U.S. Department of Justice

Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

May 13, 2003

The Honorable F. James Sensenbrenner, Jr.
Chairman
Committee on the Judiciary
U.S. House of Representatives
Washington, D.C. 20515

Dear Mr. Chairman:

Thank you for your letter of April 1, 2003, co-signed by Ranking Member Conyers, which posed several questions to the Department on USA PATRIOT Act implementation and related matters. An identical response will be sent to Congressman Conyers.

Pursuant to your request, on April 9, 2003, we notified the Committee that we had forwarded questions number 18, 19, 22, 23, 24, 31, 32 and 26, relating to the authority or operations of the Immigration and Naturalization Service, to the Department of Homeland Security for response. With this letter, we are pleased to transmit responses to the remaining questions.

While we have made every effort to answer each question thoroughly and in an unclassified format, four of the questions will require the submission of classified information. The answer to a portion of question 16(a), and questions 30 and 37 are classified and will be delivered to the Committee under separate cover. In accordance with the direction provided in the Committee's letter of April 1, 2003, and the longstanding Executive branch practices on the sharing of operational intelligence information with the Congress, the classified answers to question 1(c), and a further portion of question 16(a), will be delivered to the House Permanent Select Committee on Intelligence.

We appreciate the opportunity to provide the Committee with information on the Department's efforts in the war on terrorism. If we may be of further assistance on this, or any other matter, please do not hesitate to contact this office.

Sincerely,

Jamie E. Brown
Acting Assistant Attorney General

Enclosures

U.S. Department of Justice

Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

May 13, 2003

The Honorable John Conyers, Jr.
Ranking Minority Member
Committee on the Judiciary
U.S. House of Representatives
Washington, D.C. 20515

Dear Congressman Conyers:

Thank you for your letter of April 1, 2003, co-signed by Chairman Sensenbrenner, which posed several questions to the Department on USA PATRIOT Act implementation and related matters. An identical response will be sent to Chairman Sensenbrenner.

Pursuant to your request, on April 9, 2003, we notified the Committee that we had forwarded questions number 18, 19, 22, 23, 24, 31, 32 and 26, relating to the authority or operations of the Immigration and Naturalization Service, to the Department of Homeland Security for response. With this letter, we are pleased to transmit responses to the remaining questions.

While we have made every effort to answer each question thoroughly and in an unclassified format, four of the questions will require the submission of classified information. The answer to a portion of question 16(a), and questions 30 and 37 are classified and will be delivered to the Committee under separate cover. In accordance with the direction provided in the Committee's letter of April 1, 2003, and the longstanding Executive branch practices on the sharing of operational intelligence information with the Congress, the classified answers to question 1(c), and a further portion of question 16(a), will be delivered to the House Permanent Select Committee on Intelligence.

We appreciate the opportunity to provide the Committee with information on the Department's efforts in the war on terrorism. If we may be of further assistance on this, or any other matter, please do not hesitate to contact this office.

Sincerely,

Jamie E. Brown

Jamie E. Brown
Acting Assistant Attorney General

Enclosures

USA PATRIOT Act

1. Section 215 of the Act amended 50 U.S.C. § 1861 to allow the FBI Director or his designee (who must hold the rank of Assistant Special Agent in Charge or higher) to apply for an order from the Foreign Intelligence Surveillance Court for "the production of tangible things (including books, records, papers, documents, and other items) for an investigation to protect against international terrorism or clandestine intelligence activities . . . ." Such an investigation may only be conducted under guidelines approved by the Attorney General under Executive Order 12333 (or a successor order). 50 U.S.C. § 1861(a)(2)(A).

A. What guidelines has the Attorney General approved under Executive Order 12333 or a successor order for the conduct of such investigations?

Answer: These investigations are conducted under the Attorney General Guidelines for FBI Foreign Intelligence Collection and Foreign Counterintelligence Investigations, which were approved pursuant to Executive Order 12333.

B. Before such an order can be sought, do the guidelines require that the FBI have already established probable cause that a person under investigation is an agent of a foreign power? What is the Department's definition of "probable cause" and how has it changed since September 11, 2001?

Answer: The Department does not have the authority to define "probable cause"; it is a statutory and constitutional term. Except where a statute has been amended, the term has not changed meaning since September 11, 2001.

Section 215 of the USA PATRIOT Act (Act) added the current version of 50 U.S.C. § 1861 to the Foreign Intelligence Surveillance Act (FISA). In order to obtain business records, section 1861(b)(2) requires the Department to demonstrate to the Foreign Intelligence Surveillance Court (FISC) that the records are sought "for an investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution." The Guidelines do not impose a probable cause requirement over and above the requirements Congress set forth in the statute.

Congress did not authorize a new innovation with section 215. Grand juries investigating ordinary crimes traditionally have had the power to issue subpoenas to all manner of businesses, including libraries and bookstores. For example, in

the so-called Unabomber investigation of the mid-1990s, federal grand juries subpoenaed library records at Brigham Young University, the University of Utah, Northwestern University, the University of California, the University of Montana, and the Missoula County Library in order to determine who had checked out the four books cited in the "Unabomber Manifesto." Section 215 simply provided that this investigative tool is also available for foreign intelligence and terrorism investigations.

Importantly, section 215 of the USA PATRIOT Act imposes more restrictions on its use than a federal grand jury subpoena for the same records. First, a court must explicitly authorize the use of section 215 to obtain business records. By contrast, a grand jury subpoena is issued on the authority of the district court and clerk of the court but without any prior judicial review or approval. Second, section 215 contains explicit safeguards for activities protected by the First Amendment, unlike federal grand jury subpoenas. And, third, as noted above, section 215 requires, for an investigation relating to a U.S. person, that the information be sought in an investigation to protect against international terrorism or clandestine intelligence activities. By contrast, a federal grand jury can obtain business records whenever such records are relevant to a grand jury investigation of any federal crime. *See generally United States v. R. Enterprises., Inc.,* 498 U.S. 492 (1991).

C. Please produce all guidelines approved under Executive Order 12333 or a successor order for the conduct of such investigations.

Answer: These guidelines are classified at the Secret level. Under section 3.3 of Executive Order 12333, the Guidelines "shall be made available to the congressional intelligence committees." As required, we have provided the House Permanent Select Committee on Intelligence (HPSCI) with the Guidelines, and, pursuant to the Committee's April 1, 2003, letter, we will provide HPSCI with another copy for the review of the House Committee on the Judiciary.

2. Such investigations also may not be conducted of a United States person solely on the basis of activities protected by the First Amendment to the Constitution of the United States. 50 U.S.C. § 1861(a)(2)(B). Other authorities under the Foreign Intelligence Surveillance Act ("FISA") are also subject to the limitation that an investigation of a United States person in which those authorities are used may not be conducted solely on the basis of activities protected by the First Amendment to the U.S. Constitution. See, e.g., 50 U.S.C. § 1842 (regarding pen register and trap and trace orders under FISA).

A. In seeking such orders, does the government make an explicit certification that an investigation of a United States person is not being conducted solely

on the basis of activities protected by the First Amendment to the Constitution of the United States?

Answer: 50 U.S.C. § 1842(c)(2) requires that an application for a pen register or trap and trace device include a certification "that the information likely to be obtained is foreign intelligence information not concerning a United States person or is relevant to an ongoing investigation to protect against intemational terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the First Amendment to the Constitution." Accordingly, applications concerning United States persons made under this section include a certification by a Department attorney that the investigation of a United States person is not being conducted solely upon the basis of activities protected by the First Amendment.

50 U.S.C. § 1861(b)(2) requires that each application for access to certain business records "shall specify that the records concerned are sought for an authorized investigation in accordance with subsection (a)(2) to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities." Section 1861(a)(2)(B) requires that an investigation under this section of a United States person not be conducted solely upon the basis of activities protected by the First Amendment to the Constitution. Section 1861 does not require that an application concerning a United States person make an explicit certification that the investigation is not being conducted solely on the basis of activities protected by the First Amendment.

B. In issuing such orders, does the court make an express finding that an investigation of a United States person is not being conducted solely on the basis of activities protected by the First Amendment to the Constitution of the United States?

Answer: With respect to orders for a pen register or trap and trace device, 50 U.S.C. § 1842(d)(1) states that "[u]pon application made pursuant to this section, the judge shall enter an ex parte order as requested, or modified, approving the installation and use of a pen register or trap and trace device if the judge finds that the application satisfies the requirements of this section." The statute does not require the FISC to make an express finding that the investigation of a United States person is not being conducted solely on the basis of activities protected by the First Amendment of the Constitution of the United States. However, the judge may approve the application only if he or she finds that the application satisfies all the requirements of the section 1842, and -- as noted above -- section 1842(c)(2) provides that the application shall include a certification that investigation of a United States person is not being conducted solely upon the basis of activities

protected by the First Amendment.

With respect to orders for access to certain business records, 50 U.S.C. § 1861(c)(1) provides that "[u]pon application made pursuant to this section, the judge shall enter an ex parte order as requested, or as modified, approving the release of records if the judge finds that the application meets the requirements of this section." The statute does not require the FISC to make an express finding that the investigation of a United States person is not being conducted solely on the basis of activities protected by the First Amendment of the Constitution of the United States. However, the judge may approve the application only if he or she finds that the application satisfies all the requirements of the section 1861, and -- as noted above -- section 1861(a)(2)(B) requires that an investigation not be conducted of a United States person solely upon the basis of activities protected by the First Amendment to the Constitution of the United States.

3. The Department has increased the use of "national security letters" that require businesses to turn over electronic records about finances, telephone calls, e-mail and other personal information.

A. Please identify the specific authority relied on for issuing these letters.

Answer: Congress has authorized the issuance of National Security Letters in 12 U.S.C. § 3414(a)(5) (the Right to Financial Privacy Act); 15 U.S.C. §§ 1681u and 1681v (the Fair Credit Reporting Act); 18 U.S.C. § 2709 (the Electronic Communications Privacy Act); and 50 U.S.C. § 436(a) (relating to records of persons with authorized access to classified information, who may have disclosed that information to a foreign power).

B. Has any litigation resulted from the issuance of these letters (i.e. challenging the propriety or legality of their use)? If so, please describe.

Answer: There has been no challenge to the propriety or legality of National Security Letters.

4. Has any administrative disciplinary proceeding or civil action been initiated under section 223 of the Act for any unauthorized disclosure of certain intercepts? If so, please describe each case, the nature of the allegations, and the current status of each case.

Answer: There have been no administrative disciplinary proceedings or civil actions initiated under section 223 of the Act for unauthorized disclosures of intercepts.

5. In the Administration's 2004 Budget Request, DOJ is requesting $22 million to

establish an automated cross-case analytical system to facilitate sharing case specific information through the agencies that belong to the Organized Crime Drug Enforcement Task Force Program. These include law enforcement agencies in DOJ, the Department of Homeland Security, and the Department of Treasury. Is this system also intended to facilitate implementation of the authority to share criminal investigative information with intelligence officials under Section 203 of the Act? Will it be used for that purpose?

Answer: The Department's 2004 budget request is specifically intended to establish and support a central warehouse for drug investigative information and to enable the Organized Crime Drug Enforcement Task Force (OCDETF) and its member agencies to undertake cross-case analysis of that drug information. However, the system may indirectly facilitate or enhance efforts to share investigative information with intelligence officials. In particular, the proposed system would be co-located with the Foreign Terrorist Tracking Task Force (FTTTF), not only enabling OCDETF to leverage FTTTF's existing technology and analytical tools, but also enabling FTTTF, as appropriate, to extract relevant drug investigative information. To the extent such information included foreign intelligence information, FTTTF would certainly ensure that the information was shared in accordance with the Act and the Attorney General's September 23, 2002, Guidelines Regarding Disclosure to the Director of Central Intelligence and Homeland Security Officials of Foreign Intelligence Acquired in the Course of a Criminal Investigation. In addition, the proposed system will likely utilize the Special Operations Division (SOD) as a clearinghouse for the distribution of tips and leads to the field. Given that SOD already has established protocols for the identification and dissemination of foreign intelligence information, such protocols certainly would be applied to any intelligence gained from the data warehouse.

6. **What has been the role of the Department in establishing standards or procedures regarding implementation of the authorities provided in Section 358 (Bank Secrecy Provisions and Activities of United States Intelligence Agencies to Fight International Terrorism)? Please provide any written guidance regarding the requirements of that section that the Department has either issued or approved.**

Answer: The Department of Justice has not been involved in establishing standards or procedures regarding implementation of the authorities provided in section 358. Nonetheless, criminal investigations of terrorism violations in which the Department is involved -- such as violations of 18 U.S.C. §§ 2339A and 2339B, which prohibit providing material support or resources either to terrorists or to designated foreign terrorist organizations -- have substantially benefitted from section 358, which allows financial regulators to share certain financial information related to terrorism with intelligence and criminal investigators.

7. **What are the dollar amounts that have been paid under the reward authorities provided in Section 501 of the Act or the terrorism related awards under the newly**

enacted 28 U.S.C. § 530(C)(b)(1)(J)? How many non-U.S. citizens have received rewards under these authorities?

Answer: As of April 30, 2003, the Department of Justice has provided a total of $245,000.00 in reward payments, as tracked in its accounting records (1997-2002). Current financial data does not capture these reward payments by a particular statute, nor does it delineate the citizenship of the recipients. The information that is currently available can only provide us the amount paid, and the time period in which it was paid. However, the financial data indicates that there have been no reward payments made in the last 2 years and hence the data tells us that there are currently no known rewards paid under the newly enacted 28 U.S.C. § 530C(b)(1)(J).

8. **The Administration's Office of Justice Programs 2004 Budget request includes a $12 million increase for Regional Information Sharing System (RISS) improvements. The request refers to Section 701 of the USA PATRIOT Act and states that the requested increase will be used to expand RISS's accessibility to state and local public safety agencies to share terrorism alerts and related information. Please provide the Committee with a description of the management oversight process by which DOJ will ensure that the proposed expenditures will accomplish improvements in the U.S. information infrastructure and the specific improvements that are envisioned. Please provide copies of any guidance issued to state and local agencies with respect to the further dissemination of such materials.**

Answer: Currently, 84 United States Attorneys Offices (USAOs) are using the Regional Information Sharing Systems Program (RISS.net) as a method to communicate with the Department's state and local law enforcement partners. In the USAOs, there are nearly 600 "Access Officers" of RISS.net. These users typically include the Anti-Terrorism Task Force Coordinators, Counterterrorism Attorneys, OCDETF Attorneys, Intelligence Analysts, and Law Enforcement Coordinating Committee Coordinators. Additionally, in many districts the United States Attorney, First Assistant United States Attorney, and Criminal Chief also utilize the RISS System. The Department expects the remaining USAOs to be fully vetted for RISS in the very near future.

The RISS Program is funded, managed and monitored by the Bureau of Justice Assistance (BJA) of the Office of Justice Programs (OJP). Each of the six projects is monitored on an annual basis by BJA program staff and the OJP Office of General Counsel (OGC). The OGC monitoring focuses on compliance with the "Criminal Intelligence Systems Operating Policies," which are designed to ensure that information in the system is relevant, updated, and based on a reasonable suspicion of criminal activity.

While this level of monitoring and oversight will continue, we intend to refine our focus to ensure that the enhancements to the RISS.net system are responsive to the need for expansion, both with respect to terrorism and to the broader public safety audience

envisioned in the USA PATRIOT Act. We are working very closely with the Department of Homeland Security (DHS), both at the Chief Information Officer level and with the Information Analysis and Infrastructure Protection Directorate (IA&IP), to ensure that the RISS infrastructure enhancements are consistent with the statutory authorities and responsibilities of DHS.

In addition, BJA's overall information technology (including RISS) is, in large measure, guided by the Global Justice Information Sharing Initiative, a Federal Advisory Committee made up of State and local constituency organizations that reports to the Attorney General, and Global's Intelligence Working Group, comprised of Federal, State and local intelligence officials and information sharing specialists. Specifically, RISS-ATIX is the improvement to the U.S. information infrastructure envisioned in this regard, and we are already working with DHS to provide an architecture that will provide for an effective two-way exchange of information between State and local law enforcement, public safety and other first responder agencies, and organizations and officials at DHS.

9. Under section 213 of the USA PATRIOT Act, a court may order a delay in any notice of the execution of a search warrant if "the court finds reasonable cause to believe that providing immediate notification of the execution of the warrant may have an adverse result," which is defined as (1) endangering the life or physical safety of an individual; (2) flight from prosecution; destruction or tampering with evidence; (3) intimidation of potential witnesses; or (4) otherwise seriously jeopardizing an investigation or unduly delaying trial. Please respond to the following questions regarding the use of this authority:

A. How many times has the Department of Justice sought an order delaying notice of the execution of a warrant under this section?

Answer: Whenever Justice Department personnel execute a court-issued search warrant, they always provide required notice to the person whose property has been searched. But in some cases – *e.g.*, when it is necessary to protect human life, or to avoid compromising an investigation – federal law authorizes the Department to delay giving notice for short periods of time.

The Department has had the legal authority to delay giving notice that a warrant had been executed since before the USA PATRIOT Act. But the law was a mix of inconsistent rules, practices, and court decisions that varied widely from jurisdiction to jurisdiction across the country. This lack of uniformity hindered terrorism cases and other complex nationwide investigations.

Section 213 of the USA PATRIOT Act resolved this problem by establishing a uniform statutory standard. Now, a court can delay the required provision of notice if it finds "reasonable cause" to believe that immediate notification may have an adverse result as defined by 18 U.S.C. § 2705 (including endangering the

life or physical safety of an individual, flight from prosecution, evidence tampering, witness intimidation, or otherwise seriously jeopardizing an investigation or unduly delaying a trial). The section requires that notice be provided within a "reasonable period" of a warrant's execution, and a court can further extend the period for good cause.

Section 213's "reasonable cause" standard is in accord with prevailing caselaw for delayed notice of warrants before the USA PATRIOT Act. *See, e.g., United States v. Villegas*, 899 F.2d 1324, 1337 (2d Cir. 1990) (government must show "good reason" for delayed notice of warrants). It also is consistent with the exceptions to the general rules that agents must "knock and announce" before entering, and that warrants must be executed during the daytime. *See Richards v. Wisconsin*, 520 U.S. 385 (1997) (no-knock entry to execute warrant is justified when the police have "reasonable suspicion" that knocking and announcing their presence would be dangerous or futile or would inhibit the effective investigation); Fed. R. Crim. P. 41(c)(1) ("The warrant shall be served in the daytime unless the issuing authority, by appropriate provision of the warrants, and for reasonable cause shown, authorizes its execution at times other than daytime.").

As of April 1, 2003, the Department of Justice has requested a judicial order delaying notice of the execution of a warrant under section 213 forty-seven times, and the courts have granted every request.

B. How many times has a court ordered the delay in such notification?

Answer: As of April 1, 2003, courts have ordered the delay in such notification each of the forty-seven times requested by the Department.

10. That same section allows the notice to be delayed when the warrant prohibits the seizure of among other things, any tangible property, unless "the court finds reasonable necessity for the seizure." 18 U.S.C. § 3103a (b)(2).

A. Since the enactment of that section, how many times has the government asked a court to find reasonable necessity for a seizure in connection with delayed notification under this section?

Answer: Whenever Justice Department personnel execute a court-issued warrant authorizing the seizure of property, the Department provides required notice to the person whose property was seized. In some highly sensitive cases, however, it is necessary that courts be able to authorize a temporary delay in giving that notice.

Section 213 of the USA PATRIOT Act is designed primarily to allow courts to authorize delayed notice of *searches*. But it also enables courts, in certain narrow circumstances, to authorize delayed notice of *seizures*. Section 213 expressly

requires that any warrant issued under it must prohibit the seizure of any tangible property, any wire or electronic communication, or (except as expressly provided in chapter 121) any stored wire or electronic information. Courts can waive this requirement only if they find "reasonable necessity" for the seizure.

As of April 1, 2003, the government has asked a court to find reasonable necessity for a seizure in connection with delayed notification under this section fifteen times, and the courts have granted fourteen of the requests.

B. On what grounds has the government argued that seizure was reasonably necessary under a warrant for which the government also asked for delayed notification?

Answer: The government has argued that seizure was necessary: (1) to prevent jeopardizing the investigation by protecting the safety of confidential informants; (2) to prevent compromising an investigation by preventing the removal or destruction of evidence; and/or (3) to seize controlled substances that are inherently dangerous to the community.

C. How often has a court found "reasonable necessity for the seizure" in connection with a warrant for which it also permitted delayed notification?

Answer: As of April 1, 2003, a court has found reasonable necessity for the seizure in connection with a warrant for which it also permitted delayed notification fourteen times.

D. How often has a court rejected the government's argument that a seizure was reasonably necessary in connection with a warrant for which the government sought delayed notification?

Answer: As of April 1, 2003, a court once has rejected the government's argument that a seizure was reasonably necessary. In that one instance, the government requested a delayed-notice warrant to permit federal agents to check a storage unit that was believed to contain information concerning credit card fraud, false identification documents, and other such material. The government also sought authority to seize the items discovered to prevent their possible destruction or removal. The court authorized the warrant but did not authorize seizure because it believed that photographs of relevant items in the storage unit would be sufficient.

E. On what grounds have the courts found that the seizures were reasonably necessary in connection with warrants for which delays in notification were granted?

Answer: The courts have found that the seizures were necessary: (1) to prevent jeopardizing the investigation by protecting the safety of confidential informants; (2) to prevent compromising an investigation by preventing the removal or destruction of evidence; and/or (3) to seize controlled substances that are inherently dangerous to the community.

F. What grounds have the courts rejected as establishing reasonable necessity for a seizure in connection with a warrant for which the government sought delayed notification?

Answer: In the one instance, the government requested a delayed-notice warrant to permit federal agents to check a storage unit that was believed to contain information concerning credit card fraud, false identification documents, and other such material. The government also sought authority to seize the items discovered to prevent their possible destruction or removal. The court authorized the warrant but did not authorize seizure because it believed that photographs of relevant items in the storage unit would be sufficient.

11. That same section allows a court to order delayed notice when "the warrant provides for the giving of such notice within a reasonable period of its execution, which may be extended for by the court for good cause show." 18 U.S.C. § 3103a(b)(3).

A. What are the shortest and longest periods of time for which the government has requested initial delayed notice?

Answer: The most common period of delay authorized by courts is seven days. Courts have authorized specific delays of notification as short as one day and as long as ninety days; other courts have permitted delays of unspecified duration lasting until the indictment was unsealed.

B. On what grounds has the government argued that the period of delayed notification was reasonable?

Answer: The government has argued that the delay period was reasonable in light of the need: (1) to protect the physical safety of cooperators, confidential sources and informants; (2) to prevent the harassment or intimidation of witnesses; (3) to prevent compromising an investigation, which may cause the subject to flee; and/or (4) to prevent the removal or destruction of evidence by avoiding disclosure of the scope and nature of the investigation.

C. How often has the government sought an extension of the period of delayed notice?

Answer: As of April 1, 2003, the government has sought an extension of the period of delayed notice 248 times. This number includes multiple extensions for a single warrant. For example, if a court authorizes a delay of notification for seven days and the investigation lasts one month, the government might seek four renewals.

D. On what grounds has the government asked for an extension of the period of delayed notice?

Answer: The government has sought extensions of the delayed notice period: (1) to permit the imminent arrest of subjects; (2) to protect the physical safety of confidential sources and informants; (3) to prevent the harassment or intimidation of witnesses; (4) to prevent jeopardizing undercover investigations; (5) to prevent compromising an investigation, which may cause the subject to flee; and/or (6) to prevent the removal or destruction of evidence by avoiding disclosure of the scope and nature of the investigation.

E. How often has a court rejected the government's request for delayed notification on the ground that the period for giving delayed notice was unreasonable?

Answer: As of April 1, 2003, a court has never rejected the government's request for delayed notification on the ground that the period for giving delayed notice was unreasonable.

F. On what grounds have the courts rejected the government's position that the period for giving delayed notice was reasonable?

Answer: As of April 1, 2003, no court has rejected such a request.

G. How often has a court rejected the government's request for an extension of the period of delayed notification?

Answer: As of April 1, 2003, no court has rejected such a request.

H. On what grounds have the courts rejected the government's argument that an extension of the period for delayed notice was reasonable?

Answer: As of April 1, 2003, no court has rejected such a request.

12. On January 21, 2003, the *Wall Street Journal* published an article entitled "New Powers Fuel Legal Assault on Suspected Terrorists." That article claims that the Department of Justice is using information that was "previously largely unavailable" and that had been obtained from FISA surveillance to support

criminal prosecutions. According to the article, this information is now available to prosecutors as a result of the FISA Review Court's decision regarding the meaning of the Act's amendment to FISA permitting the government to obtain a surveillance order when "a significant purpose," (rather than "the purpose") of the surveillance is to collect foreign intelligence.

A. Prior to the FISA Review Court's decision, as long as surveillance was properly ordered for "the purpose" of collecting foreign intelligence, was there any legal impediment to prosecution of a crime using evidence obtained under FISA?

Answer: Prior to the Foreign Intelligence Surveillance Court of Review's decision in *In re Sealed Case*, 310 F.3d 717 (2002), there was no legal impediment to the use of evidence obtained pursuant to FISA in a criminal prosecution. Under 50 U.S.C. §§ 1806 and 1825 as originally enacted, information properly obtained or derived from a lawful FISA search or surveillance could be used in a proceeding, including a criminal proceeding, with the approval of the Attorney General. There are published decisions of the federal Courts of Appeals in which such information was used in a criminal prosecution. *See*, *e.g.*, *United States v. Duggan*, 743 F.2d 59 (2d Cir. 1984).

While there was no *legal* impediment to introducing in a criminal prosecution evidence obtained through FISA before the USA PATRIOT Act and the decision of the Court of Review, as a *practical* matter such evidence was unavailable because of the metaphorical "wall" between law enforcement and intelligence activities. This wall – which derived from certain court decisions and administrative practice by the Department – prevented the sharing of information between, and coordination among, law enforcement and intelligence officials, thereby interfering with a comprehensive and effective defense of the national security against international terrorism and other threats. The wall – and how it was affected by the USA PATRIOT Act, revised Department guidelines issued in March 2002, and the Court of Review's decision – are described in the answer to Question 12(C).

B. Please identify all cases brought since the FISA Review Court's decision that use information that was previously unavailable under FISA procedures.

Answer: After enactment of the USA PATRIOT Act, and even prior to the Court of Review's decision, the Attorney General instructed all United States Attorneys to review intelligence files to determine whether there was a basis for proceeding criminally against subjects of intelligence investigations. This substantial effort represented an enhanced level of review by criminal prosecutors of national security investigative matters. The overall goal of the effort was to protect the Nation from further terrorist attacks by identifying evidence of felonies that had

been, or were about to be, committed.

On October 1, 2002, the Attorney General addressed the United States Attorneys and instructed each of them to develop a plan to monitor terrorism and intelligence investigations, and to ensure that information regarding any individual who poses a threat of terrorism to America is shared with other agencies and that appropriate criminal charges are considered.

Almost 4,500 intelligence files were considered as part of the review process and most of these files have been now been reviewed by a criminal prosecutor pursuant to the Attorney General's directive. Evidence or information from this review has been incorporated in numerous cases.

C. Please explain why such information was unavailable and why it became available following the FISA Review Court's decision.

Answer: Before the USA PATRIOT Act, the metaphorical "wall" between the intelligence community and federal law enforcement often precluded effective and indeed vital information sharing, perversely creating higher barriers in the most serious cases. This wall, which derived from certain court decisions, was established in written Department guidelines in July 1995. Sections 218 and 504(a) of the Act – as implemented by Department guidelines issued in March 2002 that were approved by the Court of Review in November 2002 – finally permitted the coordination between intelligence and law enforcement that is vital to protecting the Nation's security.

The wall between intelligence and law enforcement resulted from perceived differences between legal authorities that permit the Federal Bureau of Investigation (FBI) to engage in electronic surveillance in the course of its foreign counterintelligence function, on the one hand, and its law enforcement function on the other. These perceived differences created an artificial dichotomy between intelligence gathering and law enforcement, and FISA and Title III (which authorizes electronic surveillance in criminal cases).

As enacted in 1978, FISA required that "the purpose of electronic surveillance is to obtain foreign intelligence information," a term that was (and still is) defined to include information necessary to the ability of the United States to "protect" against espionage or international terrorism. *See* 50 U.S.C. §§ 1804 (a)(7)(B), 1801(e). Courts interpreted "the purpose" to mean "the primary purpose," and they interpreted "foreign intelligence information" to include information necessary to the ability of the United States to protect against espionage or international terrorism *using methods other than law enforcement*. Thus, according to this judicial interpretation of FISA, that statute could be used only if the primary purpose of surveillance or a search was the protection of national

security using non-law enforcement methods; gathering evidence to support the prosecution of a foreign spy or terrorist could be a significant purpose of the surveillance or search, but only if that prosecutorial purpose was clearly secondary to the non-law enforcement purpose. As a practical matter, courts determined the government's purpose for using FISA by examining the degree of coordination between intelligence and law enforcement officials: the more information and advice exchanged between these officials, the more likely courts would be to find that the primary purpose of the surveillance or search was law enforcement, not intelligence gathering. This legal structure created what the Court of Review termed "perverse organizational incentives," expressly discouraging coordination in the fight against terrorism. *In re Sealed Case*, 310 F.3d at 743.

To maintain the ability to present viable FISA applications under this perceived legal standard, the Justice Department issued written guidelines in July 1995 that limited the contacts between Department personnel involved in foreign intelligence collection and those involved in law enforcement. This wall between intelligence and law enforcement allowed for intelligence information – including information developed from FISA-approved methods – to be shared with prosecutors and criminal investigators only where such information established that a crime "has been, is being, or will be committed." In such circumstances, the intelligence officials could seek approval to "throw information over the wall." The decisions on when to take this action, however, resided *solely* with intelligence officials.

This policy proved to be wholly unworkable, as it entrusted the decision whether to share information with those who were not best positioned to apply the applicable standards. Only the law enforcement agents and prosecutors pursuing a particular criminal investigation can determine what evidence is pertinent to their case. In contrast, intelligence officials, who focus on the development of foreign intelligence for national security purposes rather than collecting and reviewing information for a particular criminal investigation, rarely consider the potential evidentiary value of a particular piece of information, unless such information self-evidently proves that a crime has been, or may be, committed. Thus, as a matter both of perceived legal imperative and of Department culture, it was impossible to permit full coordination between intelligence and law-enforcement personnel and to combine foreign intelligence and law enforcement information into a seamless body of knowledge. Indeed, law enforcement and intelligence personnel could not speak openly to each and share information beyond the piecemeal sharing envisioned by the previously existing rules. As a result, sharing under these guidelines was relatively rare and generally not meaningful.

The reexamination of these perceived standards became more urgent after the September 11 attacks, when the Attorney General clarified that the Department's primary mission was the prevention of terrorist attacks before they occur. This

goal could not be achieved where personnel needed for key preventative tools (including criminal investigation and prosecution and immigration enforcement) did not have the full range of actionable intelligence, including information developed through FISA methods. The USA PATRIOT Act addressed this problem by making two changes to FISA. First, section 218 displaced the "primary purpose" standard, permitting the use of FISA when a "significant purpose" of the search or surveillance was foreign intelligence. Second, section 504(a) clarified that coordination between intelligence and criminal personnel was not grounds for denial of a FISA application.

Following enactment of the USA PATRIOT Act, the Department promulgated new procedures dated March 6, 2002, that expressly authorized – and indeed required – coordination between intelligence and law enforcement. These revised procedures were rejected in part by the FISC on May 17, 2002, but were approved in full by the Court of Review on November 18, 2002. (The decisions of both courts are attached.)[1] In addition to confirming that the Department's revised procedures were valid under FISA, as amended by the USA PATRIOT Act, the Court of Review also noted that the judicial decisions and administrative actions that established the wall between intelligence and law enforcement were not even required by FISA *prior to* the amendments enacted by the USA PATRIOT Act. *See In re Sealed Case*, 310 F.3d at 723-27, 735. In December 2002, the Department issue field guidance with respect to the March 2002 procedures and the Court of Review's decision. (A copy of the field guidance is attached.)[2]

The enhanced ability to coordinate efforts and share information – permitted as a result of sections 218 and 504(a) of the USA PATRIOT Act, the Department's March 6, 2002 procedures, and the Court of Review's decision – has allowed the Department of Justice to investigate cases in a more orderly, efficient, and knowledgeable way, and has permitted all involved personnel, both law enforcement and intelligence, to discuss openly legal, factual, and tactical issues arising during the course of investigations. These substantive and procedural improvements have maximized the prospects that the option best calculated to protect the national security and the American people will be chosen in any individual case. In sum, the Department has developed counterterrorism tools and methods that plainly would not have been possible under the previous standards.

The recent indictment of Sami Al-Arian and other alleged members of a Palestinian Islamic Jihad (PIJ) cell in Tampa, Florida, illustrates a case that benefitted from the new standards. The allegations contained in the conspiracy indictment were based largely on electronic surveillance authorized pursuant to

[1]Attachments A and B.

[2]Attachment C.

FISA and conducted prior to the USA PATRIOT Act. Before the Act, the Department was required to submit repeated certifications that the primary purpose of the proposed surveillance methods was intelligence, as opposed to criminal law enforcement. Moreover, special handling procedures were imposed in this investigation on intelligence officials to guard against information sharing that was believed to be improper. On several occasions, information developed through FISA surveillance was identified as potentially relevant to a criminal case against Al-Arian and others, and the FBI's intelligence personnel notified the Criminal Division of this information. The Criminal Division duly disseminated this information to the U.S. Attorney in Tampa, as envisioned by the July 1995 rule. However, the existing protocols denied criminal prosecutors and investigators full access to information obtained through FISA, and they prevented criminal and intelligence personnel from coordinating their parallel investigations.

The USA PATRIOT Act's amendments to FISA and the new rules adopted by the Department pursuant to those amendments enabled criminal investigators in Tampa finally to obtain and systematically consider the full range of evidence of the alleged conspiracy. After the Court of Review's decision confirmed the Department's understanding of the Act, this information, which existed in the FBI's intelligence – but not criminal – files, became available and was examined. Armed with the entire intelligence yield, prosecutors for the first time were able to consider the comprehensive history of the surveillance of Al-Arian and others, to understand the context of their communications, and to document the decade-long conspiracy that is alleged. Such a comprehensive review and evaluation would not have been possible under the old rules. Thus, the USA PATRIOT Act was critical to the Department's ability to safeguard the Nation's security by bringing criminal charges against Al-Arian and others in February 2002.

In order to ensure that – as with the Al-Arian case – criminal investigators benefit from now-available intelligence information, after enactment of the USA PATRIOT Act the Attorney General directed that prosecutors review existing intelligence files to determine whether they contained evidence of crimes. This process, which is almost completed, involved the detailed review of almost 4,500 files. The Attorney General also directed, in October 2002, that each United States Attorney know fully the FBI's intelligence cases in their Districts. These efforts, along with coordination between law enforcement and intelligence personnel in ongoing investigations, have been made possible by the USA PATRIOT Act and are essential to preventing terrorism before it occurs and locating and prosecuting terrorists.

13. The FISA Review Court's decision permits enhanced coordination between law enforcement and intelligence officials.

A. What FISA-related training is currently being planned or conducted?

B. What topics will it address?

C. Who will give the training?

D. Who will receive the training?

E. Is the training going to be coordinated with the Intelligence Community in general and/or the Director of Central Intelligence?

Answer to A through E: In the past year, the Department's Office of Intelligence Policy and Review (OIPR) has conducted FISA training for FBI and/or US Attorney's Office personnel in various cities, including San Diego, Portland, Denver, Houston, Detroit, Chicago, New York, Washington, and Boston, and at the FBI Academy in Quantico.

Between May and September 2003, eight training sessions are planned for FBI and US Attorney's Office personnel. Approximately 100 FBI agents and prosecutors are expected to attend each session. Most of the sessions will occur at the National Advocacy Center in South Carolina, while others are expected to occur in Washington, DC. In addition to FISA, topics covered by these sessions will include an overview of the intelligence community; information sharing and coordination between the intelligence community and law enforcement agencies; FBI intelligence investigations; law enforcement investigations and collection tools; litigation involving classified information; training on sections 203 and 905 of the USA PATRIOT Act, and training as required by section 908 of that Act; and the handling of classified information. OIPR, the FBI, the Criminal Division, the Executive Office for U.S. Attorneys, the Central Intelligence Agency, the Department of Homeland Security and other entities have been planning the training, and will conduct it jointly. Additional training also will be conducted for FBI personnel involved in national security investigations who are unable to attend one of these eight training sessions.

14. How many emergency FISA surveillance orders did the Department of Justice process between FISA's enactment and September 11, 2001? How many has it processed since September 11, 2001? Has the change from 24 to 72 hours in 50 U.S.C. 1805(f) and 1824(e) facilitated the use of FISA emergency searches and surveillance, and if so, how?

Answer: From the enactment of FISA in 1978 through September 11, 2001, available records indicate that Attorneys General issued 47 emergency authorizations for electronic surveillance and/or physical searches under FISA. Between September 11, 2001 and September 19, 2002, the Attorney General made 113 emergency authorizations for

electronic surveillance and/or physical searches under FISA. Of course, following September 11, 2001, the Department conducted the most extensive investigation in the history of the United States, with the overriding goal of preventing another catastrophic terrorist attack occurred against the American people and the United States homeland. FISA was the critical investigative tool in that effort.

The change from 24 to 72 hours in the pendency of the Attorney General's emergency approval authority under FISA before review by the FISC has enabled the Department to respond more quickly, and therefore more effectively, to threats against our national security. By lengthening the time before approval is sought from the FISC, the Department has been able to use the emergency authority to obtain information that otherwise might well have been unavailable. Moreover, by providing additional time, the Department has been able to submit more thoroughly vetted applications originating in Attorney General emergency approvals to the FISC for its review.

15. Since enactment of the USA Patriot Act, what procedures have been implemented to improve the efficiency of processing FISA applications?

Answer: On April 15, 2002, the Counsel for Intelligence Policy -- who is responsible for OIPR – reported to the Deputy Attorney General on actions taken at that time to improve the FISA process. These reforms included:

- A requirement that, to improve the prioritization of FISA applications, renewal applications to the FISC were to be made at the FISC's regular sessions, in the absence of exigent circumstances. This new requirement has enforced a more orderly preparation of renewal applications and limited the more labor-intensive "special" sessions to higher priority initiations and other, operationally driven exigencies.

- Refined procedures for the vetting and requesting of emergency Attorney General approvals under FISA. In order to ensure that requests from the FBI for emergency approvals reflected the priorities of Bureau management, such requests are now made only by the Assistant Directors for Counterintelligence or Counterterrorism or their Deputies.

- Establishment of regular meetings between OIPR and FBI managers to set and review priorities under FISA.

- Expanded OIPR presence at FBI field offices on a continuous basis. Specifically, OIPR has placed one of its line attorneys in New York on a temporary basis to work with the New York field office, has hired an attorney to begin work on a permanent basis in San Francisco, and plans to hire attorneys permanently assigned to New York, possibly Chicago, and with other key field offices as budgets permit.

- Appointment of an Assistant Counsel in OIPR to establish, with FBI attorneys, a joint FISA training program for all FBI foreign counterintelligence agents.

- Adjustments by the Counsel and his Deputy for Operations, on a continuing basis, to improve the workloads, procedures, substance, and flow of the FISA process. To accommodate multiple emergency and other requests that at times may overpower OIPR duty officers, for example, the Counsel or Deputy for Operations has adjusted workloads, called for volunteers, or taken other management action to keep OIPR line attorneys productive and effective.

On January 27, 2003, the Counsel for Intelligence Policy reported on the status of additional steps taken by the FBI and the Department to improve the efficiency of the FISA application process. These steps include:

- Revised filing procedures with the FISC that enable it to review, adjudge, and issue orders more efficiently.

- Procedures enabling FBI field offices to submit FISA requests directly to OIPR, rather than just through FBI headquarters, to accelerate the application process.

- Standardization of requests from the FBI for FISA authorities that will enable faster preparation of applications.

- A major reorganization approved by the Director of FBI of the units and process for handling FISA within FBI headquarters that will enable the Bureau to handle and track applications to the FISC, and to distribute its orders, more efficiently. Specifically, in November 2002, the FBI created the FISA Unit within the Office of General Counsel to perform the administrative support functions for the FISA process. The FISA unit (1) ensures that all FISA applications move expeditiously through the FISA process, coordinating with the field divisions, FBI headquarters substantive units, the National Security Law Unit (NSLU), and OIPR, (2) is overseeing the development and implementation of an automated tracking system that will electronically connect the field divisions, FBI headquarters, NSLU, and OIPR, and (3) distributes all FISA court orders and warrants to the field divisions, telecommunications carriers, Internet service providers, and others.

- An affirmation of the need for regular meetings between OIPR and Bureau managers to review priorities and dockets for applications to the FISC.

- Approval by the Attorney General of OIPR's assigning attorneys to work in the field at FBI field offices to improve the preparation and handling of FISA applications and to facilitate the sharing of intelligence information between Department components in a manner consistent with FISA and applicable Court orders.

Moreover, the Department has increased the capacity of OIPR by increasing the hours and workloads of OIPR attorneys, detailing lawyers from other components of the Department to OIPR, and hiring additional attorneys. In particular, since September 11, 2001, 16 lawyers have been detailed to OIPR from elsewhere in the Justice Department, and OIPR has hired 15 new attorneys. The FBI is making similar adjustments to increase the staffing of the NSLU.

Finally, the Department has, in coordination with the FBI, undertaken a substantial training program outlined in the answer to Question 13.

16. In testimony presented to the Senate Judiciary on March 4, 2003, FBI Director Robert Mueller stated that:

> **The FBI's efforts to identify and dismantle terrorist networks have yielded major successes over the past 18 months. We have charged over 200 suspected terrorists with crimes - half of whom have been convicted to date. The rest are awaiting trial. Moreover, our efforts have damaged terrorist networks and disrupted terrorist plots across the country. In the past month alone, the FBI has arrested 36 international and 14 domestic suspected terrorists.**

A. What authorities under the USA PATRIOT Act were used in identifying and dismantling terror networks and were relied upon to prevent terrorist plots?

Answer: The Department of Justice and the FBI have used numerous authorities provided by the USA PATRIOT Act in the investigation of the September 11 terrorist attacks, and the continuing efforts to detect and prevent terrorism before it occurs and to arrest and prosecute terrorists. The Department and FBI have used, among others, investigative authorities provided in the following sections of the Act:

- 201: Adds certain terrorism crimes to the list of offenses for which wiretap orders are available.

- ➢ These provisions have proven to be beneficial to law enforcement officials, as several wiretap orders have used this expanded list of terrorism offenses.

- 203: Permits law enforcement to share grand jury and electronic, wire, and oral interception information containing foreign intelligence or counterintelligence with federal law enforcement, intelligence, protective, immigration, national defense, or national security officials.

  - ➢ The Department has made disclosures of vital information to the Intelligence Community and other federal officials under section 203 on dozens of occasions.

  - ➢ On September 23, 2002, the Attorney General issued guidelines that establish procedures for the disclosure to the Intelligence Community of grand jury and electronic, wire, and oral interception information that identifies a United States person, as defined by federal law. These guidelines include important privacy safeguards. For example, they require that all such information be labeled by law enforcement agencies before disclosure to intelligence agencies and be handled by intelligence agencies pursuant to specific protocols designed to ensure its appropriate use.

- 205: Authorizes the FBI to expedite employment of translators in the fight against terrorism.

  - ➢ The Bureau has hired 264 new translators to support counterterrorism efforts, including 121 Arabic and 25 Farsi speakers.

  - ➢ The Bureau also is working to implement its Law Enforcement and Intelligence-agency Linguist Access system (LEILA), which will store data regarding the proficiency and security clearance levels of linguists available to the Bureau and its partner agencies. LEILA will work across agency lines to maximize the use and availability of the intelligence community's language resources.

- 207: Increases authorization periods for FISA searches and electronic surveillance.

  - ➢ While the details of FISA operations are classified, the FISA court has authorized operations under section 207. The USA PATRIOT Act has not only provided additional time to government

investigators targeting potential terrorist activity, but has also helped the government and the FISC to focus their efforts on more far-reaching terrorism-related cases.

- 209: Allows voice mail stored with a third party provider to be obtained with a search warrant (upon a showing of probable cause), rather than with a more time-consuming wiretap order.

  ➢ Since the USA PATRIOT Act was passed, such warrants have been used in a variety of criminal cases to obtain key evidence, including voice-mails in the accounts of foreign and domestic terrorists.

- 210: Clarifies the types of records that law enforcement can subpoena from electronic communications providers to include the means and source of payment, such as bank accounts and credit card numbers.

  ➢ Prosecutors in the field report that this new subpoena authority has allowed for quick tracing of suspects in numerous important cases, including several terrorism investigations and a case in which computer hackers attacked over fifty government and military computers.

- 211: Clarifies that statutes governing telephone and Internet communications (and not the burdensome provisions of the Cable Act) apply to cable companies that provide Internet or telephone service in addition to television programming.

  ➢ Cable companies that provide telephone and Internet services are now subject to search warrants, court orders, and subpoenas to the same extent as all other communications carriers, ensuring that terrorists and other criminals are not exempt from investigations simply because they choose cable companies as their communications providers.

- 212: Allows computer-service providers to disclose communications and records of communications to protect life and limb; clarifies that computer-hacking victims can disclose non-content records to protect their rights and property.

  ➢ Section 212 has been used to disclose vital information to law enforcement on many occasions, including one case where such records enabled agents to trace kidnappers' communications. This provision also proved invaluable in the investigation of a bomb

threat against a school. An anonymous person, claiming to be a student at a high school, posted on an Internet message board a bomb death threat that specifically named a faculty member and several students. The owner and operator of the Internet message board initially resisted disclosing to law enforcement any information about the suspect for fear that he could be sued if he volunteered that information. Once agents explained that the USA PATRIOT Act created a new provision allowing the voluntary release of information in emergencies, the owner turned over evidence that led to the timely arrest of the individual responsible for the bomb threat. Faced with this evidence, the suspect confessed to making the threats. The message board's owner later revealed that he had been worried for the safety of the students and teachers for several days, and expressed his relief that the USA PATRIOT Act permitted him to help.

- 216: Amends the pen register/trap and trace statute to clarify that it applies to Internet communications, and gives federal courts authority to authorize the installation and use of pen registers and trap and trace devices in other districts.

  ➢ The Department has used the newly-amended pen/trap statute to track the communications of (1) terrorist conspirators, (2) at least one major drug distributor, (3) thieves who obtained victims' bank account information and stole the money, (4) a four-time murderer, and (5) a fugitive who fled on the eve of trial using a fake passport.

  ➢ This new authority was employed in the investigation of the murder of journalist Daniel Pearl to obtain information that proved critical to identifying some of the perpetrators.

  ➢ The Deputy Attorney General has issued a memorandum to field offices clearly delineating Department policy regarding the avoidance of "overcollection," the inadvertent collection of "content" when using pen/trap devices. This guidance will help protect the privacy of Internet users by ensuring that only addressing information, and not the content of their communications, is collected and used pursuant to section 216. (A copy of this memorandum is attached.)[3]

[3]Attachment D.

- 217: Allows victims of computer-hacking crimes to request law enforcement assistance in monitoring trespassers on their computers.

  ➢ This provision has been used on several occasions. Computer security officials and law enforcement investigators around the country universally have praised this provision, and the Department is committed to implementing it fully.

- 218: Allows law enforcement to conduct FISA surveillance or searches if "a significant purpose" is foreign intelligence.

  ➢ As explained in the answer to question 12, this change has allowed increased coordination between intelligence and law enforcement personnel in foreign counterintelligence investigations in which FISA is being used.

- 219: Permits federal judges, in terrorism investigations, to issue search warrants having effect outside the district.

  ➢ This provision has been used on at least three occasions. One noteworthy example occurred during the ongoing anthrax investigation, when FBI agents applied for a warrant to search the premises of America Media, Inc., in Boca Raton, Florida—the employer of the first anthrax victim. Because of section 219, agents were able to obtain a search warrant from the federal judge in Washington, D.C., overseeing the wide-ranging investigation. This saved investigators from wasting valuable time on petitioning another judge in another district for that authority.

- 220: Permits a court with jurisdiction over the offense to issue a search warrant for electronic evidence in possession of an Internet service provider located in another district.

  ➢ This provision has dramatically reduced the unnecessary administrative burdens in the court districts that are home to large Internet providers, such as the Northern District of California and the Eastern District of Virginia. The enhanced ability to obtain this information quickly has proved invaluable in several time-sensitive investigations, such as one involving the tracking of a fugitive, and another involving a hacker who stole a company's trade secrets and then extorted money from the company.

- 319: Permits the forfeiture of funds held in United States interbank accounts.

➢ On January 18, 2001, a federal grand jury indicted James Gibson for various offenses, including conspiracy to commit money laundering, and mail and wire fraud. Gibson, a lawyer, had defrauded his clients, numerous personal injury victims, of millions of dollars by fraudulently structuring settlements. Gibson and his wife, who was indicted later, fled to Belize, depositing some of the proceeds from their scheme in two Belizean banks. The Department's efforts to recover the proceeds initially proved unsuccessful. Although Belize's government initially agreed to freeze the monies, a Belizean court lifted the freeze and prohibited the government from further assisting American law enforcement agencies. Efforts to break the impasse failed, while the Gibsons systematically looted their accounts in Belize, purchasing yachts and other luxury items. Following the passage of the USA PATRIOT Act, a seizure warrant was served on the Belizean bank's interbank account in the United States pursuant to section 319, and the remaining funds were recovered.

➢ In December 2001, the Department also used section 319 to recover almost $1.7 million in funds. This money will be used to compensate the victims of the defendant's fraudulent scheme.

- 373: Makes it unlawful to run an unlicensed foreign money transmittal business; eliminates prior requirement that the defendant have known about the state licensing requirement.

➢ On April 30, 2002, a federal jury in Boston convicted Mohamed Hussein on two charges of running a foreign money transmittal business (Barakaat North America, Inc.) without a license in violation of section 373. The al-Barakaat network was affiliated with and received funding from al Qaeda. In 2000 and 2001, after Hussein ignored Massachusetts's warning that his business needed to be licensed, nearly three million dollars was wired from his Boston bank account to the United Arab Emirates. On July 22, 2002, Hussein was sentenced to one and a half years in prison, to be followed by two years of supervised release.

- 402: Appropriates funds to triple the number of INS agents on the northern border and allocates monies to the INS and the Customs Service to make improvements in technology for monitoring the northern border and acquiring additional needed equipment.

- The INS has rapidly implemented section 402, and committed to hiring 245 new agents and assigning them to the Canadian border by December 2002. The INS has arranged recruitment visits by over 300 trained border patrol agents to colleges, universities, and military installations. Since September 2001, the INS has received over 65,000 applicants for agent positions, and the agency is making selections at the rate of 1,000 per month (these selections are in various stages of the pre-employment process). The INS has also added five additional border agent basic training classes to its training schedule.

- The INS also has worked to quickly install the Integrated Intelligence Surveillance System (ISIS) at 55 northern border sites. When it is completed in approximately 18-24 months, ISIS, a computer-aided detection system, will provide 24-hour/7-day border coverage through ground-based sensors, fixed cameras, and other technology. The INS further has enhanced border security by deploying three new single-engine helicopters and 500 infrared scopes for border agents at northern border stations. These scopes significantly increase agents' night-vision capability while on patrol.

• 403: Requires the FBI to share information in its National Crime Information Center (NCIC) files with INS and the State Department for purposes of adjudicating visa applications.

  - On April 11, 2002, the Attorney General issued a major directive on the coordination of terrorism-related information. That directive requires all of the Department's investigative components, including the FBI, to include in the NCIC database the names, photographs, and other identifying data of all known or suspected terrorists.

  - Since the USA PATRIOT Act was passed, the FBI has given the State Department over 8.4 million records from NCIC databases. The FBI also has provided to the INS 83,000 comprehensive records of key wanted persons in the NCIC databases, as well as information regarding military detainees in Afghanistan, Pakistan, and Guantanamo Bay. The INS has been working with the FBI and United States Customs Service to provide to INS officers at airports NCIC data on alien passengers. An information system to permit such NCIC searches is on schedule to be deployed by the end of fiscal year 2003.

- 414: Encourages the Attorney General to expedite the implementation of the integrated entry and exit data system authorized by Congress in 1996.

  ➢ The INS has established a multi-agency office to ensure that the system is swiftly put into operation. On December 31, 2003, the system should be operational for all travelers to the U.S. at all air and sea points of entry. The system should be up and running at the 50 largest land points of entry one year later, and at all points of entry for all travelers by December 31, 2005.

- 416: Requires the Attorney General to implement and expand the foreign student visa monitoring program authorized by Congress in the 1996 Illegal Immigration Reform and Immigrant Responsibility Act.

  ➢ The INS began enrolling schools for SEVIS on July 1, 2002. On May 16, 2002, the INS published a proposed regulation that set a January 30, 2003 deadline for all schools and programs to use SEVIS for all of their foreign students. The INS has set up an outreach program for eligible schools demonstrating the benefits of SEVIS, developed training program materials, set up training sessions, begun a competitive process to select contractors to assist with the certification of schools prior to enrollment, and published a variety of guidelines and memoranda concerning SEVIS implementation.

- 801: Makes it a federal offense to engage in terrorist attacks and other acts of violence against mass transportation systems.

  ➢ The Department attempted to use section 801 in against "shoebomber" Richard Reid, who has been convicted of attempting to ignite a bomb hidden in his shoes during an international flight. A federal judge dropped the charge, concluding that airplanes do not fall within the meaning of "mass transportation vehicle." Congress subsequently closed this loophole in section 609 of the "Prosecutorial Remedies and Tools Against the Exploitation of Children Today Act of 2003," or "PROTECT Act."

- 805: Enhances the ban on material terrorist support by making it apply to experts who provide advice or assistance to be used in preparing for or carrying out terrorism crimes, and to acts occurring outside the United States. The section also adds to the list of underlying terrorism crimes for which provision of material support is barred, makes it clear that prohibited material support includes all types of monetary instruments, and enhances penalties for material support.

- On October 21, 2002, six United States citizens who live near Buffalo, New York were indicted on charges of providing support or resources to terrorists. In the early summer of 2001, these men allegedly participated in weapons training at a terrorist training camp in Afghanistan known to be used by al Qaeda. At a safehouse on the way to the camp, they are alleged to have seen a video on suicide bombing that featured the attack on the USS Cole, in which 17 U.S. sailors were murdered. The indictment alleges that the defendants also were trained in the use of assault rifles, handguns, and long range rifles. While they were at the camp, Osama bin Laden visited and delivered a speech instructing the approximately 200 trainees in anti-American and anti-Israeli sentiment as well as general al Qaeda doctrine.

- On October 30, 2002, two Pakistani nationals and one United States citizen were charged with conspiring to provide Stinger anti-aircraft missiles to anti-U.S. forces in Afghanistan. Syed Mustajab Shah, Muhammed Abid Afridi and Ilyas Ali were charged with conspiracy to distribute heroin and hashish and conspiracy to provide material support to al Qaeda. The defendants allegedly arranged to exchange 600 kilograms of heroin and five tons of hashish for cash and four Stinger missiles, and stated that they intended to sell the missiles to al Qaeda forces in Afghanistan.

- On November 1, 2002, four men, including a United States citizen and a U.S. resident, were charged with conspiracy to distribute cocaine and conspiracy to provide material support to a foreign terrorist organization in a drugs-for-weapons plot to deliver $25 million worth of weaponry to the United Self-Defense Forces of Colombia (known by its Spanish language acronym, "AUC"). The AUC – whose leader, Carlos Castaño-Gil, was charged with five counts of drug trafficking in September 2001 – is an 8,000-member Colombian paramilitary group listed on the State Department's Foreign Terrorist Organization List. The two U.S.-based defendants allegedly sought to broker a deal between an undercover law enforcement officer and the other two defendants, who are high-ranking AUC leaders. The charges assert that, under the agreement, the AUC would have exchanged cocaine for five shipping containers full of Russian- and Eastern European-made weaponry, including shoulder-fired anti-aircraft missiles, 9,000 assault rifles, and 3,000 grenades.

- Section 905: Requires federal law enforcement agencies to disclose expeditiously to the Director of Central Intelligence any foreign intelligence acquired by the Department in the course of a criminal investigation, except when disclosing such information would jeopardize an ongoing investigation.

  ➢ On September 23, 2002, the Attorney General released guidelines that formalize the procedures and mechanisms already established for the Department of Justice and other federal law enforcement agencies that acquire foreign intelligence in the course of a criminal investigation.

Whether the Department has used the surveillance techniques and other amendments authorized by sections 204, 206, 214, and 215 is classified. Accordingly, the answer relating to the Department's use of sections 204, 214 and 215 will be delivered to the Committee under separate cover. The answer relating to the Department's use of section 206 will be provided to the House Permanent Select Committee on Intelligence (HPSCI) pursuant to the direction in the Committee's letter of April 1, 2003, and in keeping with the longstanding Executive branch practice on the sharing of operational intelligence information with Congress.

B. In your judgment, how many of those investigations would have been much more difficult or impossible without the authorities available under the Act?

Answer: In our judgment, the Government's success in preventing another catastrophic attack on the American homeland in the 20 months since September 11, 2001, would have been much more difficult, if not impossibly so, without the USA PATRIOT Act. The Department's overall experience is that the authorities Congress provided in the Act have substantially enhanced our ability to prevent, investigate, and prosecute acts of terrorism.

Some of the authorities provided in Title II of the Act substantially eased administrative burdens and increased the efficiency of law enforcement without changing the underlying substantive legal standards – for example, sections 219 and 220. In such cases, the USA PATRIOT Act's authorities made available resources that otherwise would have been devoted to administrative tasks, thereby maximizing the law enforcement personnel available to investigate terrorists. In other instances, the Act in fact allowed the Department to access information that previously had been unavailable, as a legal or practical matter, or simply more difficult to obtain. For example, the Department's response to question 12, *supra*, explains how section 218 of the Act facilitated the terrorism investigation of Sami Al-Arian and other alleged members of a Palestinian Islamic Jihad cell in Tampa, Florida.

17. The Act supplemented the government's authority to freeze and forfeit assets of suspected terrorists and terrorist organizations. Please provide the Committee with information related to the freezing or confiscation of such assets since the enactment of the Act.

A. Please identify all suspected terrorists or terrorist organizations whose assets the federal government has frozen or forfeited?

Answer: Since September 11, 2001, the United States has frozen over 600 bank accounts and $124 million in assets around the world. We have conducted 70 investigations into terrorist financing with 23 convictions or guilty pleas to date.

The Department of Justice has not been given the responsibility of freezing terrorist assets held in the United States. Such freezing results from the designation of terrorist-related groups and individuals under Executive Order 13224 and the International Emergency Economic Powers Act (IEEPA), both of which are enforced by the Treasury Department's Office of Foreign Assets Control (OFAC). However, Justice Department lawyers have successfully defended in court a number of these freezings – for example, on December 31, 2002, the Seventh Circuit upheld Treasury's freeze on the assets of Global Relief Foundation, which is believed to have supported Osama bin Laden, al Qaeda, and other known terrorist groups. *See Global Relief Found. v. O'Neill*, 315 F.3d 748 (7th Cir. 2002).

In most terrorism cases, it has not been necessary for the Justice Department to seek forfeiture of U.S.-based terrorist assets under the USA PATRIOT Act's new authorities, because the assets had already been frozen by OFAC. "Forfeiture," unlike freezing, enables a court to transfer to the United States the ownership of assets which are the proceeds of or are related to a particular crime. Section 806 of the USA PATRIOT Act expanded the government's authority to forfeit terrorist-related assets; this change was codified at 18 U.S.C. § 981(a)(1)(G). After September 11, 2001, the Department of Justice filed a seizure warrant on a New Jersey bank account suspected of containing assets belonging to one or more of the 19 dead hijackers. The Department also included a forfeiture count in the Texas indictment of Hamas leader Musa Abu Marzook, *United States v. Elashi*, CR No. 3:02-CR-052-R (N.D. Tex. filed Dec. 17, 2002). Each of these actions, however, were based on pre-USA PATRIOT Act authority.

B. Please identify the specific authority, whether or not under the Act, that the federal government has asserted in freezing or forfeiting the assets of suspected terrorists or terrorist organizations.

Answer: The judicial forfeiture action in the Marzook case was predicated on money laundering. Assets of terrorists and terrorist organizations, and those who act for or on behalf of, provide financial or other support for, or are otherwise associated with them, can also be frozen pursuant to Executive Order 13224 (Global Terrorism) and Executive Order 12947 (Individuals and Groups who Threaten Middle East Peace Process).

C. Have any seizures or forfeitures been challenged in court?

Answer: The Civil Division of the Justice Department has been involved in judicial challenges to the OFAC designation and freezing actions of terrorist-related entities that have a U.S. presence. These challenges involved two Illinois-based charities suspected of being associated with al Qaeda (Benevolence International Foundation and Global Relief Foundation), a Texas entity believed to be a Hamas front (Holy Land Foundation for Relief and Development) and two entities affiliated with an al Qaeda-connected Somalian financial network known as al-Barakaat (Global Service International, Inc. and Aaran Money Wire Service).

D. What have been the results of any such challenges?

Answer: The United States was successful in defending the Holy Land Foundation challenge in district court, and the case is now on appeal to the D.C. Circuit. One issue remains in the district court and has been stayed. The Seventh Circuit affirmed the district court's denial of a preliminary injunction in Global Relief Foundation and ruled in favor of the government on all of the statutory and constitutional claims raised in the appeal. The government has moved to dismiss the remaining issues in the case on the grounds that the administrative record amply supports Global Relief's designation under Executive Order 13224. Although the designations of certain Barakaat-related entities have been withdrawn, their challenge has not yet been dismissed.

E. Has any court, pursuant to section 316 of the Act (codified at 18 U.S.C. § 983 note), admitted evidence that would otherwise be inadmissible in a forfeiture proceeding? If so, on what circumstances justified admitting such evidence in such cases?

Answer: Because no forfeiture cases have yet been brought pursuant to 18 U.S.C. § 981(a)(1)(G), there has been no occasion to invoke the tool provided in section 316 of the Act. To the extent that section 316 also applies to freezing orders and confiscations under IEEPA, the Department of Justice is unaware of any instances where the evidentiary rules discussed in section 316 were invoked.

18. Section 402 authorizes appropriations to triple the number of INS Border Patrol Agents and Inspectors in each state along the Northern Border, and also authorizes appropriations to provide necessary personnel and facilities to support such personnel.

A. How many additional Inspectors has the INS hired at the Ports of Entry along the Northern Border?

B. How many of those hires are working as Inspectors along the Northern Border at this time?

C. By how many Inspectors has the total staffing at the ports along the Northern Border increased since September 11, 2001?

Answer: Pursuant to the Committee's April 1, 2003, letter, in light of the transfer of the Immigration and Naturalization Service (INS) to the Department of Homeland Security (DHS), we have referred these questions to DHS for a response. We previously provided the Committee with a copy of this referral.

19. What technology improvements have been completed and what additional technology improvements are planned for FY2003 expenditures to improve Northern Border security?

Answer: Pursuant to the Committee's April 1, 2003, letter, in light of the transfer of the INS to DHS, we have referred this question to DHS for a response. We previously provided the Committee with a copy of this referral.

20. Subtitle B of Title IV of the USA PATRIOT Act gives the Attorney General additional authority to detain certain suspected alien terrorists, and improves systems for tracking aliens entering and leaving the United States and for inspecting aliens seeking to enter the United States. Section 411 amends the Immigration and Nationality Act (INA) to broaden the scope of aliens ineligible for admission or deportable due to terrorist activities, and defines the terms "terrorist organization" and "engage in terrorist activity."

A. Has the INS relied upon the definitions in section 411 of the Act to file any new charges against aliens in removal proceedings? If so, how many times has it used each provision?

Answer: Prior to the transfer of the INS to DHS, the INS had not relied upon the definitions in section 411 of the Act to file any new charges against aliens in removal proceedings.

Despite the fact that this authority has not yet been used, each case is reviewed for the potential use of the section 411 amendments to the immigration law. The options in reviewing the case of a suspected alien terrorist range from continuing an ongoing intelligence-gathering operation to criminal prosecution to removal, including both conventional removal under Title II of the Immigration and Nationality Act (INA) to removal before the Alien Terrorist Removal Court under Title V of the INA. Cases are reviewed with the goal of taking the appropriate action to protect the national security.

In the past, decisions have been made to forego filing security-related charges (that would include the amendments made by section 411 of the USA PATRIOT Act) for a variety of reasons, including: (1) the fact that the underlying evidence on the security-related removal charge is classified and cannot be declassified; (2) there was a clear non-security-related charge of removability that would result in a more expeditious removal since security-related charges of removal may generate more litigation; (3) aliens charged with security-related grounds of removal have asserted claims for asylum based on the fact that they have been labeled as "terrorists" by the United States government, thus prolonging the proceedings.

B. In your July 26, 2002 response, you stated that one alien had been denied admission under these new provisions. Have any aliens been denied admission under these grounds since that response?

Answer: Prior to the transfer of the INS to DHS, at least three aliens had been denied admission under these new provisions.

C. What effect have the amendments to the INA in section 411 of the Act had on ongoing investigations in the United States?

Answer: Since passage of the Act and before transfer of INS to DHS, INS and the Department's Criminal and Civil Divisions issued field guidance and undertook numerous training efforts to familiarize INS field attorneys and officers, Assistant U.S. Attorneys, FBI officials, and other federal personnel with the new provisions. This guidance is being employed in pending investigations.

D. Section 212(a)(3)(F) of the INA, as amended by section 411 of the Act, renders inadmissible any alien who the Attorney General determines has been associated with a terrorist organization and intends while in the United States to engage solely, principally, or incidentally in activities endangering the United States. Has the Attorney General made such a determination with respect to any alien thus far?

Answer: The Justice Department had not made use of this provision prior to the transfer of INS to DHS.

The security-related cases we have encountered at ports-of-entry in the recent past have involved aliens subject to removal on other grounds. Due to the time sensitivity of such cases, it was more expeditious to deny admission based on other charges than to refer the cases to the highest levels of the Departments of Justice and State. Nevertheless, we believe that this authority is an important tool to maintain in current law for use in appropriate cases.

E. Have there been any challenges to the constitutionality of the charges added to the INA by section 411 of the Act? If so, please identify the case(s) and the status of the proceedings.

Answer: Because, prior to the transfer of the INS to DHS, the INS had not relied upon the definitions in section 411 of the Act to file any new charges against aliens in removal proceedings, this question is inapplicable.

21. Section 412 of the Act provides for mandatory detention until removal from the United States (regardless of relief from removal) of an alien certified by the Attorney General as a suspected terrorist or threat to national security. It also requires release of such alien after seven days if removal proceedings have not commenced, or if the alien has not been charged with a criminal offense. In addition, this section of the Act authorizes detention for additional periods of up to six months of an alien not likely to be deported in the reasonably foreseeable future if release will threaten our national security or the safety of the community or any person. It also limits judicial review to habeas corpus proceedings in the U.S. Supreme Court, the U.S. Court of Appeals for the District of Columbia, or any district court with jurisdiction to entertain a habeas corpus petition, and limits the venue of appeal of any final order by a circuit or district judge under section 236A of the INA to the U.S. Court of Appeals for the District of Columbia.

A. At the time of your July 26, 2002 response, you had not used the authority in Section 412. Have you used the authority since that response? If so, please state:

i. How many of the aliens for whom certifications have been issued have been removed?

ii. How many aliens for whom the Attorney General issued certifications are still detained? At what stage of the criminal or immigration proceedings are each of those cases?

iii. How many of the aliens who were certified have been granted relief? How many of those aliens are still detained?

iv. Have any challenges to certifications under section 236A(a)(3) of the INA been brought in habeas corpus proceedings in accordance with section 236A(b)? If so, please identify the case(s) and the status of each proceeding.

v. Has the Attorney General released any aliens detained under section 236A because the alien was not charged with a criminal offense or placed into removal proceedings within seven days?

vi. How many non-certified aliens have received relief from removal and remain detained longer than 6 months since such relief was ordered?

Answer to i through vi: Prior to the transfer of INS to DHS, the Attorney General did not use the authority provided by section 412 of the USA PATRIOT Act for the mandatory detention of certified aliens. Numerous aliens who could have been considered for section 236A certifications have been detained since September 11, 2001 and the enactment of the USA PATRIOT Act. It has not been necessary, however, to use the new certification procedure in these particular cases because traditional administrative bond proceedings have been sufficient to detain these individuals without bond. We believe that this authority should be retained for use in appropriate situations.

22. On September 20, 2001, the INS issued an interim rule amending the period of time that an alien may be detained while the agency assesses whether to issue a Notice to Appear (NTA), placing the alien in immigration proceedings. Prior to amendment, the INS was required to issue an NTA within 24 hours of the alien's arrest. As amended, the INS has 48 hours after an alien is arrested to decide whether to issue an NTA, "except in the event of an emergency or other extraordinary circumstance in which case a determination will be made within an additional reasonable period of time."

A. What is the authority for the INS to detain an alien for longer than 48 hours without filing charges?

B. How many aliens have been detained for more than 48 hours without being charged under the authority in this regulation?

C. What is the longest period that an alien has been detained without being charged under the authority in this regulation?

D. Have any challenges to this regulation been brought in judicial proceedings? If so, please identify the case(s) and the status of each proceeding.

Answer: Pursuant to the Committee's April 1, 2003, letter, in light of the transfer of the INS to DHS, we have referred these questions to DHS for a response. We previously provided the Committee with a copy of this referral.

23. Since September 11, 2001, the government has required that certain non-citizens from certain Middle Eastern countries register with the INS (or its successor agency).

A. How many terrorists or suspected terrorists have been investigated and/or detained as a result of the requirement that non-citizens register with the federal government?

B. What is the government's policy regarding whether non-citizens are able to have counsel present during the registration process, specifically during the interview?

C. If counsel are not permitted at any point, what is the government's authority for denying such right to counsel?

Answer: Pursuant to the Committee's April 1, 2003, letter, in light of the transfer of the INS to DHS, we have referred these questions to DHS for a response. We previously provided the Committee with a copy of this referral.

24. Since September 11, 2001, how many individuals have been deported from the United States? To what countries were those individuals deported? What was the racial and ethnic background of such individuals? For what reason were these individuals deported?

Answer: Pursuant to the Committee's April 1, 2003, letter, in light of the transfer of the INS to DHS, we have referred this question to DHS for a response. We previously provided the Committee with a copy of this referral.

Attorney General's Investigative Guidelines

25. On May 14, 2002, the Department issued revised investigative guidelines that established procedures for the initiation of investigations by the Federal Bureau of Investigation ("Bureau").

A. Why were the guidelines for General Crimes and Domestic Security Investigations revised when the apparent threat against the United States is a threat from foreign terrorist groups? Do these guidelines apply only to investigations of U.S. citizens? Are U.S. citizens not subject to the foreign intelligence investigative guidelines?

Answer: In May 2002, the Attorney General issued a revised version of the Attorney General's Guidelines on General Crimes, Racketeering Enterprise and Terrorism Enterprise Investigations (the Guidelines). The previous version of the Guidelines also governed criminal investigations of domestic and international terrorism. The revision of the Guidelines was critical in providing the FBI with the appropriate tools to combat terrorism, because foreign terrorists often engage in conduct that violates the criminal laws of the United States. These guidelines apply to criminal investigations of citizens and non-citizens alike. Similarly, both citizens and non-citizens are subject to the classified foreign intelligence guidelines, though in certain instances standards in those guidelines are different for U.S. persons and non-U.S. persons.

B. The new guidelines allow FBI agents to attend a public event, such as a political demonstration or a religious service, and to use data mining services, provided doing so is for the purpose of preventing or detecting terrorism. How will it be determined that the purpose of attending the event or using the service is to prevent or detect terrorism? How does the amount of evidence establishing that predicate differ from the amount of evidence that would be sufficient to check out leads or open a preliminary inquiry? What level of predication is required to permit FBI agents to attend public events or to use data mining services?

Answer: The revised Attorney General's Guidelines were designed to afford FBI agents the same degree of access to publicly available information as all other members of the general public enjoy. The old Guidelines did not clearly authorize agents to gather information for counterterrorism or other law enforcement purposes – for example, by visiting public places, or researching publicly available information – unless they were looking into particular crimes or criminal enterprises. In effect, agents had to wait for terrorist plots to develop, and for some lead or evidence to come from others, before they could begin gathering information. The revised Guidelines were designed to enable law enforcement to proactively gather intelligence that could be useful to detecting and preventing terrorist attacks, by attending public events or collecting publicly available information.

Agents can do so, however, only to the extent that such events or information are available to any other member of the general public. Part VI.A.2 of the Attorney General's Guidelines specifically provides that "[f]or the purpose of detecting or preventing terrorist activities, the FBI is authorized to visit any place and attend any event that is open to the public, on the same terms and conditions as members of the public generally." The Guidelines specifically mandate that "[n]o information obtained from such visits shall be retained unless it relates to potential criminal or terrorist activity" and prohibit the FBI from "maintaining

files on individuals solely for the purpose of monitoring activities protected by the First Amendment or the lawful exercise of any other rights secured by the Constitution or laws of the United States."

The Guidelines also authorize the FBI to operate and participate in identification, tracking, and information systems for the purpose of identifying and locating terrorists, excluding or removing from the United States alien terrorists and alien supporters of terrorist activity as authorized by law, assessing and responding to terrorist risks and threats, or otherwise detecting, prosecuting, or preventing terrorist activities.

The Guidelines authorize the FBI to engage in these activities (subject to certain limitations, including those mentioned above) in the absence of a pre-existing lead or specific predication. This authority is designed to enable the FBI to draw proactively on available sources of information in order to prevent acts of terrorism. The determination whether a proposed use of this authority is for the purpose of preventing or detecting terrorism is made by the relevant FBI field office, and an agent who attends a public event when unrelated to preventing or detecting terrorism is subject to sanction for violating the Guidelines.

The Guidelines also recognize three levels of investigative activity: (1) the prompt and extremely limited checking out of initial leads; (2) preliminary inquiries (which are undertaken when there is information or an allegation that indicates the possibility of criminal activity and the responsible handling of which requires some further scrutiny beyond checking initial leads); and (3) full investigations (which may be initiated where facts or circumstances reasonably indicate that a federal crime has been, is being, or will be committed).

C. Since the issuance of these guidelines, how many religious sites (mosques, churches, temples, synagogues, etc.) have federal authorities entered in an official capacity without disclosing their identities? Please provide the total number of such sites and a breakdown of how many were affiliated with each particular type of site (mosque, church, temple, synagogue, etc.).

When agents visit religious sites pursuant to AG guidelines, what investigative tools are they permitted to use (i.e., wearing a wire, placing a listening device in the site)? If the information obtained from such visits is found unrelated to any criminal or terrorist investigation, when is such information destroyed and in what manner? Have, and if so provide details, any terrorism-related investigations or prosecutions resulted from such visits?

Answer: The revised Attorney General's Guidelines clarify that agents who are investigating individuals with ties to religious groups may use the same

techniques they would use when investigating any other person. Individuals affiliated with religious entities are not singled out for special scrutiny. But neither will they have effective immunity from lawful investigations.

The old Guidelines did not clearly state that FBI agents could investigate terrorists with ties to mosques in the same way they could investigate suspects with ties to other sorts of entities. As a result, agents were reluctant to follow suspected terrorists into mosques – even when those facilities were held open to all members of the general public. The lack of clear authority to proactively collect terrorism-related information may have hampered the FBI's investigation of Sheik Omar Ahmad Rahman, who was convicted for his role in the 1993 World Trade Center bombing. According to one media account:

> Although the FBI placed Rahman's bodyguard and driver under loose surveillance, Rahman himself was never questioned or put before a grand jury. Nor were his offices bugged, according to a former senior FBI official. Records of Rahman's mosques in Brooklyn and Jersey City were never subpoenaed, and no wiretaps were put on the mosques' phones, the official said.

FBI Wary of Investigating Extremist Muslim Leaders, WASH. POST, Oct. 29, 2001, at A04.

The new Guidelines simultaneously enhance the FBI's ability to visit public places and attend public events, and impose significant limitations designed to safeguard the civil liberty and privacy of law-abiding citizens. The new Guidelines allow FBI agents, like any community police officer, to visit public places and attend public events, but only "on the same terms and conditions as the general public." In addition, the Guidelines prohibit agents from retaining any information from such visits unless it relates to potential criminal or terrorist activity.

Because the FBI only retains from such visits information about potential terrorist attacks or other criminal conduct, it does not keep records or statistics reflecting the number of occasions that agents have visited public places. However, in response to numerous requests, officials in the FBI's Office of the General Counsel recently conducted an informal survey of the FBI's field offices. Their discussions with approximately 45 field offices indicate that fewer than ten of those offices have conducted investigative activities at mosques since September 11, 2001. All but one of those visits were conducted pursuant to, or were related to, open preliminary inquiries or full investigations. In the one reported instance where a visit was conducted pursuant to the Guidelines provision authorizing agents to visit public places and attend public events, no information relating to

potential terrorism or criminal activity was found and, therefore, no substantive information from the visit was retained in FBI records.

D. Since the issuance of these guidelines, how many public meetings, and what types of such meetings (rallies, town halls), have federal authorities entered in an official capacity without disclosing their identities?

When agents visit public meetings pursuant to FBI guidelines, what investigative tools are they permitted to use (e.g., wearing a wire, placing a listening device in the meeting area)? If the information obtained from such visits is found unrelated to any criminal or terrorist investigation, when is such information destroyed and in what manner? Have, and if so provide details, any terrorism-related investigations of prosecutions resulted from such visits?

Answer: The new Guidelines allow the FBI to proactively visit public places and attend public events to detect or prevent terrorist activities prior to developing evidence of the possibility of criminal activity or a specific lead. Use of this tool is explicitly limited to the detection and prevention of terrorist activities. If an agent desires to collect evidence of non-terrorism crimes by visiting public places and attending public events, he or she must first be within one of the categories of authorized investigative activity – either the prompt and extremely limited checking out of leads, a preliminary investigation, or a full investigation.

The investigative techniques that are authorized during attendance at public places depend upon the stage of the investigation when the public visit occurs. For example, the Guidelines bar the use of non-consensual electronic surveillance except during a full investigation. Moreover, all constitutional, statutory, and regulatory restrictions on the use of any investigative technique must, of course, be observed.

FBI agents who visit public places and events may not retain any information unless it relates to terrorism or other criminal activity. As a result, the Department has not maintained centralized statistics on how many times agents attend public meetings.

E. Are FBI agents required to record in writing – before they use data mining techniques or attend a public event under the guidelines -- how such activity is for the purpose of detecting or preventing terrorism?

Answer: There is currently no requirement that agents record in writing the purpose for which they use information systems. The determination whether a proposed use of this authority is for the purpose of preventing or detecting terrorism is made by the relevant FBI field office, and an agent who attends a

public event when unrelated to preventing or detecting terrorism is subject to sanction for violating the Guidelines.

F. The changes to the preliminary inquiry procedures extended the period that such an inquiry can remain open and allowed extensions for up to a year without notice to FBI Headquarters. In considering this change, did you find that your field agents had been reluctant to conduct preliminary inquiries because they could not keep them open long enough without burdensome approval requirements? What other problems did the 90-day limit present to agents? What other problems did requiring approval from Headquarters to continue a preliminary inquiry present to agents? How does Headquarters conduct important analysis of information generated by a preliminary inquiry if Headquarters is unaware of the inquiry for a year?

Answer: The revised Guidelines extend the period to complete the preliminary inquiry to 180 days. Additional extensions of time may be granted for 90-day periods. The first two extensions may be granted by the Special Agent in Charge (SAC), upon a statement of reasons why further investigative steps are warranted when no "reasonable indication" of criminal activity exists. All extensions following the second extension may only be granted by FBI Headquarters, upon receipt of a written request and the statement of such reasons.

The prior 90-day limit did not always afford a sufficient period within which to make an appropriate analysis of the value of continuing the investigation.

Finally, agents are required to share foreign intelligence collected during criminal investigations -- including during preliminary inquiries -- with the intelligence community pursuant to the Attorney General's Guidelines Regarding Disclosure to the Director of Central Intelligence and Homeland Security Officials of Foreign Intelligence Acquired in the Course of a Criminal Investigation, adopted on September 23, 2002.

G. The Guidelines now permit a Special Agent in Charge to open a terrorism enterprise investigation without obtaining approval from FBI Headquarters. Instead, Headquarters must only be notified. What is contained in the required notice? Does the notice provide enough of a description of the evidence to permit FBI Headquarters to make an evaluation of the evidence and determine whether the investigation should continue or is it simply a formal notification that such an investigation has been opened and/or is continuing? Will the information in the notification be sufficient to use it to coordinate that investigation with others?

Answer: As part of the initiation of a Terrorism Enterprise Investigation (TEI), field offices are required to submit to FBI Headquarters a communication setting

forth a factual description describing how the predication standards for the initiation of the TEI have been satisfied. Additionally, a Section Chief within the Counterterrorism Division must concur with the initiation of the TEI. FBI Headquarters must also submit to the Department of Justice a memorandum justifying the initiation of the TEI. These procedures are described in Part III.B of the Attorney General's Guidelines on General Crimes, Racketeering Enterprise and Terrorism Enterprise Investigations. (A copy of the Guidelines is attached.)[4]

Finally, with respect to coordination of terrorism investigations, field agents are required to share foreign intelligence collected during criminal investigations with the intelligence community pursuant to the Attorney General's Guidelines Regarding Disclosure to the Director of Central Intelligence and Homeland Security Officials of Foreign Intelligence Acquired in the Course of a Criminal Investigation, adopted on September 23, 2002. Such sharing does not ordinarily occur through FBI Headquarters.

H. Who at the Bureau is responsible for making and approving the decision for a field agent to enter a public place, and must such approval be in writing prior to entering the public place?

Answer: The Guidelines do not require supervisory approval before an agent enters a public place on the same terms and conditions as members of the public generally.

I. After a field agent visits a public place or event, are any notes or other records of what he or she observed retained? If so, under what circumstances, for what reasons, and for how long are they retained? Under what circumstances is information related to protected 1st Amendment activity retained in FBI or DOJ files? Are any records retained if a preliminary inquiry is never opened?

Answer: No substantive information obtained from the visit may be retained unless it relates to potential criminal or terrorist activity. If information obtained during the visit rises to the level of a lead, such information must be properly documented, including a statement describing how the information is related to potential criminal and/or terrorist activity, and then filed accordingly. If the visit does not develop information relating to potential criminal or terrorist activity, an agent must note in the file the date, time and place visited and that the visit had negative results.

J. Who has access to any records and how does the FBI keep them secure?

---

[4]Attachment E.

Answer: The FBI is subject to numerous laws, regulations, and policies regarding access to and the security of FBI systems and records. Safeguards include maintaining records in limited access space and password protections on computerized data. All FBI personnel are required to pass an extensive background investigation. Information is accessed only by authorized FBI personnel or by non-FBI personnel properly authorized to assist in the conduct of an agency function related to the information.

K. Given the transfer of a substantial number of agents into terrorism investigations, what training did those agents receive on the use of the Guidelines?

Answer: One hundred of the agents transferred to counterterrorism squads have received training on the Guidelines at the Basic Counterterrorism Operators In-service at the FBI Academy in Quantico, Virginia; 160 more agents will receive this training at the same course that started April 21, 2003. In January 2003, training on the revised Guidelines was given at the annual Chief Division Counsel (CDC) conference. The goal was to enable the CDCs to provide subsequent training to agents stationed in their respective field offices. In addition, instruction on the revised Guidelines was given during a recent Joint Terrorism Task Force conference.

L. With the FBI's authority to "data mine" under the Guidelines, many fear that the FBI will have too much information and that the Bureau does not currently have the tools necessary to make good use of intelligence or to keep vast amounts of information secure. What has been done and is being done to improve the Bureau's ability to interpret all of this new data? What security measures have been implemented to prevent unauthorized access to such data?

Answer: The Secure Counterterrorism Operational Prototype Environment (SCOPE) and Investigative Data Warehouse constitute the FBI's programs to provide current technologies to investigators and analysts and to collaborate with its law enforcement and intelligence partners. SCOPE will allow the FBI to use a number of specialized tools to identify and present hidden relationships found in data. The FBI is also utilizing software products that allow for the search, retrieval, and categorization of information. In addition, the CIA and NSA are helping to upgrade the FBI's analytic tradecraft by training and co-locating their personnel with FBI analysts.

With respect to security, please see the answer to question (J), *supra*. The same FBI security measures apply for preventing unauthorized access to law enforcement data. It is restricted to those with a need to know and is limited to official duties. Access to all data is logged and recorded. Specifically, the FBI

Special Technologies Applications Section (STAS) implements user-access-control by issuing a user-ID and password to every authorized user. It implements role-based security by assigning every user to roles that are required for their position, and labels every record in the database with necessary tags to protect the confidentiality of the data. Distribution procedures require that all reports be vetted through an FBI agent who reviews the dissemination list and report produced.

M. Since the Guidelines permit the use of "publicly available" information, what efforts are going to be made to verify the accuracy of the data retrieved? Will agents be required to attempt to independently verify retrieved information for accuracy?

Answer: Safeguards to ensure the accuracy and reliability of information are essential components of any effective information system. Pursuant to a directive of the Director of the FBI, Reports Officers are being assigned to Headquarters and Field Offices to vet information provided to law enforcement, intelligence, and policy entities and to ensure its accuracy.

In collecting information for law enforcement purposes, it is impossible to determine in advance what specific information is relevant, timely, and complete. With the passage of time information may acquire new significance as further investigation brings new details to light. Trained investigators and analysts exercise due diligence to verify information through links, relationships, and other interpretations discovered during investigative efforts.

N. What type of supervision will be required when agents use data mining? Will field agents be able to initiate data mining on their own or will they be required to obtain approval from a supervisor?

Answer: Since all FBI personnel using information systems will have the proper security clearance, access and need to know, general supervision guidelines will apply. Agents are able to access information systems based on their own investigative need and authorization, and the system will keep track of where and what is accessed. Supervisors can review this information as necessary.

O. What data mining services has the FBI used? How long will data obtained through data mining be retained and how will it be indexed?

Answer: The FBI does not use a data mining service but typically uses search engines, queries and indexing programs in order to collate and access its information systems. Search results from such information systems will be maintained in accordance with the Federal Records Act and applicable records

disposition schedules. Data is indexed in accordance with FBI Indexing Guidelines.

P. In its May 2002 Report on Financial Privacy, Law Enforcement, and Terrorism, the Prosperity Task Force on Information Exchange and Financial Privacy outlined many problems with sharing too much information with too many countries and without proper controls. How has the FBI protected against the wide distribution of information to too many countries without proper controls?

Answer: The FBI, Department of Justice, and Intelligence Community have substantial controls on dissemination of information to foreign countries. These controls are extensive and complex in nature and are applied according to the manner in which information is obtained and disseminated. For example, any dissemination of information first depends upon the means by which it was collected/obtained – *e.g.*, via federal grand jury or other subpoena process, court authorized criminal search warrants and Title III electronic surveillance orders, consent searches, FISA-authorized searches and surveillance collections, National Security Letters, and other sensitive and classified intelligence collection methods and sources.

Dissemination of information obtained via criminal court authorized processes is subject to controls imposed by various court orders, statutes, and the Federal Rules of Criminal Procedure. Dissemination of information obtained or derived from FISA is likewise subject to controls imposed by the FISA and the Foreign Intelligence Surveillance Court. Furthermore, the FBI's National Security Law Unit and the Department's Office of Intelligence Policy and Review are consulted on and provide appropriate advice on dissemination of FISA and foreign intelligence information. Information obtained or derived from the FISA process is always appropriately marked as such to ensure any dissemination complies with relevant procedures and controls. With regard to foreign intelligence information, the Director of Central Intelligence formulates policy concerning relationships between the U.S. Intelligence Community and foreign intelligence services. Classified information is designated by established classification levels and marked according to established classification standards which include appropriate controls over dissemination of the information. As is the case with information obtained or derived from grand jury subpoenas and Title III orders, the USA PATRIOT Act removed many barriers to the timely sharing of information between counterintelligence and counterterrorism intelligence operations and criminal investigations. While many barriers have been removed, extensive controls over dissemination of information still remain. With regard to information obtained or derived from other than the means addressed above, dissemination to foreign governments is carefully scrutinized and evaluated according to a number of factors ranging from the sensitivity and potential

importance of the information to the status of the country to which the information is to be provided, and is evaluated in context with the reason the information was requested and the intended use of the information. In short, the FBI does not and cannot haphazardly disseminate information to foreign countries without proper controls and careful evaluation.

Q. Since Syria, Cuba, Libya, Iran, Iraq, China, and others are members of Interpol and share in the international information exchange system, what procedures prevent these countries from receiving information on terrorist suspects who may be supported by participating countries?

Answer: The information provided by an Interpol Member Country remains the Member Country's information and that Member Country controls the distribution and use of that information and can ask for the information to be deleted or adapted. For example, when a Member Country, providing information to the Interpol General Secretariat (IPSG), asks for database checks to be completed or queries other Member Countries and provides a copy to the IPSG, the Member Country provides information regarding any further distribution of this information. The Member Country may advise that the information cannot be released without prior authorization, may specifically state which countries, regions or zones can receive the information, or may designate that the information can be provided to all Interpol Member Countries. Most Member Countries utilize a mixture of all three options, depending on the sensitivity of the investigation and the specific information. Many Member Countries also have a routine rule regarding most police information, including or excluding specific countries or regions. As such, information provided by the United States remains U.S. information, and the U.S. controls the distribution and use of that information.

R. The Guidelines permit acceptance and retention of information "voluntarily provided by private entities." What will the FBI do to ensure the accuracy of the information received from such sources? To what extent have such "private entities" been third parties as opposed to the specific individuals to whom the information pertained? How does the Department interpret "voluntarily" (e.g., does it mean the information was unsolicited, was provided pursuant to a government request, or was provided pursuant to a government subpoena?)?

Answer: Evaluation of source information has always been a fundamental component of FBI investigations. Historically, agents have received information from various sources, including criminal informants, anonymous callers, or other sources of information. The decision to take action based on such information, its use in obtaining investigative tools such as search warrants and electronic surveillance court orders, and ultimately the use of such information in a criminal

prosecution have always required an assessment of the reliability of the information provided by the source and/or the credibility of the source of information.

The FBI does not have readily available data indicating to what extent private entities voluntarily providing information have been third parties, as opposed to specific individuals to whom the information pertained.

The FBI interprets "voluntarily" as meaning the information was provided other than in response to compulsory process (*e.g.*, a grand jury or other subpoena).

S. Where and how is information obtained through data mining stored? Is access to data obtained through data mining limited to those involved in a particular investigation? How is erroneous information corrected or purged, if at all? Has the Department issued written policies to provide guidance in this area? Does it plan to issue such policies?

Answer: To the extent that Department activities in the collection, use or dissemination of records are subject to Privacy Act restrictions, the Department must comply with these restrictions, regardless of the medium involved.

Information obtained by the FBI is stored in appropriate FBI systems in both hard copy and electronic format. Access to data is governed by applicable legal restrictions, including the Privacy Act. Amendment or correction of data is conducted in accordance with the Privacy Act. Sections 16.40 to 16.55 of Title 28, Code of Federal Regulations, contain Department of Justice Privacy Act rules.

Has, and from what companies, the Department purchased information or entered into contracts with data mining companies? To what extent and how will persons listed in such information be able to correct errors or inaccuracies?

Answer: The Department has purchased information or entered into contracts with companies that warehouse public source information. Persons listed in those data collections should seek to correct errors or inaccuracies with source agencies. The FBI has access to Lexis/Nexis news, public source and financial data on a query basis; however, it is currently not aggregated with any other data. Commercial data from Choicepoint and iMap is also available for our unclassified users and its use is based on acceptable DOJ privacy constraints. The FBI also has access to a number of other databases from non-DOJ components of the intelligence community at the classified level that are currently being used for data-mining and pattern recognition. A listing of all the classified databases that are available through Intelink, Intelink-S, and CT-Link should be addressed to the Director of Central Intelligence. Additionally, the FBI has access to a number of

unclassified sources from non-DOJ components such as the State Department VISA application database and INS data, as well as unclassified data from the Open Sources Information System (OSIS) as part of the intelligence community.

T. Is retained information reviewed at reasonable intervals to determine its continuing relevance to antiterrorism efforts? If so, who is responsible for performing such reviews?

Answer: Yes, retained information is reviewed at reasonable intervals to determine its relevance. Reviews may be routinely performed by analysts, case agents, task force members, supervisors, and legal counsel. In the course of an investigation, trained investigators and analysts exercise due diligence to verify information through links, relationships and other interpretations discovered during the use of information systems and other investigative efforts.

Miscellaneous Authorities

26. There have been numerous reports that the Department of Justice has detained individuals as material witnesses, presumably pursuant to judicial orders under 18 U.S.C. § 3144, in connection with terrorism investigations. Please provide the Committee with the following information with respect to each such detainee since September 11, 2001: (1) the length of detention of each detainee; (2) the number of such detainees who either sought review of or filed an appeal from a detention order under 18 U.S.C. § 3145; and (3) the results of such review or appeal.

A. Were these individuals given access to legal counsel? If not, why not?

Answer: Every single person detained as a material witness as part of the September 11 investigation has been represented by counsel. Indeed, material witnesses have the right to a lawyer who can assist them in challenging the legality of the detention at any time. The witnesses get counsel at their first appearance before a judge. The court will appoint free counsel for material witnesses who are financially unable to obtain adequate representation. *See* 18 U.S.C. § 3006A(a)(1)(G) ("[r]epresentation shall be provided for any financially eligible person who . . . is in custody as a material witness"). Other witnesses may retain counsel of their choice.

Every single person detained as a material witness as part of the September 11 investigations was found by a federal judge to have information material to the grand jury's investigation. An individual may be detained under the material witness statute, 18 U.S.C. § 3144, only when a federal judge concludes that (1) his testimony is "material in a criminal proceeding," (2) it may become impracticable to secure his presence by subpoena, and (3) he meets the criteria for detention under the Bail Reform Act, 18 U.S.C. § 3142. These witnesses also all have the

right to be presented promptly before a judge to have bond set and to argue that they should be released on bond. In some cases, the Government has agreed to release individuals on bond, and courts have released witnesses on bond in a few additional cases. *See, e.g., United States v. Awadallah*, 202 F. Supp. 2d 55 (S.D.N.Y. 2002). Material witnesses have status hearings in court, when requested by their counsel or scheduled by the judge, regarding the length of their detention and progress toward obtaining their testimony.

We note that Rule 6(e) requires secrecy of everyone involved in the grand jury process *except* the witness. Thus, each of the detained material witnesses is free to identify himself publicly. The fact that few have elected to do so suggests they wish their detention to remain non-public.

With respect to the request for details about material witnesses detained during terrorism investigations, the Department of Justice has consistently taken the view that Federal Rule of Criminal Procedure 6(e) and court orders in individual cases prohibit it from revealing the exact numbers of material witnesses who are detained pending their testimony before a grand jury. The Department also cannot reveal the details of cases, as that would reveal the direction and focus of secret grand jury proceedings. In addition, disclosing such specific information would be detrimental to the war on terror and the investigation of the September 11 attacks. Thus, it continues to be imperative that the specific number of material witnesses detained as part of the September 11 investigation, the districts and investigations to which they relate, and the length of their detention not be released.

Likewise, the Department cannot provide the number of detainees who may have appealed their detention orders, or the results of such appeals, except where they have been made public by the courts. *See, e.g.*, *United States v. Awadallah*, 202 F. Supp. 2d 55 (S.D.N.Y. 2002); *In re the Application of the United States for a Material Witness Warrant*, 213 F. Supp. 2d 287, 288 n.1 (S.D.N.Y. 2002) (neither the witness's name nor identifying facts are set forth in the opinion because the matter was sealed as proceedings ancillary to grand jury proceedings). We note that the use of the material witness statute is rarely challenged on appeal, probably because the use of the statute in grand jury proceedings is an appropriate law enforcement technique authorized by Congress, routinely used by the Department, and repeatedly approved by federal courts nationwide. *See Bacon* v. *United States*, 449 F.2d 933 (9th Cir. 1971), *In re the Application of the United States for a Material Witness Warrant*, 213 F. Supp. 2d 287 (S.D.N.Y. 2002).

There have been some misconceptions in the public about the number of material witness warrants that the Government issued as part of its September 11 investigation, as well as the circumstances, length, and terms of these detentions. Notwithstanding the restrictions noted above on releasing specific information

about material witnesses, the Department is able to provide some general information about these material witnesses:

- As of January 2003, the total number of material witnesses detained in the course of the September 11 investigation was fewer than 50.

- Approximately 90% of these material witnesses were detained for 90 days or less.

- Approximately 80% of these material witnesses were detained for 60 days or less.

- Approximately 50% of these material witnesses were detained for 30 days or less.

- The few individuals detained for more than 90 days were detained for an extended period of time in part because they pursued litigation that precluded obtaining their testimony, made efforts to proffer or seek immunity before testifying, or took other actions that delayed the proceedings. While such actions are legitimate, they often take time to resolve and can result in longer detention. Moreover, some detainees facing deportation did not pursue efforts to provide prompt testimony.

B. What is the percentage breakdown for the detainees in terms of national origin, race, and ethnicity?

Answer: We do not maintain data on these characteristics of detained material witnesses.

C. Please list the charges that the Department has brought against each such detainee.

Answer: We can only provide information about those material witnesses whose status has been made public in court proceedings. In this regard, Osama Awadallah was charged with perjury; Abdallah Higazy was charged with lying to federal agents; Mohammed Osman Idris was charged with false statements on a passport application; Mohammed Hassan El-Yacoubi was charged with false statements on a passport application; Saleh Ali Almari was charged with conspiracy to commit mail and wire fraud; Earnest James Ujaama was charged with conspiracy to provide material support to Al Qaeda and with using, carry, possessing and discharging a firearm during a crime of violence; and Zacarias Moussaoui was charged with conspiracy to commit acts of terrorism transcending national boundaries, conspiracy to murder United States employees, conspiracy to commit aircraft piracy, conspiracy to use weapons of mass destruction, conspiracy

to destroy aircraft, and conspiracy to destroy property. Most material witnesses remain witnesses and have not been charged with a criminal offense.

D. Please provide the legal basis for detaining those individuals who have been cleared of any connection with terrorism beyond the date of such clearance.

Answer: When a material witness has satisfied his warrant by providing the relevant information he possesses, the warrant is dismissed and the witness is then released *unless* he is transferred to custody on another legal basis, such as immigration charges or federal or state criminal charges.

E. Please provide a list of all requests by the government to seal proceedings in connection with any of the detainees and copies of any orders issued pursuant thereto.

Answer: We are prohibited by court orders from providing any information regarding specific sealed material witness proceedings, including copies of sealing orders. We routinely move to seal *all* grand jury material witness proceedings pursuant to Rule 6(e) of the Federal Rules of Criminal Procedure.

27. On October 31, 2001, the Department of Justice promulgated an interim rule, with provision for post promulgation public comment, that requires the director of the Bureau of Prisons to monitor or review the communications between certain inmates and their lawyers for the purpose of deterring future acts that could result in death or serious bodily injury to persons or substantial damage to property that would entail the risk of death or serious bodily injury to persons. 66 Fed. Reg. 55062, 55066 (2001).

A. How many inmates have been subject to the interim rule?

Answer: The Attorney General has ordered the monitoring of attorney communications for a single inmate: Sheik Omar Ahmad Rahman, who was convicted for his part in the 1993 plot to bomb the World Trade Center. He is confined in the Administrative Maximum United States Penitentiary in Florence, Colorado.

A federal grand jury has indicted Rahman's lawyer, Lynne Stewart, for helping him communicate with his terrorist associates outside of prison. According to the indictment, Stewart distracted prison guards while Rahman and his translator discussed whether to continue to comply with a cease-fire in terrorist activities against Egyptian authorities.

Rahman and his attorneys were notified that their communications were subject to monitoring. No monitoring has occurred, however, because the inmate and his attorneys thus far have chosen not to communicate further with each other.

B. The interim rule required prior written notification to an inmate and any attorneys involved "[e]xcept in the case of prior court authorization. 66 Fed. Reg. at 55066. Under this exception to the required notification, how many cases were there/are there where inmates and their attorneys were not notified that their communications were monitored?

Answer: In our interpretation, the requirement that prior written notification be given to an inmate and attorneys involved "[e]xcept in the case of prior court authorization" refers to a court-authorized interception. While there may have been cases where inmates have been targeted and conversations have been intercepted between such inmates and their attorneys, Title III requires that those conversations be minimized, *i.e.,* not listened to after initial identification of the parties involved, due to the attorney-client privilege. There also may have been cases where attorneys have been the subject of an investigation and, as a result, had their conversations intercepted. Such conversations would have also been minimized under established procedures. Neither the Department, nor any federal law enforcement agency to our knowledge, maintains any records that track the number of attorneys and/or inmates whose communications were intercepted and/or monitored by prior court authorization.

C. The interim rule prohibited disclosure of information prior to approval of disclosure by a federal judge, except where the person in charge of the monitoring determines that acts of violence or terrorism are imminent. How many times did the person in charge of the monitoring disclose information after approval by a federal judge? After a determination that acts of violence or terrorism are imminent?

Answer: As indicated in the answer to question 27(A), *supra*, no monitoring has occurred under the interim rule. Thus, there have been no occasions in which information obtained through monitoring has been disclosed.

D. How many post-promulgation comments were received by the Department of Justice?

Answer: The Bureau of Prisons received thousands of form letters and approximately 30 substantive comments on the interim rule during the comment period.

E. Is the Department of Justice considering any revisions to the interim rule?

Answer: The Department of Justice is considering the comments and is in the process of preparing the final rule.

28. The Department of Defense has detained two United States citizens in military prisons in the United States as enemy combatants. These detentions have been challenged in court, where the Department of Justice has represented the Department of Defense. Has the Department of Justice received any information regarding the detention by the Department of Defense within the United States or abroad of any other United States citizens? Does the Department of Justice have any agreement, arrangement, or understanding, formal or informal, with the Department of Defense regarding the detention of United States citizens as enemy combatants?

Answer: At this time, the Department of Justice is aware of the detention by the Department of Defense (either within the United States or abroad) of no United States citizens as enemy combatants besides Yaser Hamdi and Jose Padilla.

As the question notes, the Department of Justice has represented officials of the Department of Defense who have been named respondents in habeas corpus actions brought on behalf of detained enemy combatants. The Department of Justice is assigned that role by statute. *See* 5 U.S.C. § 3106. Thus, at least to this extent, the Department of Justice has a "formal" "arrangement" with the Department of Defense regarding the detention of U.S. citizens as enemy combatants and litigation surrounding such detentions. The Department of Justice and Department of Defense also maintain lines of communication to ensure that intelligence concerning persons who may properly be deemed enemy combatants (a category that might, from time to time, potentially include U.S. citizens) is shared in a timely manner in order to permit each department to carry out its functions.

29. FBI Director Robert Mueller announced the formation of "flying squads" that would be prepared to be deployed on short notice into terrorism investigations.

A. Have these "flying squads" been formed?

Answer: Yes, the Flying Squads were created in June 2002.

B. How many agents are assigned to a flying squad?

Answer: Two flying squads have been formed within the FBI's Counterterrorism Division, with a total of 24 agents. Both flying squads are managed by a Unit Chief and supported by a Supervisory Special Agent for administrative deployment matters. Each of the two flying squads is led by a Team Leader (Supervisory Special Agent), an Assistant Team Leader (Term-Supervisory Special Agent), and is staffed with nine Special Agents.

C. What kind of training have the flying squad agents received?

Answer: Flying squad agents have received training in post-blast investigations and personal safety while working in an overseas environment. In the near future, they will receive specialized training in the following: major case management, basic statement analysis, effective interrogation and negotiation techniques, crisis management, FISA, weapons of mass destruction, advanced overseas security awareness, U.S. Embassy operations, U.S. intelligence community operations and issues, and other specialty areas.

D. Have they been deployed into investigations?

Answer: Yes, the flying squads have been deployed into investigations.

E. If so, how many times?

Answer: Since their establishment, the flying squads have deployed 23 times (12 domestically and 11 internationally).

F. Did they prove to be a useful addition to the investigation to which they were deployed?

Answer: Yes. Flying squads have been used to very good operational effect. They have been deployed at the direction of FBI Headquarters executive management, field office management and Legal Attaches. The flying squads, as necessary, have been accompanied by an array of FBI operational and supporting assets, including terrorist financial operations and analysis, intelligence, laboratory/forensics and substantive investigative specialists. The flying squads have proved useful in assisting FBI field offices and Legal Attaches in their terrorism investigations, to determine the whereabouts of all subjects, assess their involvement in terrorist activities, determine links to others, and to fully exploit all investigative techniques (*e.g.*, FISA). The flying squads have provided guidance, strategies, and analytical support to the requested field offices or Legal Attaches and have recommended various courses of action. Such assistance has been very beneficial to the terrorism investigative efforts of field offices and Legal Attaches.

30. Does the FBI use, as one of its terrorism investigative tools, aircraft to conduct surveillance of various persons or locations? What type of information is sought using such surveillance?

Answer: The answer to this question is classified and, accordingly, will be delivered to the Committee under separate cover.

31. Has the DOJ through any of its agencies formulated a policy position regarding criteria for establishing the authenticity of foreign government-issued identity cards since the passage of the USA PATRIOT Act? If so, please produce a copy of that position.

Answer: Pursuant to the Committee's April 1, 2003, letter, in light of the transfer of the INS to DHS, we have referred this question to DHS for a response. We previously provided the Committee with a copy of this referral.

32. Has the DOJ through any of its agencies, including especially the INS, prepared or issued a policy with regard to security standards and acceptance of "Matricula Consulars" identity cards issued by foreign governments to persons who are residing in the United States but who may not be lawfully present in the United States.? If so, has that policy been provided in writing to the Office of Management and Budget, the Secretary of State, or the Secretary of the Treasury? If such a policy has been prepared, please provide a copy to the Committee.

Answer: The Department of Justice is currently participating in an interagency process to develop an Administration policy regarding consular identification cards. We refer you to DHS for information related to the former INS on this issue.

33. Regarding the FBI's National Crime Information Database, has the Department lifted a requirement that the FBI ensure the accuracy and timeliness of information about criminals and crime victims before adding it to the database? Please provide a copy of any memoranda pertaining to the requirement that was lifted.

Answer: The FBI recently obtained a limited Privacy Act exemption for the National Crime Information Center (NCIC) database but the exemption does not change any of the requirements for entry, audit, validation, and hit confirmation of NCIC records as provided for in the Criminal Justice Information Services (CJIS) User Agreement and the NCIC 2000 Operating Manual.

Paragraph (j)(2) of the Privacy Act permits the head of any agency to promulgate rules to exempt any system of records within the agency from certain provisions of the Privacy Act. When an agency claims an exemption, it must publish reasons for the exemption in the Federal Register and afford the public an opportunity to comment.

Paragraph (e)(5) of the Privacy Act states that agencies shall maintain all records used by the agency in making any determination about any individual "with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination."

On January 31, 2003, the FBI published a proposed rule in the Federal Register exempting the NCIC (JUSTICE/FBI-001) from paragraph (e)(5) of the Act. *See* 68 F.R.

4974 (Jan.31, 2003). No comments were received regarding the proposed rule. Accordingly, after the close of the public comment period, on March 24, 2003, the FBI published a final rule exempting NCIC from paragraph (e)(5) of the Act. *See* 68 F.R. 14141 (Mar. 24, 2003).

34. Is the FBI ordering its field offices to ascertain the number of mosques and Muslims in their areas? Is the government seeking membership lists from mosques? If so, why? From how many mosques is the government seeking such lists? How, if at all, has the agency reassigned its agents as a result? How many investigations of or prosecutions for terrorism as a result of these activities?

Answer: The FBI has undertaken a broad demographic assessment for the primary purpose of providing FBI Executive management with a snapshot of each field office's working environment and of the communities they serve. As a relatively small part of that broad assessment, information concerning the number of mosques and the approximate size of the Muslim population in a given geographic area was collected, mostly from publicly available sources.

If the FBI is to perform effectively its primary mission of detecting and preventing acts of terrorism, our field offices need to reach out to the overwhelmingly law-abiding and patriotic members of these communities to help us locate terrorists and their supporters who may reside among them in an effort to avoid detection. The demographic survey has facilitated the FBI's efforts in knowing where these communities are concentrated and where to turn for assistance.

For example, the FBI has reached out to these communities to assure them that, despite the emphasis on counterterrorism, investigating civil rights remains a high priority of the FBI. The FBI field offices have been tasked to contact Muslim leaders for the purpose of establishing a dialogue and discussing procedures for alerting the local FBI office to such issues. Over 500 such meetings have occurred since September 11, 2001.

35. Is the Department assisting in the implementation of the Computer Assisted Passenger Prescreening System (CAPPS I or II), which would be used to screen airline passengers?

A. To what extent is the Department, or any of its components, providing information about specific persons for inclusion in CAPPS?

Answer: CAPPS I and CAPPS II are projects of the Transportation Security Administration (TSA), which is part of DHS. CAPPS II is currently under development and will function as a server that, when operational, will examine and check passenger identification with associated information in airline passenger name records. Following this check, CAPPS II will then match the

individual passenger name characteristics against numerous government databases and other criminal and public databases.

One of the databases that CAPPS II, when operational, proposes to access is the Violent Gang Terrorist Organization File (VGTOF) that is maintained by the FBI. The VGTOF is the FBI's primary list of suspected terrorists. An individual may be entered into VGTOF by FBI field offices if there is an open terrorism case in the field office. In addition, even if no case has been opened by a field office, an individual's name may also be entered into VGTOF by the FBI's Terrorist Watch and Warning Unit if the individual is of special interest to the Counterterrorism Division at FBI Headquarters.

B. From what databases or other sources, including companies, does such information come from?

Answer: As previously mentioned, FBI field offices, based on an open terrorism case, and the FBI's Terrorist Watch and Warning Unit may enter an individual's name into VGTOF. Information regarding an individual to be entered in VGTOF may come from but is not limited to: leads developed during an open terrorism case in FBI field offices, human intelligence sources, court authorized electronic surveillance sources, and information shared with the FBI by other law enforcement, intelligence, and homeland security agencies.

C. What checks are in place to ensure that the information is accurate and does not constitute inappropriate profiling?

Answer: TSA can provide additional information regarding the accuracy of the information accessed by CAPPS II.

D. In what manner are individuals afforded an opportunity to correct erroneous or inaccurate information?

Answer: TSA can provide additional information regarding the correction of erroneous or inaccurate information found in CAPPS II.

36. "Operation Liberty Shield" involves stopping cars at airports, checking the identification of truckers who transport hazardous material on the highway, and monitoring Internet and financial transactions.

A. Please identify the specific authority on which "Operation Liberty Shield" was created and implemented.

B. What level of predication is required before an agent may monitor the Internet and financial transactions?

C. What terrorism-related investigations and/or prosecutions have resulted from Operation Liberty Shield?

Answer: Pursuant to the Committee's April 1, 2003, letter, in light of the transfer of the INS to DHS, we have referred these questions to DHS for a response. We previously provided the Committee with a copy of this referral.

37. There have been three successive FBI sweeps since September 11, 2001, to monitor, question, arrest, detain, or deport various immigrants. The first sweep focused on young Arab and Muslim males and occurred in the months following September 11, 2001. The second sweep occurred in March 2002 and centered on thousands of individuals of Middle Eastern and South Asian heritage. The third sweep occurred in March 2003 as part of "Operation Liberty Shield." Please provide information on each of these operations.

A. When were the plans for such operations first considered by the Department?

B. What guidance was provided to U.S. Attorney's Offices and/or FBI offices with respect to questions that should be asked of such immigrants?

C. What has been the outcome of each of these plans? Please provide details such as how many were monitored, questioned, arrested, detained, or deported for each operation. Please provide details as to the number and types of terrorism-related investigations and prosecutions that have resulted from these sweeps.

D. Please identify the specific authority relied on to create and implement these plans, including the monitoring, questioning, arrests, detentions, and deportations.

Answer: The answers relating to these questions are classified, and, accordingly, will be delivered to the Committee under separate cover.

38. In August 2002, a Justice Department rule went into effect giving authority to state and local police to enforce immigration laws.

A. Which state and local governments are using this new authority and to what extent?

B. How many immigration violations were found as a result of state and local law enforcement participation under this new authority?

C. Have any persons or groups affected by this new authority (e.g. immigrants, civil rights organizations) submitted any formal complaints to the Department (including the Inspector General) regarding this authority. If so, please provide details.

Answer to A through C: The only rule that went into effect in August 2002 giving authority to state and local police to enforce immigration laws was the Mass Influx Rule, published at 67 F.R. 48354 (July 24, 2002). This rule, which implements authority given the Attorney General in section 372 of the Illegal Immigration Reform and Immigrant Responsibility Act of 1996 (IIRIRA), Pub. L. No. 104-208, Div. C., 110 Stat. 3009-46, gives state and local police the authority to assist federal immigration officers in the event of a mass influx of aliens as declared by the Attorney General (now the Secretary of DHS). This rule requires the signing of a Memorandum of Understanding with the state or local government and requires training, although under a rule published on February 26, 2003, the training requirement may be abbreviated or waived in unanticipated situations requiring an expeditious response to protect the public safety, public health, or national security. To date, there has been no declaration that a situation of a mass influx of aliens exists. Consequently, no state or local government has exercised this authority, and therefore no immigration violations were found as a result of state and local law enforcement participation under this new authority. We are not aware of any complaints regarding this authority (other than comments received during the rule-making process).

This question may be referring to the inherent arrest authority that is possessed by States. This power is not the creation of the federal government. However, the Attorney General did cite this authority on June 5, 2002, in announcing the development of the National Security Entry-Exit Registration System (NSEERS). He stated the following:

> "When federal, state and local law enforcement officers encounter an alien of national security concern who has been listed on the NCIC [National Crime Information Center] for violating immigration law, federal law permits them to arrest that individual and transfer him to the custody of the INS. The Justice Department's Office of Legal Counsel has concluded that this narrow, limited mission that we are asking state and local police to undertake voluntarily – arresting aliens who have violated criminal provisions of Immigration and Nationality Act or civil provisions that render an alien deportable, and who are listed on the NCIC – is within the inherent authority of the states."

With respect to the legal authority of state and local law enforcement officers to arrest such aliens, the Justice Department's Office of Legal Counsel (OLC)

previously had opined that states possess inherent authority to arrest aliens for criminal immigration law violations generally. In April 2002, OLC additionally opined that states also possess inherent authority to arrest aliens whose names have been entered into the NCIC database because they have both (1) violated *civil* provisions of the federal immigration laws that render them deportable and (2) been determined by federal authorities to pose special risks, either because they present national security concerns or because they are absconders who have not complied with a final order of removal or deportation. The federal government has never preempted this authority; the only barriers to executing such arrests are statutes or policies that states or municipalities may have imposed upon themselves.

This authority is crucial to the success of the absconder initiative. Although every absconder has potentially committed a criminal immigration violation because ignoring a final order of removal is a criminal act, the crime occurred only if the act was "willful." As of February 2003, 1,141 absconders had been apprehended, with 545 removed from the United States, 391 in the custody of federal immigration authorities awaiting removal, and 44 under criminal prosecution by the United States Attorneys for various crimes. Some of the apprehensions involved local law enforcement officials. Others did not. We do not have a statistical breakdown indicating which of these arrests involved civil immigration violations or which local law enforcement agencies, if any, were involved.

The exercise of this arrest authority in the context of the absconder initiative has not generated any formal complaints by arrested aliens. However, there has been one highly-speculative lawsuit on the issue, *Tejeda-Delgado, et. al., v. City of Los Angeles*, in which several removable plaintiffs (who were not arrested) claim that the INS conspired to have the Los Angeles Police Department wrongfully arrest them for civil deportation purposes by posting their names in the NCIC database.