necessarily an accurate measure of the significance of the case in our counterterrorism efforts. Our strategy emphasizes prevention, and a prevention strategy requires us to engage the enemy earlier than if we waited for them to act first. Again, we cannot wait for terrorists to strike to begin investigations and make arrests. We must use the full range of criminal offenses at our disposal to charge offenses that fit the facts before those who would do us harm put their plans into action. Thus we use non-terrorism offenses, such as false statement charges, immigration fraud, and use of fraudulent travel documents, in terrorism cases. These offenses carry lesser penalties than offenses associated with completed terrorist acts, yet the appropriate charging of such offenses is so important to our disruption of terrorist plans that the Department has urged prosecutors to undertake initiatives to increase their use of these statutes. Defendants have also been sentenced to time served and immediately deported resulting in what would appear to be short sentences, but the result is that the defendant is removed from the United States.

#### Effect of FBI Transition on its Traditional Law Enforcement

**91. The FBI's primary focus after 9/11 must be on stopping terrorism, and the FBI has formally reallocated 1,143 agents to terrorism-related programs. But according to Inspector General Fine, the FBI in FY2004 was utilizing almost 2,200 fewer field agents to investigate its more traditional crime matters than in FY2000. During that same time, the FBI opened 28,331 fewer criminal cases (a 45% reduction), and reduced the number of matters referred to U.S. Attorneys for prosecution by 6,151 (27%). Inspector General Fine noted that, for some specific crime areas, such as financial institution fraud, there is now "an investigative gap." We are also hearing of how FBI surveillance squads are increasingly being used for counterterrorism instead of traditional law enforcement surveillance, in areas such as organized crime. Is this drop-off likely to be the FBI's new norm? Would additional resources substantially increase the number of FBI arrests and referrals for prosecution in these traditional areas?**

---

<sup>4</sup>Among the 29 charged cases that did not result in a criminal conviction and are no longer pending, 4 defendants were transferred to Customs and Immigration Enforcement (ICE) custody for removal or deportation; 8 were indicted on or have pled guilty to other charges; 8 were dismissed on the government's motion for evidentiary or other reasons; 1 died while still a fugitive; and 1 had his charges dropped after he was designated an enemy combatant by the President.

**Response:**

The FBI has a broad mission with varied and competing challenges. In order to discipline the FBI's approach to these challenges, we have considered the interaction of three factors: (1) the significance of the threat to the security of the United States as expressed by the President in National Security Presidential Decision Directive 26; (2) the priority the American public places on various threats; and (3) the degree to which addressing the threat falls most exclusively within the FBI's jurisdiction. Weighing and evaluating these factors resulted in the FBI's top ten priorities. The first eight are listed in order of priority. The final points (collaborative partnerships and technology improvement) are key enabling functions that are of such importance they merit inclusion. The priorities are:

1. Protect the United States from terrorist attack;
2. Protect the United States against foreign intelligence operations and espionage;
3. Protect the United States against cyber-based attacks and high-technology crimes;
4. Combat public corruption at all levels;
5. Protect civil rights;
6. Combat transnational and national criminal organizations and enterprises;
7. Combat major white collar crime;
8. Combat significant violent crime;
9. Support federal, state, local, and international partners;
10. Upgrade technology to successfully perform the FBI's mission.

The FBI staffs and works high priority matters before lower ones. Support processes, including hiring and technological competence, serve our highest priorities first and resources are allocated and applied to each FBI mission according to its priority. The counterterrorism effort has received significant financial and human capital resources since 9/11/01; those resources have been used to build our capabilities and to re-engineer the FBI into a proactive, intelligence-gathering organization committed to protecting the United States from future terrorist attacks.

While our national security efforts remain our top priority, the FBI continues to fulfill our crime-fighting responsibilities as well. As the Committee was informed by the Director in his opening statement, public corruption is the top criminal priority for the FBI. Over the last two years, the FBI's investigations have led to the conviction of over 1,000 government employees involved in corrupt activities, including 177 Federal officials, 158 state officials, 360 local officials, and more than 365 police officers. Among its other priorities, the FBI also continues to focus on implementing the National Gang Strategy, along with ATF. This strategy is designed to identify the prolific and violent gangs in the United States

and to aggressively investigate, disrupt, and dismantle their criminal enterprises through prosecution under appropriate laws.

As always, the FBI will work with DOJ, OMB, and the Congress to determine whether to seek additional resources in support of the FBI's numerous responsibilities.

**92. I understand that the President's budget from OMB for FY2007 recommends only one new agent to be added to the overall staffing total for the entire FBI, nationwide. Do you believe that the FBI, on this proposed budget, can continue to perform its expanding responsibilities in the areas of counterterrorism and counterintelligence, while still adequately maintaining its traditional law enforcement capabilities?**

**Response:**

For the FBI to perform its law enforcement and national security responsibilities it requires both qualified personnel to fill agent, analyst, and other support positions, and infrastructure, including IT systems and SCIFs. In each year since FY 2002, the FBI has received funding from Congress to bolster its infrastructure and to hire thousands of new positions (1,681 SA and 4,347 support positions from FY 2003 through FY 2006). However, even with infrastructure successes like IDW and other IT systems, the FBI's infrastructure has not kept pace. The FY 2007 budget was formulated with this in mind and it focuses on providing the infrastructure and tools necessary for agents and analysts to do their jobs, from \$100 million to move the Sentinel project forward to \$64 million to build new SCIFs across the country. While additional personnel may be necessary in the future, the FY 2007 budget provides the infrastructure resources necessary for current FBI personnel to be more effective and efficient in their jobs.

**93. I understand that thought has been given to using the "intelligence" model more broadly within the FBI, allowing cases to be opened and investigations begun without the predicate of suspicion of a crime. While this may be a necessary step to prevent major crimes such as terrorism, there are profound implications for the nation's leading law enforcement body to be investigating Americans who are not, at the time, in violation of the law. What is your view on the necessity to open preliminary investigations to identify the potential intent to commit crimes, and the ways in which such investigations can be safeguarded against intruding on civil liberties?**

**Response:**

The FBI does not open either preliminary or full investigations without predication. To fulfill its mission, though, the FBI is responsible for identifying threats that are not readily observable. To do this, we have required our field

offices to learn about their territories using domain management, which gives field offices a top-down understanding of their territories that complements the intelligence derived from cases. The field offices use these assessments to identify and prioritize threats and to make better-informed decisions about where to focus resources to most effectively disrupt those threats. This learning process is nonintrusive. FBI offices learn from confidential human sources, local officials, concerned citizens, and businesses. If a field office learns of a potential national security threat (for example, if a source indicates the presence of a terrorist cell), that field office may open a threat assessment to determine the validity of the threat. Threat assessments are conducted using nonintrusive techniques that are generally different from domain management only in the sense that the assessment is focused on the possibility of an identified threat. The threat assessment is designed precisely to gain information about a focused issue without intruding on civil liberties. If a threat assessment validates a potential threat, then a predicated investigation may be opened.

We are aware that we cannot be effective in either our criminal mission or our intelligence mission without the support of the public. If the FBI were to investigate Americans without predication, we would quickly lose the confidence of the public, which is a significant source of the information we need to accomplish our missions.

Information Technology Concerns: “Virtual Case File” and “Sentinel” Systems

**94. According to the Inspector General’s March 2006 Audit Report 06-14, the FBI had not disclosed its specific cost estimates for Sentinel because the contract had not yet been awarded, but “[a]ccording to the FBI, a more precise cost estimate will be available once the FBI awards the Sentinel contract. . . .” Now that the Sentinel contract has been awarded, what are the FBI’s specific cost estimates for the Sentinel project?**

**Response:**

As indicated in response to Question 13, above, the total value of the contract with Lockheed Martin is \$305 million over 6 years, including both development and O&M. The FBI estimates that the total cost of the Sentinel program, including program management, systems development, O&M, and IV&V, will be \$425 million over 6 years.

**95. According to that same audit, the Sentinel acquisition plan identified seven risk factors, including concerns about scope creep and that initial program costs may be underestimated. The audit also noted that the Program Management Office has not yet been fully staffed, that “it is critical for the FBI to fully staff the PMO office as soon as possible” and “for the PMO to have stable leadership,” and that “[w]ithout a fully staffed,**



**stable and capable PMO managing the project on a daily basis, Sentinel is at risk.” Both this IG audit and the GAO’s Linda Calbom identify weaknesses in FBI cost control, and warn that the FBI will be “highly exposed to the same types of negative outcomes that they experience with Trilogy” unless these weaknesses are corrected. Please explain how the FBI has addressed or is addressing these concerns.**

**Response:**

Please see the responses to subparts a and d of Question 55, above, regarding cost control issues. The FBI has strengthened its internal controls and contract oversight in several ways in order to avoid a repetition of prior problems.

- First, the Sentinel contract has clear reporting requirements and defined deliverables in each contract phase (each of the four phases delivers capability to the end-user), and the contract can be terminated at any point should these results be unsatisfactory.
- Second, those responsible for contract management have clearly defined roles and responsibilities, and the management function is structured so as to ensure that accountable personnel review all documentation and expenses. The FBI has implemented measures to verify the FBI's receipt of deliverables and to validate their costs when invoiced. This contract management function will be supplemented by internal financial management audits.
- Third, an IV&V specialist will report directly to the FBI's CIO and will independently assess the efficiency and progress of the PMO and the work of the Sentinel contractors.
- Fourth, to eliminate the likelihood of "scope creep," any significant requirement changes must first be approved by the FBI's Deputy Director.

Please see the response to Question 62, above, regarding the PMO's staffing.

**96. According to the Inspector General’s March 2006 audit, the FBI plans to reprogram funds to pay for the first two phases of Sentinel. Congress approved the first phase (\$97 million in reprogramming of FY2005 funds) in November, with more than \$27 million of this reprogramming coming from Counterterrorism and intelligence-related activities. While the audit noted that the FBI’s divisions and offices had reported an ability to absorb this first diversion of funds to Sentinel, they also reported that “a second reprogramming of the same magnitude would damage their ability to fulfill their mission.” The auditors also noted concern “that diverting substantial funds from such mission-critical areas could begin eroding the FBI’s operational effectiveness.” Does the FBI plan to seek a second**

**phase of reprogramming of funds to pay for Sentinel? Given that we are already hearing anecdotal stories about FBI field offices placing monthly caps on agents' gasoline expenditures, how can it do this without compromising its operational effectiveness?**

**Response:**

Please see the response to Question 61, above.

**97. The Inspector General also noted concerns “that the FBI has not yet adequately examined or discussed Sentinel’s ability to connect with external systems in other [DOJ] components, the [DHS], and other intelligence community agencies. If such connectivity is not built into Sentinel’s design, other agencies could be forced into costly and time-consuming modifications to their systems to allow information sharing with the Sentinel system.” For example, the DEA’s Deputy CIO already reported in that same audit how its new case management system “is not compatible with Sentinel as currently designed.” Once Sentinel is implemented, do you anticipate that Congress will face substantial additional costs in the future based on a need to implement interoperability between the various intelligence and law enforcement agencies’ systems?**

**Response:**

Please see the response to Question 63, above.

**98. On a practical level, once Sentinel is fully implemented, and a local cop makes a traffic stop of the next Mohammed Atta (i.e., a terrorist whose name and identifiers are on the FBI’s terrorist watchlist), will the local cop or a local police station be able to perform a Google-like electronic search to find that out? If not, why not, and what more will it take to get to that place?**

**Response:**

The FBI intends for Sentinel to interface with the N-DEx system. With this interface, local law enforcement with access to N-DEx will be able to perform searches on Sentinel data exchanged with N-DEx.

**FBI Activities at Pomona College, California**

**99. I have been contacted by several constituents concerning an FBI informational interview of Professor Tinker Salas, a professor of Latin American history at Pomona College in California. Can you please provide me with a description of the circumstances surrounding this interview, and whether you believe the agents’ actions were appropriate?**

**Response:**

Although the FBI is not at liberty to disclose information pertaining to FBI investigations, the interview of Professor Tinker-Salas was conducted for reasons unrelated to his position as an academic professor. As a general matter, the FBI conducts interviews to gather information that is pertinent to our responsibilities to protect the national security. Overt interviews, in which FBI agents identify themselves and the interviewee is free to decline to speak, are frequently used to gather basic information from people who wish to cooperate with the FBI. In this case, it is worth noting that Dr. Tinker-Salas is a noted historian with a deep understanding of Venezuelan politics, culture and history. The FBI did not intend to, nor did it, violate Dr. Tinker-Salas' First Amendment rights.

**NSA Surveillance Program**

**100. Has the FBI received, via information sharing, information from the NSA's domestic wiretapping conducted outside of FISA? If so, is a system in place, either at the FBI or NSA, to identify when information was obtained without a FISA warrant? Does the FBI have any minimization procedures in place for information shared with the FBI by the NSA that has been obtained outside of existing FISA procedures? If so, please describe those procedures and the date when they were enacted.**

**Response:**

It is not appropriate to discuss the operational details of the Terrorist Surveillance Program in this context. The full Senate Select Committee on Intelligence has been fully briefed on the operational details of the TSP described by the President.

**101. Has the FBI, like the NSA, conducted non-Title III domestic electronic surveillance (hereinafter "domestic wiretapping") without obtaining or seeking a FISA warrant? If not, why has the FBI chosen not to do what the NSA has done? If so, please describe (in a classified submission, if necessary) the nature of the FBI's activities, the date on which such domestic wiretapping without FISA court approval began, and the reason(s) why the FBI determined that FISA warrants were not legally required for these activities.**

**Response:**

All electronic surveillance conducted by the FBI is in accordance with the Constitution and laws of the United States. The FBI conducts domestic electronic surveillance pursuant to Title III and FISA. In addition, the FBI engages in two types of surveillance without court order: consensual monitoring (based on the consent of one party to the conversation) and under circumstances in which there is no reasonable expectation of privacy. The TSP is not a "domestic" surveillance

program. Rather, that program targets for interception only international communications where NSA determines there is probable cause to believe that at least one party to the communication is a member or agent of al-Qa'ida or an affiliated terrorist organization.

**102. In his written testimony, Inspector General Fine noted how the FBI has reported a variety of claims of civil rights and civil liberties violations to the President's Intelligence Oversight Board ("IOB"), including some in FYs 2004 and 2005 relating to "intercepting communications outside the scope of the order from the FISA court," and how "[n]ot all possible violations were attributable solely to FBI conduct." Did the FBI ever submit, to the IOB, concerns about the NSA's (or the FBI's, or any other agency's) activities relating to domestic wiretapping without a FISA warrant? If so, please provide the date and subject matter of such submissions, and please produce all such submissions that the FBI sent to the IOB (in classified form, if necessary).**

**Response:**

The FBI's obligation is to report intelligence activities affecting FBI investigations that violate law, AG Guidelines, or the FBI's internal policies established to protect the rights of United States persons. Because DOJ has opined that the TSP is lawful, there has been no basis for reporting activities related to that Program to the Intelligence Oversight Board.

**Questions Posed by Senator Feingold**

**National Security Letters**

**103. When you appeared before the Judiciary Committee on May 2, 2006, I asked you about the disparity between the number of National Security Letters (NSLs) that were issued in 2005 versus the number of Section 215 business records orders issued in 2005. You agreed that obtaining a Section 215 order requires judicial approval, and that issuing a NSL does not require judicial approval, but said that you would get back to me about why so many more NSLs were issued in 2005. Please provide a response.**

**Response:**

NSLs are available to obtain the records that form the basic building blocks of most investigations (e.g., telephone records and banking records). They are used frequently and in many national security investigations (similar to the role of grand jury subpoenas in criminal investigations). Orders pursuant to Section 215 of the USA PATRIOT Act, on the other hand, are used only if the records cannot be obtained through other means (e.g., through NSL or voluntary production).

The preference toward NSLs is not borne of any desire to avoid judicial review, but rather from a desire to obtain the information needed to pursue a national security investigation in the most efficient way possible under the law. Because NSLs can be issued at the field office level, they are far more efficient than 215 orders, which require court filings.

NSA Wiretapping Program

**104. When did you first learn about the NSA wiretapping program authorized by the President shortly after September 11, which circumvented the FISA court process?**

**Response:**

Director Mueller became aware of NSA's TSP at or near the time the program commenced.

**105. Did you raise any objection to the NSA wiretapping program at the time?**

**Response:**

As I explained at the hearing, I do not believe I should go into internal discussions I may have had with others in the Executive Branch.

**106. Do you have any concern that judges would not permit the information gathered through the use of these wiretaps to be used in criminal prosecutions?**

**Response:**

The purpose of the TSP is to gather intelligence about what al-Qa'ida and affiliated terrorist organizations are planning, particularly in the United States or against United States interests, not to gather evidence for use in criminal proceedings. The FBI has used FISA and Title III as the exclusive means of eavesdropping on individuals within the United States, whether we are attempting to develop evidence for use in criminal proceedings or to gather foreign intelligence.

**107. Has anyone in the Administration, either at the White House or the Justice Department, urged you to use information derived from this wiretapping program in a criminal case?**

**Response:**

The purpose of the TSP is to gather intelligence about what al-Qa'ida and affiliated terrorist organizations are planning, particularly in the United States or against United States interests, not to gather evidence for use in criminal proceedings. No one in the Administration has urged the FBI to use information obtained through the TSP in a criminal case.

**108. Are you aware of any discussions within the Administration about authorizing warrantless physical searches of individuals' homes or offices within the United States?**

**Response:**

Director Mueller recalls no such discussions.

**USA PATRIOT Act**

**109. In March, Chairman Specter introduced legislation (S. 2369) that contained four additional changes to the Patriot Act, beyond what was in the reauthorization package.**

**a. In Chairman Specter's bill, the provision relating to Section 215 would require the government to convince a FISA judge: (1) that the business records pertain to a terrorist or spy; (2) that the records pertain to an individual in contact with or known to a suspected terrorist or spy; or (3) that the records are relevant to the activities of a suspected terrorist or spy. Do you agree this standard is adequate to provide agents with the flexibility they need? If not, please provide specific examples demonstrating why not.**

**Response:**

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

**b. Another provision would add a four-year sunset to recent changes to the National Security Letter statutes. Given that the sunset would allow existing law to govern any ongoing investigations, do you have any objection to that sunset provision?**

**Response:**

The FBI does not favor a sunset provision, since the revisions of the NSL statutes appear to be reasonable and fair both to the FBI, as the issuer of NSLs, and to NSL recipients. If these provisions prove not to work as intended, they can be revised when that conclusion is reached. Even without a sunset provision, these provisions will no doubt be reevaluated periodically to ensure they are operating as intended, and modifications may be made as needed.

**c. Another provision of the bill would make sure that recipients of business records orders under Section 215 of the Patriot Act and recipients of National Security Letters can get meaningful judicial review of the accompanying gag orders. Under the reauthorization package, the recipient would have to prove that any certification by the government that disclosure would harm national security or impair diplomatic relations was made in bad faith. This seems to be a virtually impossible standard to meet. How frequently would you estimate that FBI agents make such certifications in bad faith?**

**Response:**

The bad-faith standard to which this question refers, contained in the USA PATRIOT Improvement and Reauthorization Act of 2005 (hereinafter the "Reauthorization Act"), applies in the very limited context of a petition challenging the nondisclosure provision of a national security letter or a FISA business records order in which there has been a certification by the AG, the DAG, an Assistant AG, or the FBI Director that disclosure of the letter or the business records order may endanger the national security of the United States or interfere with diplomatic relations. We do not expect that any such certifications will be executed in bad faith. We should note, however, that under the statutory scheme contained in the Reauthorization Act, if the government invokes any other reason for nondisclosure (i.e., interference with a criminal, counterterrorism, or counterintelligence investigation or danger to the life or physical safety of any person), even if such a certification is made to that effect by one of the officials enumerated above, or if the certification is made by an official other those enumerated above, then the nondisclosure provision can be set aside if the district court finds there is no reason to believe such damage will occur. Accordingly, the bad-faith standard to which the question refers will be applicable only in a very narrow subset of all cases in which nondisclosure provisions in NSLs or business records orders are challenged. We note that there have only been two such challenges in the history of the NSL statutes (there has been no challenge to a FISA business records order), and none since the USA PATRIOT Act was reauthorized. In one of the two challenges, after the enactment of the Reauthorization Act, the government did not certify that its disclosure would cause harm and the NSL was, in fact, disclosed.

**d. Chairman Specter's bill would require that subjects of delayed notice criminal searches be notified of the search within 7 days, unless a judge grants an extension of that time. The bill would leave in place the ability to get unlimited 90-day extensions. Given that the government can obtain unlimited 90-day extensions, why not create a presumption that a citizen should be notified within 7 days if his or her home has been searched by the government?**

**Response:**

Rule 41(f) of the Federal Rules of Criminal Procedure requires the officer who executes a federal search warrant to leave a copy of the search warrant, together with a receipt for all items seized, at the place that was searched. The statute permitting delayed notice, initially enacted as part of the USA PATRIOT Act, is already an exception to the general rule. Delayed notice searches continue to be unusual and are done only when the government can demonstrate good cause for any notification delay. We believe the law correctly vests in the issuing judge the authority to determine how long that delay should be.

**Terrorist Watch List**

**110. I understand that the Terrorist Screening Center at the FBI has a redress process but works behind the scenes with other agencies to try to rectify any problems that individuals experience as a result of being mistakenly placed on a terrorist watch list or mistakenly identified as someone on the list. Should people who believe they are adversely affected by the Terrorist Screening Center watch list have the right to appeal an adverse consequence that results from it, and to take their appeal to court? How do we balance the right to appeal with the need for secrecy?**

**Response:**

TSC believes an effective redress process is critical to the public's trust in the United States Government's terrorist screening efforts and the protection of individuals' civil liberties. Therefore, it is essential that those who believe they have been adversely affected by these screening efforts have access to a review process through which errors can be identified and corrected.

When the terrorist screening process adversely affects an individual's important rights, benefits, or privileges, the individual has the right to independent review of the basis for the adverse action. For most such circumstances, a review process is already in place and is tailored to the specific context in which an individual may be affected by terrorist screening. The consolidated watchlist is largely used by agencies that have existing authority to screen individuals and take action on the grounds of terrorist connections or other disqualifying factors. Depending on what action an agency takes as a result of the terrorist screening process, the individual may have a right to a formal agency appeal or to judicial review under the Administrative Procedure Act or other applicable law.

As the question recognizes, the challenge is to balance the need for access to information in the context of an appeal with the need to protect sensitive or classified information that, if released, could undermine the effectiveness of the



consolidated watchlist or the Government's other counterterrorism efforts. In most instances, a watchlist "hit" serves only to alert the screening agency that intelligence information exists suggesting a nexus to terrorism. The screening agency can then obtain and review this intelligence and decide what action is appropriate consistent with its legal authority. When an agency takes adverse action based on the intelligence information, that information and the fact that the consolidated watchlist led the agency to examine that information become part of the agency record supporting the adverse action.

Thus far, the courts have balanced the right to appeal an agency's action with the need for secrecy by conducting *ex parte, in camera* review of any sensitive or classified information that formed the basis for agency action. This process has worked well and should serve as the model for judicial review of adverse actions that flow from the terrorist screening process.

#### Previous Letters

**111. Please respond to a letter I sent you on April 24, 2006, asking for information about FBI policy directives apparently issued in 2003 and 2004 to clarify guidelines regarding investigations that involve public demonstrations or protest activities.**

#### Response:

The FBI's response, dated 5/25/06, is provided as Enclosure B.

**112. Please respond to a September 16, 2005, letter that Senator Sununu and I sent to you, asking for follow-up information regarding a GAO report that analyzed the use of data mining technology by the Foreign Terrorist Tracking Task Force.**

#### Response:

The FBI's response, dated 11/25/05, is provided as Enclosure C.

#### Questions Posed by Senator Schumer

**113. The Inspector General reported that the FBI, "as the lead federal agency for preventing and investigating terrorism, has an overarching role in protecting the nation's seaports." (p. 13)**

**a. Do you agree with that assessment?**

**Response:**

Yes. As the lead federal agency for preventing and investigating terrorism, the FBI has a critical role in protecting the American public and all aspects of our nation's infrastructure. Consistent with HSPD 5 (2/28/03), the FBI exercises lead responsibility for criminal investigations of terrorist acts or terrorist threats by individuals or groups inside the United States, or directed at United States citizens or institutions abroad, and for related intelligence collection activities within the United States. The FBI is also aware of the responsibilities assigned to the USCG under the Maritime Transportation Security Act of 2002. The FBI is committed to working with our partners in the USCG and other Federal, state, and local agencies to make the United States, our ports, and our inland waters as secure as possible.

**b. Nonetheless, the OIG review found serious problems in the allocation of FBI resources and interagency coordination to secure our ports. Do you agree with that OIG assessment?**

**c. Do you think those deficiencies are acceptable?**

**Response to subparts b and c:**

The FBI engages in the ongoing review of resource allocation and believes its port security resources are properly allocated. The FBI does and will continue to address any identified deficiencies in our operations or our coordination with others. With the benefit of a national MSP management vehicle at FBIHQ and the full-time and collaborative participation in an MSP by the FBI, NCIS, and USCG, the FBI believes interagency coordination is currently effective and continually improving.

**d. The OIG made 18 recommendations for improving FBI efforts on port security. Do you intend to follow all of them? If not all, why not?**

**e. What steps have been taken to follow these recommendations so far?**

**f. How many remain, wholly or in part, undone?**

**Response to subparts d-f:**

The FBI responded to the OIG report by letter from CTD Assistant Director Willie Hulon to IG Fine dated 3/17/06 (Enclosure A). That letter identifies the steps the FBI has taken and is taking in response to each of the OIG's findings and recommendations. The FBI is preparing a formal reply to the report that

documents these and subsequent steps taken, and this process will be repeated every 90 days until the FBI has completed its response to all report findings and recommendations.

**114. While I appreciate all the improvements you are trying to make so that the Sentinel program does not meet the same fate as the Virtual Case File system, I remain concerned about the possibility of a repeat fiasco. I would like to know who is ultimately responsible for this program, success or failure.**

**a. Specifically, whose job is on the line if this attempt does not work properly?**

**Response:**

The FBI's CIO (Zalmay Azmi) and Program Management Executive (Dean Hall) are responsible for the Sentinel program.

**b. The Inspector General has already identified six “continuing concerns” with the Sentinel project. Do you agree with his assessment?**

**Response:**

The DOJ IG outlined seven recommendations in its final pre-acquisition report on Sentinel. The Sentinel PM concurred with those recommendations and had already been taking steps to improve management efforts.

The Sentinel PMO recently received a follow-up "Analysis and Summary of Actions Necessary to Close the Report" from the IG. In that follow-up request, the IG informed the FBI that all seven recommendations are considered "resolved" and will be considered "closed" when specified conditions are met. The Sentinel PMO has submitted a response outlining the actions already taken or, in the case of responsive actions that cannot be completed in the near term, advising what intermediate actions have been taken and when the PMO expects closure.

**c. How many of these concerns have been addressed?**

**Response:**

As indicated in response to subpart b, above, the IG has informed the FBI that all seven recommendations are considered "resolved" and will be considered "closed" when specified conditions are met.

**d. The IG also points to problems with cost control, though you have apparently developed a tool to track project costs. What exactly is that tool?**

**Response:**

In March 2006, the FBI purchased the wInsight software program. wInsight is an EVM system that will provide early indications of positive or negative variances from planned or scheduled costs. The FBI is also exploring other potential tools to help manage the program. We believe that, while additional tools can help, it is ultimately the responsibility of managers to establish effective policies and procedures and to ensure compliance.

**e. Has it been working?**

**Response:**

The wInsight software has been received and data has been loaded, but it is too early to determine the value of the developmental contract. The program will be fully baselined to accommodate EVM and schedule management before development begins.

**f. Why has the OIG not been reassured by the existence of this tool?**

**Response:**

We have alerted the OIG that this tool cannot be fully evaluated at this point. We believe that when it can be more fully used, its benefits will be clear to the OIG.

**115. An article in *Newsday* pointed out in March that there is another shocking technology gap at the FBI – many agents don't have access to the Internet or Blackberries. The article noted that some FBI agents in New York City did not even have e-mail accounts. The FBI should absolutely have the tools it needs to fight terrorism and crime in the 21st century, most of all in New York City, and one of the most effective means of communications is e-mail and the Internet. FBI agents' not having e-mail or Internet access suggests too much of a pre-9/11 mentality.**

**a. Do you agree that it is important for FBI agents to be able to communicate with state and local law enforcement through the Internet?**

**b. Do you agree that the Internet and e-mail are efficient and effective means of enabling this communication?**

**c. When will FBI agents have access to e-mail and the Internet from their desks?**

**Response to subparts a-c:**

Please see the response to Question 66, above.

**116. Among the more disturbing aspects of everything the Inspector General has presented today in his written testimony are his reports of FBI intelligence violations, specifically: FBI agents intercepting communications outside the scope of FISA orders; FBI agents continuing investigative activities after the authority for the investigation expired; and third parties providing information that was not part of a national security letter request. In light of these findings, please explain the following.**

**a. Were any of these activities that the OIG defines as violations authorized by you, personally, or any deputy of yours?**

**Response:**

No. As indicated in response to Question 60, above, the errors identified by the OIG were either inadvertent or third-party errors. None were the product of directives to exceed FISA or other investigative authority.

**b. Were any of these activities authorized by the President?**

**Response:**

No.

**c. Does the use of surveillance outside the scope of FISA orders by the FBI have any connection to the NSA domestic surveillance program the President has described? Is it part of a separate program?**

**Response:**

No, in response to each question. As previously stated, the compliance issues noted by the IG were inadvertent, and not wilful, violations.

**117. The Inspector General also reports that the OIG found “significant non-compliance” by the FBI with Attorney General guidelines with respect to confidential informants, including “failure to consistently obtain advance approval prior to the initiation of consensual monitoring.” This is troubling to me, particularly in connection with the other violations we have discussed and with parts of our intelligence framework that are**

**apparently out of your control – the NSA program for example. Of course we want strong intelligence, and of course we want you to have the tools you need. However, there is no place for rule-breaking or ducking oversight in our intelligence system.**

**a. Do you agree?**

**Response:**

The FBI has worked diligently to address this issue and agrees that rule-breaking and ducking oversight have no place in our intelligence system. However, the September 2005 OIG report's findings regarding the FBI's compliance with the AG's investigative guidelines do not include findings regarding the use of confidential human sources or the use of consensual monitoring as investigative techniques.

The OIG report states as follows: "With regard to the Guidelines for conducting nontelephonic consensual monitoring under the AG's Procedures for Lawful, Warrantless Monitoring of Verbal Communications, we found the FBI was largely compliant. However, we found that 10% of the monitoring was recorded prior to obtaining requisite approval." (P. 301.) The OIG made recommendations regarding general consensual monitoring activity for body-wires and nontelephonic transmitters, but these recommendations were not specific to human source operations. The vast majority of these monitoring activities will, by their nature, involve cooperating witnesses who will be expected to testify.

As an investigative technique, consensual monitoring is most often used in criminal investigations. The examples used by the OIG regarding the receipt of approval in advance of consensual monitoring all involved criminal activity rather than intelligence gathering. Pursuant to FBI policy, confidential human sources are not ordinarily used to make consensual recordings or permitted to be present while another individual is conducting consensual recording. In the rare instances when this is desired, it must be approved by a supervisor at the ASAC level or above and the approval must be documented in the confidential human source's file.

This compliance issue is being addressed through the inspection process, training, and the Confidential Human Source Re-engineering Project, which is a collaborative effort between the FBI and DOJ to improve compliance with AG Guidelines and to develop standardized policies and processes for validating and managing confidential human sources. The FBI will use the inspection process to ensure that the required authorizations have been obtained in advance of monitoring and have been appropriately documented. Policy will also provide for the issuance of instructions to the field, including instructions to have

noncompliance addressed in employees' performance appraisals, if appropriate, and to refer egregious noncompliance to OPR.

**b. How do you respond to the OIG's findings?**

**Response:**

The FBI welcomes the OIG report and its assessment of our compliance with the four sets of general AG Guidelines that govern our investigative activity. The FBI has made significant progress in designing standardized and automated confidential human source management processes and procedures to be used with respect to all FBI HUMINT. Because we identified many of the OIG's findings in our program self-examination, our re-engineering project has already incorporated most of the OIG's recommendations.

**c. What are you doing to stop this pattern?**

**Response:**

The Confidential Human Source Re-engineering Project was initiated to develop standardized policies and processes for managing and validating human sources, thereby improving compliance with AG Guidelines. This re-engineering effort has incorporated most of the OIG's recommendations. The FBI believes these policy changes, along with the IT systems currently under development to automate workflow, will significantly reduce or eliminate noncompliance with AG Guidelines and FBI policies.

The FBI has also begun to implement an improved suite of training in support of human source operations. This effort is being led by the DI, which convened a meeting of FBI training and subject matter experts at a two-week offsite in January 2006 to develop a training plan. Some alterations to New Agent Training have already been implemented. We are also developing an advanced block of human source operations training that we plan to begin implementing by the fall of 2006.

**d. What is causing this problem?**

**Response:**

Noncompliance frequently involves exigent circumstances and inadequate understanding of AG Guidelines. Although the vast majority of SAs comply with AG Guidelines, some SAs perceive the policies implemented over the years to be conflicting and to create contradictory or excessively burdensome paperwork

requirements. The development of the FBI's new policies and processes for managing confidential human sources, along with appropriate training regarding these new requirements and clearer consequences for noncompliance, should significantly reduce these incidents.

**118. The OIG made 28 recommendations for improving Counterterrorism Task Forces.**

**a. How many of those do you intend to follow? If not all, why not?**

**Response:**

The FBI intends to follow the 15 of the 28 recommendations that pertain to the FBI. The remaining 13 of the 28 recommendations pertain to agencies other than the FBI. The recommendations that pertain to the FBI are: 2, 5, 6, 7, 8, 16, 17, 18, 19, 20, 21, 22, 23, 24, and 25.

**b. What steps have been taken to follow these recommendations so far?**

**c. How many remain, wholly or in part, undone?**

**Response to subparts b and c:**

The FBI had taken significant steps related to these recommendations even before the IG's report was published. Those steps are articulated in the FBI's response to the report, provided as Appendix XIV to the IG report (Report Number I-2005-007). By letter dated 7/11/06, the FBI provided to the OIG a status report reflecting the actions taken to date with respect to the outstanding recommendations. That report, which is law enforcement sensitive, is provided separately.

**Questions Posed by Senator Durbin**

**FBI Computer Capability  
Sentinel Planning**

**119. As the Sentinel information technology upgrade project commences, what specific management controls have been instituted to prevent a repeat of the problems attendant to the failed "Virtual Case File" deployment? Are there additional safeguards and protocols contemplated? If so, please explain.**



**Response:**

Please see the response to Question 95, above. In addition, please note that, while we do not anticipate that Lockheed Martin will fall short in satisfying its contract obligations, the FBI has established managerial and contractual mechanisms to track contractor performance, including the following.

- A disciplined, stable, and well-conceived program management system that includes strict adherence to the FBI's new IT LCMD and a PMO structure modeled on the program management system successfully used within the Intelligence Community.
- A risk management system under which contract performance risks and the steps being taken to mitigate them are identified on a weekly basis.
- A schedule control and monitoring system pursuant to which variances in the contractor's schedule will be identified every two weeks.
- A requirement that both Lockheed Martin and the Sentinel PMO use a certified EVM system and report on EVM status monthly, identifying baseline variances in cost, schedule, and program performance. Certification of these EVM systems requires IV&V that the system is established and performing in accordance with the national EVM standard.
- A rigorous quality assurance program that includes IV&V of the quality control systems used by both Lockheed Martin and the Sentinel PMO.
- A rigorous configuration and change control system designed to control increases in the scope of technical requirements. Scope changes will not occur unless there is a clear decision by senior executives that the change is necessary and there are adequate time and money in the program schedule and budget to implement the change. The configuration and control system will be focused on preventing unnecessary or inappropriate changes to Sentinel's Statement of Work, the System Requirements Specification, and the Technical Concept of Operations.
- An independent IV&V entity that reports to the FBI's CIO and is responsible for both ensuring that Sentinel's program requirements are valid and verifying that the prime contractor's deliverables meet those requirements.
- An award fee structure that is tied to the performance-based contract performance measurements outlined in the Statement of Work. If contract

performance problems are identified and not rectified, the FBI can reduce the amount of the fee (above contractor cost) awarded Lockheed Martin. In other words, if contract performance is stellar, Lockheed Martin's profit will be greater. If performance is substandard, the profit will be smaller or nonexistent. Also, as indicated above, if the contract performance control mechanisms identify poor contract performance that is not rectified, the Sentinel program is structured so that all or portions of the contract may be terminated.

Sentinel is a "modular build" project, with each of the four phases adding discrete functionality. The initial contract is for Phase 1. The other three phases of Sentinel development, plus O&M support, are not guaranteed work but are, instead, options to be exercised at the discretion of the government based on performance.

**120. How are you addressing the various concerns cited by the Justice Department's Inspector General in its March 2006 audit report on pre-acquisition planning pertinent to the Sentinel contract, specifically that:**

**a. The Sentinel project manager is a CIA employee on loan to the FBI for two years with the possibility of a one-year extension, which could be problematic if he decides to leave before Sentinel is fully installed.**

**Response:**

The Sentinel PM, a CIA employee detailed to the FBI, is committed to serving three years on this program. The FBI is building management depth in the Sentinel program's organization to ensure each part of the PMO includes trained back-up personnel who can ensure the continuity of the program if it should lose an employee, regardless of the employee's position or the reason for loss.

**b. The FBI has not yet adequately examined or discussed Sentinel's ability to connect with external systems -- including those in other offices in the Justice Department, the Department of Homeland Security and other intelligence agencies. For instance, the Drug Enforcement Administration, part of the Justice Department, planned to deploy its own new case management system this year and that it is not compatible with Sentinel as currently designed.**

**Response:**

Please see the response to Question 63, above.

c. The FBI planned to finance the computer upgrade by borrowing funds from other FBI programs -- including ones to fight terrorism -- that previously had been appropriated by Congress. The bureau obtained permission to use \$97 million from its fiscal 2005 budget for the Sentinel program, including about \$29 million from its counter-terrorism division, intelligence-related activities and its cyber division. Diverting substantial funds from such mission-critical areas could begin eroding the FBI's operational effectiveness.

**Response:**

Please see the response to Question 61, above.

**Currently Available Capabilities**

121. Your prepared statement describes what tasks an agent at his or [her] computer terminal can perform, but does not explain what they cannot currently accomplish. You testified a few weeks ago before the Senate appropriations subcommittee that in your FY 2007 budget, you are requesting \$100 million for Sentinel. You noted that Sentinel will leverage technology to reduce redundancy, eliminate inefficiencies, and maximize the FBI's ability to use the information in its possession. You stressed that the objectives for Sentinel include (1) delivering a set of capabilities that provide a single point of entry for investigative case management and intelligence analysis; (2) implementing a new and improved FBI-wide global index for persons, organizations, places, things, and events; (3) implementing a paperless information management and work-flow capability; and (4) implementing an electronic records management system. Furthermore a story in the May 1, 2006 issue of *The Washington Post* business section mentioned that the Sentinel contract will "link technology systems among the bureau's offices, allowing its agents to search and share information among one another and with other intelligence agencies." I conclude from these statements that agents are still operating in a paper-based case management environment, that search capabilities are not as sophisticated as they could be, and access to information and interchanges are still far short of the potential.

a. Please describe in detail what automated information access capabilities and other functions agents and analysts presently lack on their desktop computers that the Sentinel project is expected to supply? What information remains in paper form and not electronically accessible?

**Response:**

The automated Sentinel capabilities not presently on an SA's or analyst's desktop include, but are not limited to, electronic workflow management (including electronic document review, approval, and collaboration), enhanced searching of case and intelligence information, information sharing both within the FBI and

with outside entities, and activity reporting. Currently, historical case records, external documents (i.e., court orders), and multimedia formats (i.e., photographs) remain in paper form and, in some cases, are not electronically accessible.

**b. What impediments are imposed on agents now that will be alleviated through the Sentinel deployment?**

**Response:**

When Phase 4 is complete, Sentinel will have removed or substantially reduced the following impediments to the FBI's efficiency.

- The cumbersome, inefficient means of accessing case and case-related information, including manual searches of paper case files.
- The need to physically route case and intelligence documents for approval.
- The requirement to manually track, calculate, and report activity metrics.

**c. At what points in the deployment of the Sentinel system will various new capabilities be accessible?**

**Response:**

Please see the response to Question 55, above.

**OIG Concerns About Information Sharing**

**122. In March 2006, the Inspector General issued an audit report on “The FBI’s Pre-Acquisition Planning For and Controls Over the Sentinel Case Management System.” In that report, the Inspector General emphasizes that**

**“the terrorist attacks of September 11, 2001, underscore the need for agencies involved in combating terrorism to be able to communicate with one another effectively. An intelligence agency may have only partial information on a suspected terrorist, but when coupled with information that other agencies possess, a threat may become more clear. “**

**Earlier in the report, the OIG noted that the “FBI has expended little effort in assessing information sharing with other federal agencies,” that “we have no assurance that the FBI has identified all external systems with which Sentinel must connect” and that “because**

**these requirements have yet to be established, we anticipate a modification to the contract, [which] represents a potential risk of requirements creep.”**

**a. What is your reaction to these assessments? Are they valid?**

**Response:**

Please see the response to Question 63, above.

**b. Wasn't poorly defined and slowly evolving design requirements among the problems contributing to the demise of the Virtual Case File project phase of Trilogy?**

**Response:**

A number of problems contributed to our termination of the VCF project. The FBI has taken care to learn from its mistakes and lay the groundwork for a successful major investment in IT, and the approach to developing Sentinel differs substantially from the VCF approach. For example, Sentinel's requirements and contractual obligations with respect to interfacing with external systems dictate the use of specified standards and best practices. Pursuant to these requirements, when external systems are refreshed, replaced, or enhanced in the ordinary course of their maintenance and upgrading, this will be done using standards compatible with those of Sentinel so that Sentinel systems will be able to communicate with them whether or not their interactions with Sentinel systems were planned initially. This approach and similar approaches to other aspects of the FBI's IT environment will help to minimize "requirement creep."

**c. Do you agree that before proceeding too far along on the path of an expensive insular effort, it is essential to account for the necessary sharing relationships both inside and outside the Bureau and the Department, and address critical compatibility issues? How are you addressing this matter?**

**Response:**

We agree that it is important to establish efficient and productive information sharing relationships both inside the FBI and DOJ and with outside entities. For the ways in which Sentinel will optimize these relationships, please see the response to Question 63, above.

**d. What components are being incorporated into the Sentinel project to ensure system capacity to afford appropriate access to other agencies within the Intelligence Community?**

**Response:**

Please see the response to Question 63, above.

**e. Have there been any changes in the contract to comport with the suggestion of the Inspector General that “the FBI needs to focus more attention on the sharing of information between Sentinel and other agencies’ data systems in these early stages of Sentinel’s development”?**

**Response:**

Please see the response to Question 63, above.

**Sharing & Accessing of Information Beyond the FBI**

**123. In your prepared statement you acknowledge that in contrast to your optimism about the FBI’s ability to successfully function as a leading intelligence agency, others contend that the “FBI is reluctant to share information with its partner agencies.”**

**a. Why do you believe these sentiments abound?**

**Response:**

Although the FBI is now communicating its information sharing policy as clearly, as often, and as broadly as possible, we have not previously focused on the importance of that message. Our policy is to share information with authorized users as a rule and restrict or withhold only by exception. Acting on that policy every day with our many intelligence and law enforcement partners should overcome any remaining perceptions to the contrary.

**b. What is your reaction to these criticisms?**

**Response:**

While the FBI is aware of the perception that we may be reluctant to share information with partner agencies, we have also made clear to the Committee that we are pursuing numerous means of improving both the quantity and quality of shared information, doubling the number of IAs and establishing in every field office a FIG in which SAs and analysts work together with one shared mission. In addition, from January 2004 through January 2006 the FBI’s IA staffing in the FIGs increased by 61%, helping to fuel our sharing of intelligence products. Since 9/11/01, the FBI has disseminated more than 20,000 intelligence reports, assessments, and bulletins to our partners.

The FBI's commitment to information sharing is also demonstrated in recent organizational changes in the FBI, including the creation of a senior level "Information Sharing Policy Group," chaired by the EAD for the NSB. This Group brings together the FBI entities that generate and disseminate intelligence. Since its establishment in February 2004, this body has provided authoritative FBI policy guidance for internal and external information-sharing initiatives. The FBI shares information and ensures collaboration through our NISS which, along with DOJ's LEISP (of which NISS is a part), aims to ensure that those charged with protecting the public have the information they need to take action. The FBI also participates in the Global Intelligence Working Group and the Global Criminal Intelligence Coordinating Council, which were established in 2004 to set national-level policies to improve the flow of intelligence information among United States law enforcement agencies.

**c. How do you propose to change that perspective?**

**Response:**

As the FBI has stated many times, our information-sharing policy is to share with authorized users as a rule and restrict or withhold only by exception. The FBI recognizes that our success in today's threat environment depends on the successes of all of our partners, in both the law enforcement and intelligence communities, and those successes depend on getting the right information into the right hands in a timely manner. For that reason, the FBI will continue to share information as broadly as possible. The FBI has tried to assure our partners of our commitment to broad information sharing, but we understand that actions speak louder than words. Notwithstanding a possible contrary perception, therefore, the FBI will continue to engage in the broadest possible information sharing, because our nation's security depends on it.

**FBI/DHS Fingerprint Database Integration**

**124. What is the current status of the integration effort between the fingerprint databases of the FBI's IAFIS system and Homeland Security's IDENT system?**

**Response:**

With DHS' decision to transition its Automated Biometric Identification System (IDENT) to a 10-print system, the FBI began proactively working with DHS' United States Visitor and Immigrant Status Indicator Technology (US-VISIT) program and other agencies to advance interoperability efforts. In May 2005, principals from DOJ, DHS, and DOS formed an Executive Steering Committee (ESC) to guide the initiative to make IDENT and the FBI's Integrated Automated

Fingerprint Identification System (IAFIS) interoperable, creating an Integrated Project Team (IPT) structure to carry out the design, development, and implementation of an integrated information sharing solution. Under the direction of the ESC, the IPT has made progress toward achieving an interoperability solution that fully addresses interagency requirements. The IPT has completed a Concept of Operations and continues to design options for an interoperable biometric system as a foundation for information sharing based on positive identification. In addition, the IPT has identified high-level interoperability business requirements based upon the needs of IDENT and IAFIS users. These requirements are being analyzed and refined to draft functional and technical requirements needed for design development. The IPT has also identified key policy issues regarding the biometric-based sharing of criminal history and immigration history information related to agency-specific business processes and mission operations, as well as legislative mandates. The mitigation strategies necessary to resolve these issues are being discussed by IPT representatives, as well as subject matter experts within the Departments.

IDENT/IAFIS interoperability is being planned in phases: 1) Interim Solution, 2) Initial Operating Capability (IOC), and 3) Full Operating Capability (FOC). Initially, the FBI and US-VISIT will focus on developing a prototype capable of sharing, in near real time, biometric data on FBI wants and warrants, DOS Category One Visa Refusals, and DHS expedited removals. Full interoperability, which will be achieved through implementation of the IOC and FOC phases, includes sharing all biometric data and would allow agencies to access associated biographic information as allowed by law and policy.

The first step in implementing the interim solution is complete. On November 30, 2005, the FBI began the transfer of all new or updated IAFIS want or warrant records associated with FBI numbers to DHS/US VISIT, on a day-forward basis, to strengthen the screening processes at DOS consulates and DHS ports-of-entry. Before this change, the FBI transferred IAFIS records on wanted persons with a foreign or unknown place of birth, foreign or unknown citizenship, or previous immigration charge. The second step toward implementation of the interim solution is the interagency joint development of an interim Data Sharing Model (iDSM) that will allow a reciprocal sharing of biometric data subsets between IDENT and IAFIS in "near real time" beginning in September 2006.

**125. What is the prognosis and timetable for achieving fuller integration and cross-matching capabilities between IDENT and IAFIS?**



**Response:**

As indicated above, the iDSM deployment is scheduled for September 2006. A phased development plan for interoperability between IDENT and IAFIS has been adopted by the IPT to assure that the interoperability implementation schedule maintains technical alignment with the rollouts of the FBI's Next Generation IAFIS initiative, the DHS' IDENT Modernization effort, as well as the DHS transition to 10-print initiative over the next four years.

**126. What impediments hinder the IDENT/IAFIS integration effort and how do you suggest that they be overcome?**

**Response:**

The best method for sharing data between IDENT and IAFIS is still to be determined by the Interoperability IPT. A joint cost benefit analysis is currently being conducted by US-VISIT and the FBI's CJIS Division in an effort to identify the best means of exchanging data between the two systems.

**127. What catalysts would resolve the delays and accelerate progress of the IDENT/IAFIS integration?**

**Response:**

The President's FY 2007 budget supports the progress of the IDENT/IAFIS integration effort and Congressional support of the President's request would help both agencies make progress on this project.

**128. Are reported concerns (*Government Computer News*, 8/29/05) that (1) "despite continued references in official documents to the integration of the two systems, they can never be fully merged" and that (2) "parts of IAFIS contain information classified at a higher level than IDENT users are allowed to access" valid ones? How do you recommend that these issues be resolved?**

**Response:**

The IPT is considering multiple models to identify the best method for exchanging information. The IPT is also analyzing special handling requirements for protected individuals within each model.

**129. Now that a key policy discrepancy has been alleviated with the 10-print decision announced in July 2005 by Department of Homeland Security Secretary Michael Chertoff, have you or your designees discussed the operational issues directly with Secretary**

**Chertoff or any of his designees? If so, with what outcome? If not, do you anticipate discussions in the near term?**

**Response:**

Executive Management from the FBI's CJIS Division has established a strong working relationship with the Executive Management from the DHS/US-VISIT Program and DOS. As mentioned previously, representatives from these agencies lead the Interoperability ESC and have formed an IPT. ESC Meetings are conducted regularly to discuss the interoperability effort, as well as the transition to 10-print collection.

**130. What further role can the FBI play to facilitate the integration process?**

**Response:**

In order to facilitate the integration process, the FBI must maintain its current level of commitment to the interoperability effort. In addition to extensive agency participation within the interoperability IPT, collaborative efforts to obtain the support of advisory stakeholders have been a top priority of US-VISIT and the FBI's CJIS Division. For instance, representatives of the IPT attend regular working group and subcommittee meetings of the CJIS Advisory Policy Board (APB) to update interoperability progress and to obtain approval of planned efforts. The IPT has received positive stakeholder support from the APB on its interoperability efforts, as evidenced by the appointment of a DHS representative to the APB. In December 2005, the APB endorsed the current interoperability efforts.

**USA PATRIOT Act**

**131. Section 5 of the USA PATRIOT Act Additional Reauthorizing Amendments Act of 2006 (Public Law 109-178), "Privacy Protections for Library Patrons," is intended to clarify that the FBI may not issue National Security Letters to libraries that are functioning in their traditional role, including but not limited to, lending books, providing access to books or periodicals in digital form, and providing basic access to the Internet. During the debate on the USA PATRIOT Act Additional Reauthorizing Amendments Act, Senator Sununu, the legislation's author and lead sponsor, and I engaged in a colloquy on the floor of the Senate to make clear congressional intent in this respect. During the hearing, my staff provided a copy of this colloquy to your staff. I have also attached a copy of the colloquy to these questions. During the hearing, I asked you if you agreed that Section 5 clarifies that a library functioning in its traditional role is not subject to a National Security Letter. You promised to respond in writing to this question. Please do so.**

**Response:**

Pursuant to 18 U.S.C. § 2709, the FBI has always been limited in the entities on which it can serve NSLs. In the context of this particular question regarding libraries, an NSL can only be served on an entity that is an electronic communication service provider. The FBI has always understood an electronic communication service provider to be an entity that provides electronic communication services as defined by 18 U.S.C. § 2510(15). Thus, a library is only subject to an NSL if it provides electronic communication services.

Section 5 of the USA PATRIOT Act Additional Reauthorizing Amendments Act of 2006 (Public Law 109-178), "Privacy Protections for Library Patrons," states that a library functioning in its traditional role, statutorily defined as including the provision of access to the Internet, is not subject to an NSL unless the service it provides meets the definition of an electronic communication service, as defined in 18 U.S.C. § 2510(15). As the above makes clear, the FBI believes Section 5 did not actually change the law.

**Immigration Background and Name Checks**

**132. The processing of many applications for immigration benefits involves a background check by the FBI, including a criminal history check based on the applicant's name ("name check"). Please describe the background check and name check process.**

**Response:**

Several million name check requests are received by the FBI each year, and we continue to work to complete our review of a batch of 2.7 million requests submitted by USCIS in December 2002. The FBI's NNCP receives most USCIS name check requests by way of a magnetic data tape that can hold up to 10,000 names. When a data tape is received, the names on the tape are electronically checked against the FBI's UNI. These searches seek all instances in which the individual's name appears in both "main" files and "reference" files. If the individual's name appears in a "main" file, the individual is, himself, the subject of an FBI investigation, whereas the individual's inclusion in a "reference" file indicates only that the person's name appears in an FBI investigation. "References" may be associates, conspirators, or witnesses.

The majority of the names submitted on a data tape are electronically checked and returned to USCIS as having "no record" within 48 to 72 hours. A "no record" result indicates that the FBI's UNI database contains no identifiable information regarding the individual. Duplicate submissions (i.e., identically spelled names

with identical dates of birth submitted within the last 120 days) are not checked, and the duplicate findings are returned immediately to USCIS.

If the database does contain identifiable information regarding the individual, a secondary manual name search is conducted. These manual searches typically result in "no record" results within 30 to 60 days, and the USCIS is so advised. The remaining name checks (usually about 10% of those originally submitted) are identified as possibly being the subject of an FBI record. At this point, the FBI record must be retrieved and reviewed. If the record is available in the FBI's electronic record keeping system, it can be reviewed quickly. If not, the relevant information must be retrieved from an existing paper record. Review of this information is necessary to determine whether the information is positively identified with the name check requested. If the information is not identified with the request, the request is closed as a "no record," and the requesting agency is so notified.

The average time required to retrieve and review an FBI record for possible information related to a name check request depends on the number of files an analyst must obtain (which is dictated by the number of "hits" on a name), the location and availability of those files, and the amount of information contained in each file. If a file is available electronically or stored locally, the analyst will be able to obtain the file within a matter of days. If, instead, the file is located in one of over 265 different FBI locations that can house information pertinent to a name check, the file must be requested, and this process may take considerably longer.

Ultimately, less than 1% of the requests are identified with files containing possible derogatory information. If such information is located, the FBI forwards a summary to the USCIS, which adjudicates the matter (the FBI does not adjudicate applications for immigration benefits).

**133. During the hearing, I asked you about delays in FBI background checks and name checks for applicants for immigration benefits. You said that you would provide statistics on these delays. Please provide the following:**

**a. A statistical breakdown by time periods of delay.**

**Response:**

The current pending name checks submitted by USCIS are broken down as follows:

	0-30 Days	31-60 Days	61-90 Days	91-120 Days	Over 120 Days	Over 1 Year
Total USCIS Name Checks	36888	45026	31746	13934	68411	106011

**b. A statistical breakdown of the delays for different types of immigration applications.**

**Response:**

	0-30 Days	31-60 Days	61-90 Days	91-120 Days	Over 120 Days	Over 1 Year
Asylum Program	2485	3144	2349	512	3229	2977
Waivers and Misc.	1201	1604	1256	345	6556	5634
Exec Office of Immigr. Review	1096	1265	1783	752	1465	20
Naturalization	15431	21582	11941	6857	25975	44843
Personnel Security	10	4	4	1	123	464
Adjustment of Status	16665	17427	14413	5467	31063	52073
<b>TOTALS</b>	<b>36888</b>	<b>45026</b>	<b>31746</b>	<b>13934</b>	<b>68411</b>	<b>106011</b>

**c. A statistical breakdown of the delays by the applicants' country of origin.**

**Response:**

The NNCP does not track incoming USCIS name checks by country of origin, but it does attempt to process USCIS name checks on a first-in, first-out basis, unless USCIS requests that a given request be expedited.

**134. a. How does the FBI relay information regarding a completed background check to U.S. Citizenship and Immigration Services?**

**Response:**

The FBI relays information regarding a completed background check to USCIS in a couple of ways. Batch USCIS name check requests that are submitted on a magnetic data tape that result in a "no record", which means that the FBI's

Universal Index database contains no identifiable information regarding a particular individual, are returned on a magnetic data tape. If an expedited name check request results in a "no record", the result is faxed to USCIS. The results of a name check other than "no record" are provided to USCIS in a writing (paper based) and sent to USCIS Headquarters via FedEx.

**b. Have there been any cases in which the FBI has completed a background check but, due to miscommunication, CIS mistakenly believes that the check has not been completed? If yes, what has been the cause for the miscommunication and what can be done to ensure such miscommunications do not take place in the future?**

**Response:**

The FBI's NNCP personnel do not recall an instance where the results of a name check were transmitted to USCIS Headquarters, and through a miscommunication, USCIS Headquarters continued to believe the name check was still pending. The FBI is not familiar with how name check results are provided to USCIS field offices once the information is provided to USCIS Headquarters. The FBI Name Check staff and the USCIS Headquarters staff communicate on a daily basis regarding the status of name checks. Additionally, USCIS Headquarters staff receive a summary of all quarterly responses to insure accuracy regarding the status of a completed name check.

**135. Does the FBI have a process for expediting background checks for applications that have been pending for a long period of time? If not, should there be such a process?**

**Response:**

The policy of the FBI's NNCP is to process the oldest name checks first. Customer agencies, such as USCIS, may request expedited handling of specific name checks. The criteria used to determine which name checks will receive expedited handling are established by the submitting agency, including USCIS, and are not developed or evaluated by the FBI. The FBI does request that the number of expedited cases be kept to a minimum in fairness to those awaiting the results of other pending name check requests. The FBI's policy is to be responsive to our customers' needs within the limits of our resources.

**ENCLOSURE A**

**QUESTIONS 68 AND 113**

**3/17/06 LETTER  
FROM CTD AD WILLIE HULON  
To DOJ IG GLENN FINE**



U.S. Department of Justice

Federal Bureau of Investigation

---

Washington, D. C. 20535-0001

March 17, 2006

The Honorable Glenn A. Fine  
Inspector General  
Office of the Inspector General  
United States Department of Justice  
Room 4322  
950 Pennsylvania Avenue, Northwest  
Washington, D.C. 20530

Dear Mr. Fine:

I would like to thank you for providing the Federal Bureau of Investigation (FBI) the opportunity to respond to your report entitled, "The FBI's Efforts to Prevent and Respond to Maritime Terrorism."

I recognize the substantial challenge the Office of the Inspector General (OIG) has in producing timely reports on complex issues such as this. This challenge is even more difficult when assessing FBI operations because of the rapid changes it continues to undergo to optimally position itself to address the evolving threats to our Nation.

In large part, the FBI agrees with the findings and recommendations of this report. Accordingly, Executive Management from the Counterterrorism Division (CTD) of the FBI and personnel from the appropriate programs within the FBI have reviewed OIG's draft report concerning the FBI's efforts to prevent and respond to maritime terrorism. Ideally, we would like for the report to be updated to provide a current status of maritime security efforts in the FBI, and to that end have set forth several points of information for you to consider.

- The FBI initiated the Maritime Security Program (MSP) in July 2005. This proactive measure was taken by CTD Executive Management in recognition of the potential threat of maritime terrorism. It is worth noting that this program was established without additional funding by reallocating resources within CTD.
- Availability of resources has also influenced the FBI's participation in various exercises. Although the FBI would like to participate in additional exercises, the FBI is currently able to support the joint exercises that are coordinated through the National Exercise Program.
- The FBI is actively working with the United States Coast Guard (USCG) and other agencies to resolve potential coordination issues in advance of actual threats and incidents in the maritime domain.



Mr. Glenn A. Fine

Additionally, the following comments are to correct or clarify statements made in the text of the audit report:

4. Page “v”, first paragraph and page 25, first paragraph: The MSP prepared an Electronic Communication (EC) to the field to request that an FBI Special Agent (SA), as opposed to a Task Force Officer (TFO) be designated as the primary Maritime Liaison Agent (MLA). Although this EC was drafted, it was not approved by CTD management. As a result, in many Field Offices a TFO serves as the primary or only MLA.
5. Page “vi”, first bullet: This point may need to be modified to include the capabilities of the Laboratory Division’s Hazardous Materials Response Unit (HMRU) in dealing with a weapon of mass destruction (WMD) incident. HMRU provides technical and scientific operational response to WMD incidents, including, but not limited to, crime scene management, evidence recovery, emergency decontamination and scientific assessments. The responsibilities of the Hazardous Devices Response Unit (HDRU) includes the response to threats and actual devices before they are detonated or used in an "attack." HDRU does not respond to post-detonation attacks; that is the responsibility of HMRU and/or the Laboratory Division's Explosive Unit.
6. Page “viii”, last paragraph: The statement, “The FBI has not collected complete data on the number of suspicious activities or terrorist threats involving seaports,” is correct. However, the MSP has begun to collect this information from all available sources. The MSP has created a data base to capture this information which will be used to identify and track possible trends in suspicious activity at ports and port facilities. The MSP is also in the process of creating a standardized reporting mechanism for use by the MLAs when responding to incidents. These reports will be maintained in the MSP case file and the information will also be entered into the data base. Finally, the MSP maintains liaison with other agencies and the private sector, such as the USCG, Office of Naval Intelligence (ONI) and the International Council of Cruise Lines (ICCL), for the sharing of pertinent threat information.
7. Page 20, bottom of the page: It should be noted that the MSP will present the 2006 Maritime Liaison Agent Training Conference in Long Beach, California from 04/03-07/2006. The Port of Long Beach is one of the busiest ports in the United States with a variety of inter-modal transportation systems. This site was specifically chosen because it offers hands on/familiarization training using various port facilities and vessels. The curriculum for this conference is expected to include presentations on the impact of maritime directives under the National Strategy for Maritime Security (NSMS); informant and liaison development; legal issues; enhancing maritime domain awareness; the FBI’s capabilities and resources to respond to a maritime incident; and guidance to the field on best practices.
8. Page 24, first full paragraph: The report indicates that as a result of placing responsibility for managing the MLA Program under the MSP, all of the FBI’s transportation related counterterrorism programs are located within the same

Mr. Glenn A. Fine

organizational unit. This is not the case as the National Joint Terrorism Task Force (NJTTF) initiated the Rail Liaison Agent (RLA) Program via EC dated 10/24/2005. The NJTTF requested each Field Office to designate an FBI SA or TFO as a primary and secondary RLA. A separate initiative is currently underway to evaluate the feasibility of creating a program or unit focused on all aspects of the transportation sector. It is important to note this initiative is unfunded and would be created by reallocating existing resources.

9. Page 24, last paragraph: The report mentions that one of the objectives of the MSP was to create a website on the FBI's Intranet to facilitate the dissemination of information pertaining to directives, training, intelligence and other matters. This objective has been accomplished. The MSP website address is <http://ctd.fbinet.fbi/semu/maritime/>. This website contains information on maritime directives including National Security Presidential Directive (NSPD)-41/Homeland Security Presidential Directive (HSPD)-13, the NSMS and key supporting plans; maritime related statutes; intelligence reports; points of contact; and links to related programs including the Directorate of Intelligence (DI), and the Office of the General Counsel (OGC). Information is continually updated or added to the website. The MLAs are notified of information posted to the website via e-mail. The website has generated positive feedback from the MLAs and is a readily available source of standardized information for the field.
10. Page 24, last paragraph: The report also mentions that another objective of the MSP was to review maritime related suspicious activity reports to identify any trends that may be indicative of pre-operational planning. As noted above, the MSP has already started this process, which is ongoing. This effort is complicated by the lack of standardized reporting and difficulty in retrieving this information, as stated elsewhere in the findings.
11. Page 25, middle of the page: The report states that the MSP has not reviewed the eight supporting plans under the NSMS to identify the FBI's responsibilities nor identified all of the FBI's representatives assigned to the corresponding working groups. That information was supplied to OIG at the inception of the MSP. Since then, the MSP has thoroughly reviewed NSPD-41/HSPD-13, the NSMS and all eight of the supporting plans. The FBI's responsibilities under these directives have been identified and are being addressed. NSPD-41/HSPD-13, the NSMS and key supporting plans are posted to the MSP website. Due to limited resources, the MSP must prioritize which of the working groups to attend in support of these efforts. In that regard, representatives from the MSP have regularly attended and participated in the Maritime Security Policy Coordinating Committee (in support of Executive Management); the Maritime Security Working Group; the Maritime Operational Threat Response (MOTR) Implementation Team; and the Maritime Domain Awareness Implementation Team. In addition, an interagency MOTR Joint Working Group (JWG) has recently been established to address the planning, standardization and exercise requirements that will be deleted from the final version of the MOTR Plan as the Homeland Security Council has indicated. The MSP participates in this JWG as well as the Border and Transportation Security Policy Coordinating Committee.

Mr. Glenn A. Fine

12. Page 25, fourth paragraph: The report states neither the MSP's FY 2006 goals and objectives nor the critical duties of an MLA include the need for the FBI to develop relationships with people who can inform the FBI about maritime operations. It should be noted that at the time the MSP's goals and objectives were established (via EC dated 08/19/2005), the MSP did not have responsibility for managing the MLA Program. In fact, the first objective identified in that EC was to coordinate with the NJTTF to assume responsibility for the MLA Program. That objective was accomplished on 10/04/2005, when the MSP assumed responsibility for managing the MLA Program.

Furthermore, within the goals and objectives (via EC dated 08/19/2005), the MSP established various objectives for the field. One of these objectives was to "ensure effective liaison between the MLA and various law enforcement agencies, port and shipping officials in respect to counterterrorism preparedness." In the goals and objectives EC, the MSP identified five core competencies which included the establishment of a human intelligence base.

Finally, in an EC to all Field Offices dated 07/12/2004, the NJTTF stated, "The goal of the MLA Program is to enhance the maritime environment through increased interaction between MLA members, private industry, state and local port authorities, to include law enforcement and other federal agencies with maritime responsibilities. These enhancements will result from the establishment of close working relationships between the MLAs and concerned entities within the maritime field..." The EC goes on to provide additional guidance and an extensive list of recommended liaison contacts, including participation in the local Area Maritime Security Committee (AMSC). In addition to these specific recommendations, every FBI SA, including those designated as MLAs, are evaluated on specific critical elements. One of the core critical elements for all FBI SAs is the development of an intelligence base, which includes source development. This process encompasses identifying, initiating and developing relationships with individuals or organizations that may provide information or assistance in investigations and assignments. Therefore, CTD believes the need for the FBI to develop relationships with people who can inform the FBI about maritime operations has been thoroughly addressed.

As you requested, the MSP has provided responses to pertinent recommendations. Additionally, recommendations not under MSP's purview were provided to the appropriate offices, (i.e., the DI, the Critical Incident Response Group (CIRG), and CTD's Counterterrorism Analysis Section.) Responses to the recommendations are set forth below.

#### **Recommendation #1**

**OIG Recommendation:** Ensure that MLA guidance is consistent with the actual role of MLAs.

**FBI Response:** FBI agrees with this recommendation. The MSP has already made significant progress in this regard.

Through the creation of the MSP website, which contains information on maritime directives, including NSPD-41/HSPD-13, the NSMS and key supporting plans; maritime related statutes; intelligence reports; points of contact; and links to related programs including the DI and the

Mr. Glenn A. Fine

OGC. Information is continually updated or added to the website. The MLAs are notified of information posted to the website via e-mail. The website has generated positive feedback from the MLAs and is a readily available source of standardized information for the field.

The MSP is in the process of planning the 2006 Maritime Liaison Agent Training Conference in Long Beach, California from 04/03-07/2006. This site was specifically chosen because the Port of Long Beach is one of the busiest ports in the United States with a variety of inter-modal transportation systems. The conference will include hands on/familiarization training using various port facilities and vessels. The curriculum for this conference is expected to include presentations on the impact of maritime directives under the NSMS; informant and liaison development; legal issues; enhancing maritime domain awareness; the FBI's capabilities and resources to respond to a maritime incident; and guidance to the field on best practices.

Finally, now that the MSP has responsibility for management of the MLA Program, the MSP will establish specific, quantifiably measurable and attainable goals and objectives that are consistent with the responsibilities assigned to the MLAs, to include recommendations for participation in various local working groups and liaison contacts.

## **Recommendation #2**

**OIG Recommendation:** Assign MLAs based on an assessment of the threat and risk of a terrorist attack to critical seaports.

**FBI Response:** FBI agrees with this recommendation. FBI will ensure that resources are assigned or available necessary to address the risk or threat based on the assessment.

## **Recommendation #3**

**OIG Recommendation:** Measure the amount of resources devoted to maritime efforts by establishing a maritime case classification under the general Counterterrorism Preparedness classification.

**FBI Response:** FBI agrees with this recommendation. The MSP has already taken certain steps which would enhance the FBI's ability to measure the amount of resources devoted to maritime efforts.

FBI is in the process of establishing a classification for maritime matters.

In August 2005, the MSP provided recommendations to the Counterintelligence Division for changes to the Investigative Accomplishment Report (FD-542) to capture activity conducted in support of the MLA Program. Finalization of the modifications to this report are pending.

## **Recommendation #4**

**OIG Recommendation:** Require field offices to name at least one MLA to each AMSC.

**FBI Response:** FBI agrees with this recommendation. FBI will ensure that adequate resources are dedicated to each Area Maritime Security Committee to address priority matters.

Mr. Glenn A. Fine

#### **Recommendation #5**

**OIG Recommendation:** Require field offices to immediately notify the Maritime Security Program of any MLA appointments or reassignments.

**FBI Response:** FBI agrees with this recommendation. The MSP updates the MLA list on a regular basis. The MLA list is maintained by the MSP and is available on the MSP web site. The list identifies, by Field Office, all of the MLAs as well as the JTTF Supervisors who have oversight of the MLA Program. The list provides contact information, identifies if the MLAs are assigned to a Resident Agency (RA) and which ports they cover. The MSP has advised field offices to immediately notify the MSP of any personnel changes affecting the MSP, and this guidance will be reiterated through training such as the 2006 Maritime Liaison Agent Training Conference.

#### **Recommendation #6**

**OIG Recommendation:** Ensure that the Maritime Security Program has measurable objectives.

**FBI Response:** FBI agrees with this recommendation and recognizes that significant changes and progress in the MSP require the establishment of more specific, quantifiably measurable and attainable goals and objectives.

While FBI recognizes that the goals and objectives established for the MSP (via EC dated 08/19/2005) did not include quantifiable measures, it should be noted that the MSP was a new program and no previous goals and objectives had been established. Furthermore, the MSP did not have responsibility for managing the MLA Program at the time the initial objectives were established. The first objective of the MSP was to coordinate with the NJTTF to assume responsibility for the MLA Program.

It is also worth noting that the NSMS and all of the supporting plans were released in the final quarter of 2005, after the date on which these objectives were established. Final directives under the NSMS have not been established, even as of the date of this response. Under these circumstances, it is difficult to quantify the amount of training and/or reference materials required to train MLAs in the field.

Despite the lack of specific, quantifiably measurable objectives at the inception of the program, the MSP accomplished several of the stated objectives, including the following:

- The MSP assumed responsibility for managing the MLA Program on 10/04/2005;
- Training and reference materials to assist the MLAs have been distributed via e-mail, posted to the FBI's Intranet, and will be presented at the 2006 Maritime Liaison Agent Training Conference scheduled to take place 04/03-07/2006;
- The MSP established a web site on the FBI's Intranet where current information including, but not limited to, maritime directives, statutes and intelligence is maintained;
- The MSP continually identifies, analyzes and disseminates information pertaining to maritime threats, vulnerabilities and safety/security issues;

Mr. Glenn A. Fine

- The MSP continually coordinates with other programs within the FBI to enhance situational awareness for the MSP, other programs, FBIHQ and the field;
- The MSP has already begun to review and track suspicious activity reports to determine if there are any trends which could indicate terrorist activity and has disseminated information to the field in this regard; and
- The MSP is actively engaged in liaison with other government agencies as well as the private sector. This effort and the fact that the MSP serves as a primary point of contact and a coordination center within the FBI for maritime issues has enhanced the FBI's liaison with these groups.

#### **Recommendation #7**

**OIG Recommendation:** Ensure that the Maritime Security Program's objectives include developing human intelligence.

**FBI Response:** FBI agrees with this recommendation and asserts that the MSP and the NJTTF have already provided such guidance to the MLAs.

As stated above, at the time the MSP's goals and objectives were established, the MSP did not have responsibility for managing the MLA Program. Even so, the MSP established various objectives for the field. One of these objectives was to "ensure effective liaison between the MLA and various law enforcement agencies, port and shipping officials in respect to counterterrorism preparedness." In the goals and objectives EC, the MSP identified five core competencies which included the establishment of a human intelligence base.

Prior to the existence of the MSP, in an EC to all Field Offices dated 07/12/2004, the NJTTF stated, "The goal of the MLA Program is to enhance the maritime environment through increased interaction between MLA members, private industry, state and local port authorities, to include law enforcement and other federal agencies with maritime responsibilities. These enhancements will result from the establishment of close working relationships between the MLAs and concerned entities within the maritime field..." The EC goes on to provide additional guidance and an extensive list of recommended liaison contacts, including participation in the local AMSC.

In addition to these specific recommendations, every FBI SA, including those designated as MLAs, are evaluated on specific critical elements. One of the core critical elements for all FBI SAs is the development of an intelligence base, which includes source development. This process encompasses identifying, initiating and developing relationships with individuals or organizations that may provide information or assistance in investigations and assignments. Therefore, FBI believes the need for the FBI to develop relationships with people who can inform the FBI about maritime operations has been thoroughly addressed.

The MSP also plans to address liaison and the development of a human intelligence base during the 2006 Maritime Liaison Agent Training Conference which is scheduled for 04/03-07/2006. In addition, the MSP will include specific recommendations to the MLAs in the objectives which will be established for FY 2007.

Mr. Glenn A. Fine

#### **Recommendation #8**

**OIG Recommendation:** Ensure that the FBI's MOTR operations plan examines high risk scenarios, determines the required response time, and evaluates how FBI resources would address the scenarios.

**FBI Response:** The FBI's maritime operational response plan takes into account various high-risk scenarios to include the criminal/terrorist use of biological, chemical or radiological WMD, as well as Improvised Explosive Devices (IEDs) and Improvised Nuclear Devices (INDs). Other high-risk scenarios include a large number of hostages on a maritime platform and/or the involvement of sophisticated criminal/terrorist adversaries. The TSB's tactical response to maritime threats mirrors the response to any other tactical response. That is, the FBI tactical response is a tiered approach which recognizes that local field offices will respond as necessary (Tier 1), with regional response (Tier 2) added as the evaluation of the situation may dictate. National response, as required (Tier 3), will involve the deployment of the Hostage Rescue Team (HRT), as well as other FBI SWAT teams and possibly the HDRU and the Laboratory's HMRU, as the scenarios would necessitate. Response times vary as a consequence of venue. HRT, HDRU and HMRU response times are typically notification plus four hours for deployment in addition to any travel time involved to the specific venue.

#### **Recommendation #9**

**OIG Recommendation:** Establish a requirement for joint FBI/Coast Guard exercises in field offices assessed as having high-risk seaports.

**FBI Response:** CIRG will require the fourteen (14) field offices that have been given enhanced tactical maritime training to make overtures to the USCG to conduct joint exercises on an annual basis. It should be noted that the FBI is not in a position to require USCG participation, however, the FBI will extend the invitation to the USCG as well as to other appropriate entities.

#### **Recommendation #10**

**OIG Recommendation:** Resolve potential role and incident command conflicts in the event of a maritime terrorist incident through joint exercises and, if necessary, a revised and broadened MOU with the Coast Guard.

**FBI Response:** FBI concurs in stating that this is currently being addressed through the revision of the final interagency MOTR Plan. It may be premature to determine if a revised memorandum of understanding (MOU) with the USCG will be necessary until the final MOTR Plan has been approved and vetted through exercises and/or operations. Again, the FBI is not in a position to require the USCG to enter into a renewed MOU.

#### **Recommendation #11**

**OIG Recommendation:** Prepare after-action reports after all maritime-related exercises and use the reports to identify and disseminate lessons learned and best practices.

**FBI Response:** This is being addressed in a separate joint initiative within the FBI. It is anticipated an After Action Report (AAR) template will be developed that applies to all critical incidents, special events and exercises. CIRG's Crisis Management Unit (CMU) is responsible

Mr. Glenn A. Fine

for program oversight for the production of AARs per the Manual of Investigative and Operational Guidelines (MIOG), Part 2, section 30-1.8 (1) (a), (b) and (c) which specifically sets out the requirements for AARs.

#### **Recommendation #12**

**OIG Recommendation:** Ensure that all field offices submit critical incident reports to the CIRG by January 15 each year; require the FBI's Maritime Security Program, in consultation with the CIRG, to use the reports to conduct maritime-specific reviews of the FBI's crisis management policies and practices — including any requirements for field office crisis management plans — and to disseminate maritime-related lessons learned and best practices.

**FBI Response:** CIRG's CMU ensures adherence to the MIOG's Part 2, section 30-1.8 which requires that field offices submit critical incident reports to CIRG by January 15th of each year. CTD's MSP will provide information concerning maritime related lessons learned and best practices.

#### **Recommendation #13**

**OIG Recommendation:** Assess the threat and risk of maritime terrorism compared to other terrorist threats and ensure the National Threat Assessment ranks the various modes of attack and targets.

**FBI Response:** FBI will ensure that intelligence gaps are identified and action is initiated to resolve any deficiencies.

#### **Recommendation #14**

**OIG Recommendation:** Ensure the amount of FBI resources dedicated to maritime terrorism is based on the extent of the maritime threat in relation to other threats.

**FBI Response:** FBI agrees with this recommendation. FBI will ensure that adequate resources are allocated to address priority threats.

#### **Recommendation #15**

**OIG Recommendation:** Monitor the progress of operating divisions and field offices in answering intelligence collection requirements pertaining to seaports and maritime terrorism.

**FBI Response:** The Directorate of Intelligence will provide a response to this recommendation.

#### **Recommendation #16**

**OIG Recommendation:** Focus intelligence reporting to more comprehensively address potential maritime-related terrorist targets and methods.

**FBI Response:** The Directorate of Intelligence will provide a response to this recommendation.

#### **Recommendation #17**



Mr. Glenn A. Fine

**OIG Recommendation:** Name a unit within the Counterterrorism Division to monitor the volume and substance of all FBI maritime-related intelligence.

**FBI Response:** FBI Counterterrorism Division will ensure that Maritime related intelligence as well as investigations are monitored and properly managed.

**Recommendation #18**

**OIG Recommendation:** Consider establishing a requirement for regular field office intelligence bulletins to summarize the field office's suspicious incident reporting and, if such a requirement is adopted, establish standardized frequency, content, and distribution requirements.

**FBI Response:** The Directorate of Intelligence will provide a response to this recommendation.

The FBI has prepared the appropriate responses to the recommendations found in your report. The responses have undergone a classification review (Enclosure 1) and Sensitivity Review (Enclosure 2).

The responses were coordinated through the FBI's Inspection Division. Please contact Shirlene Savoy of the Inspection Division should you have any questions. Ms. Savoy can be reached at (202) 324-1833.

I want to thank you again for your efforts in producing this report, and I welcome the opportunity to discuss in detail the progress the FBI continues to make in this area.

Please contact me should you have any questions regarding this matter.

Sincerely yours,

Willie T. Hulon  
Assistant Director  
Counterterrorism Division

**ENCLOSURE B**

**QUESTION 111**

**5/25/06 LETTER**

**FROM FBI OFFICE OF CONGRESSIONAL AFFAIRS  
TO SENATOR FEINGOLD**



U.S. Department of Justice

Federal Bureau of Investigation

---

Washington, D. C. 20535-0001

May 25, 2006

The Honorable Russell D. Feingold  
United States Senate  
Washington, DC

Dear Senator Feingold:

I am writing in response to your April 24, 2006 letter to Director Robert S. Mueller, requesting copies of policy directives mentioned in a March 14, 2006 FBI press release. By letter dated March 31, 2006, Chairman Pat Roberts requested copies of the same documents on behalf of the Senate Select Committee on Intelligence (the "SSCI"). By cover dated April 28, 2006, the FBI furnished the SSCI with copies of the referenced directives, as well as two additional directives that provide further context for the responsive materials. It is our understanding that these documents are now available for review by Senators and staff with appropriate clearances. We hope you and your staff will find these materials helpful.

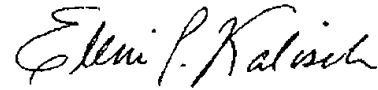
In your letter, you also inquired whether the directives cited in the March 14, 2006 FBI press release are the same as those documents cited on pages 196-197 of the September 2005 Office of Inspector General ("OIG") report entitled, "The Federal Bureau of Investigation's Compliance with the Attorney General's Investigative Guidelines." In sum, there is substantial overlap between the documents referenced in the March 2006 press release and those cited in the OIG's September 2005 report. All but one document cited by the OIG (namely, the April 2004 communication concerning "Special Events") are among the materials referenced in the FBI press release and subsequently provided to the SSCI. The documents furnished to the SSCI, however, also include two directives not cited by the OIG (one is classified; the other post-dates the documents cited by the OIG).

Finally, your letter asks for an explanation of the process that led the FBI to issue these directives and the details of any incidents that may have prompted these clarifications. The directives in question consist of six separate documents. Two of the directives were issued to provide initial guidance on new or revised Attorney General guidelines. The remaining four documents were issued to emphasize and clarify existing policies. None of the directives references specific incidents or operations. Rather, the documents reflect an ongoing dialogue between FBI Headquarters and FBI field offices, designed to underscore and complement the regular guidance provided to employees by the field-based legal advisors, known as Chief Division Counsels.

The Honorable Russell D. Feingold

We appreciate this opportunity to respond to your inquiry. Again, we hope you and your staff will find the materials furnished to the SSCI helpful and informative.

Sincerely,

A handwritten signature in cursive script, reading "Eleni P. Kalisch".

Eleni P. Kalisch  
Assistant Director  
Office of Congressional Affairs

**ENCLOSURE C**

**QUESTION 112**

**11/25/05 LETTER**

**FROM FBI OFFICE OF CONGRESSIONAL AFFAIRS  
TO SENATE COMMITTEE ON THE JUDICIARY**



U.S. Department of Justice

Federal Bureau of Investigation

---

Washington, D. C. 20535-0001

November 25, 2005

Honorable Arlen Specter  
Chairman  
Committee on the Judiciary  
United States Senate  
Washington, DC 20510

Dear Mr. Chairman:

I am writing in response to a letter dated September 16, 2005 from Senator Feingold on behalf of the Subcommittee on the Constitution, Civil Rights and Property Rights seeking information in support of the Subcommittee's oversight activity relating to recent reviews by the Government Accountability Office (GAO) of government-wide data mining projects. Senator Sununu joined in Senator Feingold's letter.

Enclosed is relevant information concerning the FBI data mining efforts referenced in the GAO reports. If the Committee has additional questions that are not addressed in the enclosed materials, we will work with your staff to schedule a briefing by appropriate FBI officials.

Please do not hesitate to contact this office if we can be of assistance regarding this or any other matter.

Sincerely yours,

Eleni P. Kalisch  
Assistant Director  
Office of Congressional Affairs

Enclosure

Honorable Patrick J. Leahy  
Ranking Member  
Committee on the Judiciary  
United States Senate  
Washington, DC 20510

Honorable Arlen Specter

Honorable Sam Brownback  
Chairman  
Subcommittee on the Constitution, Civil  
Rights and Property Rights  
Committee on the Judiciary  
United States Senate  
Washington, DC 20510

Honorable Russell D. Feingold  
Ranking Member  
Subcommittee on the Constitution, Civil  
Rights and Property Rights  
Committee on the Judiciary  
United States Senate  
Washington, DC 20510

Honorable John E. Sununu  
United States Senate  
Washington, DC 20510

## **The Federal Bureau of Investigation's Foreign Terrorist Tracking Task Force, Investigative Data Warehouse, and Intelligence Community Data Marts**

The Government Accountability Office's (GAO) May 2004 report addresses three FBI programs: the Foreign Terrorist Tracking Task Force (FTTTF), Investigative Data Warehouse (IDW) (which is the successor to the Secure Collaborative Operational Prototype Environment (SCOPE)), and Intelligence Community Data Marts (ICDM). The August 2005 GAO report further focused on the efforts of the FTTTF to locate foreign terrorists and their supporters in the United States. While the term "data mining" has been defined in various ways, the FBI typically uses this term to mean "advanced analysis" or the ability to work with large amounts of data quickly and in ways that were previously not possible computationally due to size or speed limitations. The FBI uses the FTTTF, IDW, and ICDM to search multiple sources for information in support of the FBI's mission of analyzing intelligence in order to detect terrorist activity. All three programs can be used to conduct "criterion" searches, in which they search for all entries that meet multiple criteria (including such criteria as names and other personal identifiers).

### FTTTF

The mission of the FTTTF is to provide to law enforcement and intelligence community agencies information that helps keep foreign terrorists and their supporters out of the United States or that leads to their location, surveillance, detention, prosecution, or removal. The FTTTF uses data mining tools to search large amounts of data, including open-source data, to provide law enforcement and intelligence partners with actionable intelligence. FTTTF analysts and others in the FBI access commercial databases only in accordance with applicable Attorney General Guidelines to search for information about individuals and groups in whom the FBI has a valid investigative interest. Information developed by the FTTTF is forwarded through the National Joint Terrorism Task Force to the Joint Terrorism Task Forces (JTTFs) for follow-up.

While the FTTTF searches data maintained by both government and commercial sources under appropriate circumstances, with only one exception it uploads into FBI systems (or "ingests") only government data sets. Some of these government data sets are acquired on a one-time basis and others are acquired periodically as they are updated by the originator. In all cases, the acquisition of a government data set is based on specific operational needs. Although the FTTTF does not ingest entire commercial data sets (with one exception, as noted below), it does have access to information held and maintained by commercial data providers pursuant to agreements with these providers. The FTTTF accesses this commercially available data remotely through specific queries, ingesting only the results of the query for purposes of analysis. The one commercial data set ingested by the FTTTF, which was added to the FTTTF due to the technical



limitations of the provider's system, consists of name, telephone number, and address information (i.e., an electronic telephone book).

The nature of a database query will depend on the information available at the time of the query. For example, if the FTTTF were to receive an appropriate request from a law enforcement or intelligence agency for information about one or more named individuals suspected of being foreign terrorists traveling within the United States, those names would be run through the FTTTF system and appropriate commercial data sources to obtain information on the individuals. If, instead, the FTTTF were to receive a proper request to search only information as to age, gender, country of birth, citizenship, and a specific travel pattern during a given time frame, a query would be conducted against only government databases to narrow the inquiry to specific names or personal identifiers. The search results from these government databases (a list of names or personal identifiers) could then form the basis for a query against appropriate commercial sources.

FBI investigators do not base actions or investigative conclusions on a sole fact obtained from a database. Instead, they use information obtained from both internal and external data sources as pieces of information, or "building blocks," that assist them in developing a complete investigative picture. For example, if an investigator needs information in the possession of a certain John Brown, a database may be used to locate Mr. Brown, to distinguish this John Brown from others with the same name, or even to develop questions to be used in interviewing Mr. Brown, but the database information alone would not provide a basis for arrest or similar actions. The FTTTF reduces false positive identifications through a thorough vetting protocol that is external to the FTTTF data system, pursuant to which all query results are reviewed and analyzed by highly skilled analysts. The resulting analyses are provided to operational law enforcement and national security investigators as "leads"; that is, as information those investigators can use to develop additional, actionable information. For this reason, while it is important that the FBI have access to accurate information in order to develop effective investigative strategies, investigative conclusions are not based solely on database search results.

The use of FBI data mining systems must comport with applicable Attorney General Guidelines for criminal and intelligence investigations, which permit searches for information about individuals and groups in whom the FBI has a valid investigative interest. FTTTF systems have been certified and accredited in accordance with FBI policy, and training ensures users are familiar with the appropriate usage of these systems. The FTTTF's combined access to Department of Homeland Security border information, information provided by other government agencies, FBI investigative data, and commercially available information (such as public-source data) has enabled it to evaluate more than 60,000 individuals for associations with terrorism since January 2005, resulting in the provision of more than 100 leads to JTTFs.

Section 208 of the E-Government Act of 2002, Public Law 107-347, requires that agencies conduct Privacy Impact Assessments (PIAs) for information technology systems that collect, maintain, or disseminate identifiable information regarding individuals, but exempts

national security systems from the PIA requirement. While the FTTTF system is a national security system, and is therefore exempt from the section 208 PIA requirement, FBI PIA guidelines require that a PIA be completed for any new system that collects, maintains, or disseminates information about individuals, and do not exempt national security systems. A PIA has, consequently, been conducted for the FTTTF system pursuant to these FBI PIA guidelines. The PIA incorporates the requirements of both section 208 and the implementing Office of Management and Budget (OMB) guidelines. Just as section 208 does not require that PIAs be conducted for national security systems, its requirement for publication of the PIA is also inapplicable to national security systems.

The FBI has made substantial progress implementing GAO's August 2005 recommendations. The FTTTF has applied information security measures, obtaining the Security Division's "authorization to operate," and is developing and testing a contingency plan in preparation for certification and accreditation in accordance with national security standards. In addition, as noted above, the FBI has conducted a PIA, as required by FBI PIA guidelines, incorporating the requirements of Section 208 of the E-Government Act of 2002 and OMB's implementing guidelines. Pursuant to FBI PIA guidelines, the FTTTF system has been reviewed and approved by the FBI's Senior Privacy Official acting in conjunction with the FBI's Privacy Council. While the FTTTF system is a national security system and is, therefore, exempt from the publication requirements of the E-Government Act, the FBI is reviewing the circumstances under which it might make this information available to the public while protecting classified and other law enforcement sensitive information.

### IDW

As a consequence of the terrorist attacks of September 2001, the FBI identified the need to develop tools that could serve broader FBI investigative needs by accessing myriad data sources previously not readily available using conventional software tools. SCOPE was the initial prototype effort designed to support counterterrorism initiatives. The SCOPE prototype succeeded in enhancing FBI investigative and analytical capabilities, and it soon became a key asset for nearly 500 FBI operational users. Subsequently, the IDW project was initiated, building upon the successes of the SCOPE prototype and extending its operational capabilities to a larger number of users.

The IDW program's mission is to provide a one-stop shop through which agents and analysts can develop investigative leads from a variety of data sources related to counterterrorism, counterintelligence, cyber, and criminal investigations. This information includes numerical data, text, graphics, illustrations, imagery, photos, audio, and video that can be accessed in near real time using a single web-based interface that operates independent of the location of the user and the data source. Before the development of IDW, the same information was accessible, but it had to be acquired through stand-alone, individual sources and manually aggregated. The IDW includes security features that facilitate the sharing of data among

authorized users (while preventing unauthorized access) and the auditing of users' activities to detect rogue users.

IDW is used to search only data sets that have been ingested into IDW. These data sources include primarily FBI and other government information, such as information provided by the Departments of Justice, Homeland Security, State, and Treasury, but they also include some open-source newspaper articles related to counterterrorism. IDW is not used to search outside data, including outside public-source information maintained in commercial data bases. IDW is designed to consolidate the information obtained through these searches into reports that can be disseminated for operational use both within the FBI and to appropriate outside federal, state, and local agencies.

As indicated with respect to the FTTTF, FBI PIA guidelines require that a PIA be completed for any new system that collects, maintains, or disseminates information about individuals, and a PIA has been conducted for IDW. The use of FBI data mining systems must also comport with applicable Attorney General Guidelines for criminal and intelligence investigations, which permit searches for information about individuals and groups in whom the FBI has a valid investigative interest, and IDW has been certified and accredited in accordance with FBI policy.

#### ICDM

While the ICDM was only in the planning stages when the May 2004 GAO report was drafted, elements of this initiative have since been deployed. The ICDM builds on the tools in IDW and uses IDW as a data source, searching a subset of IDW information. As is true with respect to IDW, ICDM does not query commercial databases. ICDM will operate both internally (working with real-time intelligence feeds in support of FBI analysts) and externally (sharing FBI intelligence products with appropriate agencies), providing for the near real-time provision of relevant data to analysts based on areas of interest and alerting recipients to high-priority incoming information. ICDM will link directly to IDW and provide a common web-based portal work environment, supporting queries to other databases as one means of reducing the problems inherent in stovepipe systems. Currently, ICDM is being used internally by select FBI analysts as part of the FBI Automated Messaging System. Externally, ICDM currently supports direct web-based access to other agencies' classified systems, including the Secret Internet Protocol Router Network and the secret-level INTELINK system, from any FBINET workstation. Both the internal and external ICDM systems are undergoing Operational Readiness Review and are expected to transition to full operations near the end of 2005.

As with both the FTTTF and the IDW, a PIA has been conducted for the ICDM and the ICDM has been certified and accredited in accordance with FBI policy.