



U.S. Department of Justice

Office of Legislative Affairs

Dave Blake

Office of the Assistant Attorney General

Washington, D.C. 20530

July 1, 2005

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

Dear Mr. Chairman:

Enclosed please find responses to questions posed to FBI Director Robert S. Mueller III, following Director Mueller's appearance before the Committee on April 5, 2005. The subject of the Committee's hearing was "Oversight of the USA PATRIOT Act."

We hope that this information is helpful to you. If we may be of additional assistance in connection with this or any other matter, we trust that you will not hesitate to call upon us.

Sincerely,

William E. Moschella
Assistant Attorney General

Enclosure

cc: The Honorable Patrick J. Leahy
Ranking Minority Member

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

Questions Posed By Senator Grassley

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

Specifically, you stated that,

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

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

Response:

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

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

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

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

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

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

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

Response:

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

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

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

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

Response:

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

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

Response:

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

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

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

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

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

Response:

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

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

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

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

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

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

Response:

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

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

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

Response:

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

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

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

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

Response:

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

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

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

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

Response:

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

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

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

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

Response:

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

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

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

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

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

Response:

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

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

Response:

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

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

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

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

d. How often is this data collected and analyzed?

Response:

The data are collected and analyzed on a continuing basis.

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

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

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

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

Response to a - c:

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

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

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

Response:

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

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

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

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

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

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

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

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

Response:

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

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

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

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

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

Response:

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

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

Response:

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

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

Response:

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

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

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

In addition, the DI has:

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

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

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

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

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

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

Response:

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

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

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

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

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

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

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

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

Response:

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

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

Response:

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

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

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

Response:

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

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

Response:

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

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

Questions Posed By Senator Kyl

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

Response:

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

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

Response:

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

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

Response:

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

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

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

Response:

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

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

Response:

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

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

Response:

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

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

Response:

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

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

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

Response:

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

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

Response:

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

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

Response:

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

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

Questions Posed By Senator Leahy

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

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

Response:

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

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

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

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

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

Response:

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

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

Response:

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

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

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

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

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

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

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

Response:

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

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

Response:

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

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

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

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

Response:

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

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

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

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

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

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

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

Response:

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

Rendition

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

Response:

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

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

Detainee Abuse

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

Response:

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

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

Access to Library Records

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

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

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

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

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

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

Response:

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

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

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

Response:

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

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

Response:

Please see the response to question 29a, above.

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

Response:

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

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

Response:

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

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

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

Oklahoma City Bombing

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

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

Response:

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

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

Response:

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

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

Response:

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

Follow-Up to May 20, 2004 Hearing Questions

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

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

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

Response:

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

Questions Posed By Senator Feingold

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

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

1) Has that number changed?

Response:

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

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

Response:

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

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

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

Response:

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

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

Response:

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

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

Response:

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

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

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

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

Response:

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

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

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

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

Response:

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

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

Response:

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

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

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

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

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

a. From what companies does the FBI currently subscribe?

Response:

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

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

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

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

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

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

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

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

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

b. How often do investigators use these databases?

Response:

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

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

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

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

Response:

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

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

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

Response:

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

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



U.S. Department of Justice

Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

June 29, 2005

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

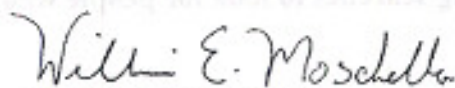
Dear Mr. Chairman:

Please find attached responses to questions for the record posed to Attorney General Gonzales following his appearance before the Committee on the Judiciary on April 5, 2005. The subject of the hearing was, "Oversight of the USA PATRIOT Act".

With this letter, we are pleased to transmit responses to a majority of the questions posed to the Attorney General. The Department is working expeditiously to provide the remaining responses, and we will forward them to the Committee as soon as possible.

We trust you will find this information helpful. If we may be of further assistance on this, or any other matter, please do not hesitate to contact this office.

Sincerely,


William E. Moschella
Assistant Attorney General

Enclosures

cc: The Honorable Patrick J. Leahy
Ranking Minority Member

Questions for the Record
Hearing before the Senate Judiciary Committee on
“OVERSIGHT OF THE USA PATRIOT ACT”
Witness: Attorney General Alberto Gonzales
April 5, 2005

Follow up Questions from Chairman Specter

At the April 5th hearing, Attorney General Gonzales indicated that delayed-notice warrants under Section 213 had been obtained approximately 155 times.

6. Do you know how many of those cases involved terrorism-related offenses or terrorism-related suspects?

ANSWER: In collecting the information to answer this question, we discovered that, in previous surveys, some U.S. Attorneys' Offices had mistakenly reported extensions of delayed-notice search warrants as new warrants, or had reported the same warrant in multiple surveys while two U.S. Attorneys' Offices had indicated a single use of section 213 when they had used multiple delayed-notice search warrants in a single investigation. These combined errors caused the numbers that we previously reported to Congress to slightly overstate our use of section 213. To the best of our knowledge, the number of uses of delayed-notice search warrants issued from the enactment of the USA PATRIOT Act through January 31, 2005 is 153. We had previously reported 155. At least eighteen of these warrants involved terrorism-related offenses or terrorism-related suspects.

7. Given the ability to conduct covert physical searches under FISA, is Section 213 really an important anti-terrorism tool?

ANSWER: Section 213 is a vital aspect of the Justice Department's strategy of prevention – detecting and incapacitating terrorists *before* they are able to strike, rather than simply waiting for terrorists to mount an attack and then prosecuting them. It is a valuable tool that provides options to law enforcement based on the uncertainty of developments in an ongoing criminal investigation. Although physical searches under FISA continue to be an option where appropriate based on the facts and circumstances of the particular case, FISA is not available in domestic terrorism investigations and in cases in which the investigation develops as an exclusively criminal investigation.

In a letter sent to the Committee on April 4, 2005, the Department indicated that, "in at least 28 instances, jeopardizing the investigation was the sole ground for seeking court approval to delay notification."

8. Can you give specific examples of cases where jeopardizing an investigation was the sole basis for delay?

ANSWER: In collecting the information to answer this question, we discovered that, in previous surveys, some U.S. Attorneys' Offices had mistakenly reported extensions of delayed-notice search warrants as new warrants, or had reported the same warrant in multiple surveys while two U.S. Attorneys' Offices had indicated a single use of section 213 when they had used multiple delayed-notice search warrants in a single investigation. These combined errors caused the numbers that we previously reported to Congress to slightly understate our use of "seriously jeopardizing an investigation" as the sole ground for seeking court approval to delay notification. To the best of our knowledge, the number of times the Department, from April 1, 2003, through January 31, 2005, has used "seriously jeopardizing an investigation" as the only ground cited for delaying notice is 32, not 28 as previously reported.

In addition to Operation Candy Box, which was detailed in our April 4, 2005, letter to the Senate Judiciary Committee, we are providing seven additional cases below. It is important to note that the thirty-two instances cited in our April 4 letter do not equate to thirty-two investigations or cases as certain investigations involved the use of multiple delayed-notice search warrants.

Example #1: In the Western District of Pennsylvania, the Justice Department obtained a delayed-notice search warrant for a Federal Express package that contained counterfeit credit cards. At the time of the search, it was very important not to disclose the existence of a federal investigation, as this would have revealed and endangered a related Title III wiretap that was ongoing for major drug trafficking activities.

An Organized Crime Drug Enforcement Task Force (OCDETF), which included agents from the Drug Enforcement Administration, the Internal Revenue Service, and the Pittsburgh Police Department, as well as from other state and local law enforcement agencies, was engaged in a multi-year investigation that culminated in the indictment of the largest drug trafficking organization ever prosecuted in the Western District of Pennsylvania. The organization was headed by Oliver Beasley and Donald "The Chief" Lyles. A total of fifty-one defendants were indicted on drug, money laundering and firearms charges. Beasley and Lyles were charged with operating a Continuing Criminal Enterprise as the leaders of the organization. Both pleaded guilty and received very lengthy sentences of imprisonment.

The Beasley/Lyles organization was responsible for bringing thousands of kilograms of cocaine and heroin into Western Pennsylvania. Cooperation was obtained from selected defendants and their cooperation was used to obtain indictments against

individuals in New York who supplied the heroin and cocaine. Thousands of dollars in real estate, automobiles, jewelry and cash have been forfeited.

The case had a discernable and positive impact upon the North Side of Pittsburgh, where the organization was based. The DEA reported that the availability of heroin and cocaine in this region decreased as the result of the successful elimination of this major drug trafficking organization. In addition, heroin overdose deaths in Allegheny County declined from 138 in 2001 to 46 in 2003.

While the drug investigation was ongoing, it became clear that several leaders of the drug conspiracy had ties to an ongoing credit card fraud operation. An investigation into the credit card fraud was undertaken, and a search was made of a Fed Ex package that contained fraudulent credit cards. Had the search into the credit card fraud investigation revealed the ongoing drug investigation prematurely, the drug investigation could have been seriously jeopardized. The credit card investigation ultimately resulted in several cases including *US v. Larry Goolsby, Sandra Young* (Cr. No. 02-74); *US v. Lasaur Beeman, Derinda Daniels, Anna Holland, Darryl Livsey and Kevin Livsey* (Cr. No. 03-43); *US v. Gayle Charles* (Cr. No. 03-77); *US v. Scott Zimmerman, Lloyd Foster* (Cr. No. 03-44). All of the defendants charged with credit card fraud were convicted except one, Lloyd Foster, who was acquitted at trial. These cases have now concluded.

Example #2: In the Western District of Texas, the Justice Department executed three delayed notice searches as part of an OCDEF investigation of a major drug trafficking ring. The investigation lasted a little over a year and employed a wide variety of electronic surveillance techniques such as tracking devices and wiretaps of cell phones used by the leadership.

During the wiretaps, three delayed-notice search warrants were executed at the organization's stash houses. The search warrants were based primarily on evidence developed as a result of the wiretaps. Pursuant to section 213 of the USA PATRIOT Act, the court allowed the investigating agency to delay the notifications of these search warrants. Without the ability to delay notification, the Department would have faced two choices: (1) seize the drugs and be required to notify the criminals of the existence of the wiretaps and thereby end our ability to build a significant case on the leadership or (2) not seize the drugs and allow the organization to continue to sell them in the community as we continued with the investigation. Because of the availability of delayed-notice search warrants, the Department was not forced to make this choice. Agents seized the drugs, continued their investigation, and listened to incriminating conversations as the dealers tried to figure out what had happened to their drugs.

On March 16, 2005, a grand jury returned an indictment charging twenty-one individuals with conspiracy to manufacture, distribute, and possess with intent to distribute more than 50 grams of cocaine base. Nineteen of the defendants, including all of the leadership, are in custody. All of the search warrants have been unsealed, and it is anticipated that the trial will be set sometime within the next few months.

Example #3: In the District of Connecticut, the Justice Department used section 213 of the USA PATRIOT Act in three instances to avoid jeopardizing the integrity of a pending federal investigation into a drug trafficking organization's distribution of cocaine BASE and cocaine. The provision was used to place a global positioning device on three vehicles.

These applications were submitted in the case of *United States v. Julius Mooring, et al.* That case was indicted at the end of April 2004, and 48 of 49 individuals charged have been arrested. As of this date, 38 of the defendants have entered guilty pleas, and several more are being scheduled. The trial of the remaining defendants is scheduled to begin on June 15, 2005. All defendants with standing to challenge any of the orders obtained have entered guilty pleas.

The Justice Department believed that if the targets of the investigation were notified of our use of the GPS devices and our monitoring of them, the purpose of the use of this investigative tool would be defeated, and the investigation would be totally compromised. As it was, the principals in the targeted drug-trafficking organization were highly surveillance-conscious, and reacted noticeably to perceived surveillance efforts by law enforcement. Had they received actual confirmation of the existence of an ongoing federal criminal investigation, the Justice Department believed they would have ceased their activities, or altered their methods to an extent that would have required us to begin the investigation anew.

In each instance, the period of delay requested and granted was 90 days, and no renewals of the delay orders were sought. And, as required by law, the interested parties were made aware of the intrusions resulting from the execution of the warrants within the 90-day period authorized by the court.

Example #4: In the Western District of Washington, during an investigation of a drug trafficking organization, which was distributing unusually pure methamphetamine known as "ice" and cocaine, a delayed-notice search warrant was sought in April 2004. As a result of information obtained through a wiretap as well as a drug-sniffing dog, investigators believed that the leader of the drug distribution organization was storing drugs and currency in a storage locker in Everett, Washington. The warrant was executed, and while no drugs or cash were found, an assault rifle and ammunition were discovered. Delayed notice of the search warrant's execution was necessary in order to protect the integrity of surreptitious investigative tools being used in the case, such as a wiretap. The investigation ultimately led to the indictment of twenty-seven individuals in the methamphetamine conspiracy. Twenty-three individuals, including the leader, have pled guilty, three are fugitives, and one is awaiting trial.

Example #5: In the Southern District of Illinois, the Justice Department used section 213 of the USA PATRIOT Act in an investigation into a marijuana distribution conspiracy. In particular, in November 2003, a vehicle was seized pursuant to authority granted under the provision.

During this investigation, a Title III wiretap was obtained for the telephone of one of the leaders of the organization. As a result of intercepted telephone calls and surveillance conducted by DEA, it was learned that a load of marijuana was being brought into Illinois from Texas. Agents were able to identify the vehicle used to transport the marijuana. DEA then located the vehicle at a motel in the Southern District of Illinois and developed sufficient probable cause to apply for a warrant to search the vehicle. It was believed, however, that immediate notification of the search warrant would disclose the existence of the investigation, resulting in, among other things, phones being "dumped" and targets ceasing their activities, thereby jeopardizing potential success of the wiretaps and compromising the overall investigation (as well as related investigations in other districts). At the same time, it was important, for the safety of the community, to keep the marijuana from being distributed.

The court approved the Department's application for a warrant to seize the vehicle and to delay notification of the execution of the search warrant for a period of seven days, unless extended by the Court. With this authority, the agents seized the vehicle in question (making it appear that the vehicle had been stolen) and then searched it following the seizure. Approximately 96 kilograms of marijuana were recovered in the search. Thirty-one seven-day extensions to delay notice were subsequently sought and granted due to the ongoing investigation.

As a result of this investigation, ten defendants were ultimately charged in the Southern District of Illinois. Seven of these defendants have pled guilty, and the remaining three defendants are scheduled for jury trial beginning on June 7, 2005.

Example #6: In the Eastern District of Wisconsin, in a drug trafficking case, a delayed-notice search warrant was issued under section 213 because immediate notification would have seriously jeopardized the investigation. In this case, the Department was in the final stages of a two-year investigation, pre-takedown of several individuals involved in the trafficking of cocaine. The Department initially received a delayed-notice search warrant for seven days, and thereafter received three separate seven-day extensions. For each request, the Department showed a particularized need that providing notice that federal investigators had entered the home being searched would compromise the informant and the investigation.

On February 14, 2004, the United States Attorney's Office for the Eastern District of Wisconsin requested a search warrant to look for evidence of assets, especially bank accounts, at a suspect's residence as well as to attach an electronic tracking device on a vehicle investigators expected to find in the garage. The purpose of the device would be to track the suspect and observe his meetings in the final weeks before the takedown. The warrant also requested delayed notice, based on the particularized showing that providing notice that federal investigators had entered the home would compromise an informant and the investigation. The court issued the search warrant and granted the delayed notification for a period of seven days. On February 15, 2004, authorized officers of the United States executed the search warrant on the subject premises.

However, agents were unable to locate the vehicle to install the electronic tracking device.

Before the expiration of the initial delayed-notice period, the Department sought an extension of the delay based on the showing that notice would compromise the informant and the investigation. The court granted a seven-day extension, but investigators were still unable to locate the suspect's vehicle during this time. During this period, however, five suspects were charged with conspiring to possess more than five kilograms of cocaine, and arrest warrants were issued for each of the individuals.

After the issuance of the arrest warrants, the Department sought its third delay in notice to allow agents to endeavor to install the electronic tracking device and to attempt to locate the five suspects. Once again, the request was based on the showing that notice would compromise the informant and the investigation. The court granted another seven-day extension, and agents were able to find a location where one suspect appeared to be staying. After locating the suspect, and before the expiration of the delayed-notice period, the government requested a separate warrant for this location and for other locations used by the conspirators. The Department also requested its fourth and final delay in the notice period to allow agents to execute the search warrants sought, and to arrest the suspects. The court granted all requests and the suspects were subsequently arrested. As required by law, notice of the searches was given upon arrest.

Example #7: In the Eastern District of Washington, in a drug trafficking and money laundering case, a delayed-notice search warrant was issued under section 213 because immediate notification would have seriously jeopardized the investigation. In this case, a district judge had authorized the interception of wire and electronic communications occurring over four cellular telephones that were being used in furtherance of drug trafficking and/or money laundering activities. On December 18, 2004, more than one month after the Drug Enforcement Administration (DEA) began surveillance, DEA agents administratively seized a black Ford Focus owned by one of the suspects based on the determination that the vehicle likely contained controlled substances.

On December 21, 2004, the DEA requested a warrant to search the seized vehicle for drugs, and the court issued the warrant based on the DEA's articulation of probable cause. On the same day, the search warrant was executed on the suspect's vehicle, which was still in the DEA's possession pursuant to the administrative seizure. During the search, agents located approximately two kilograms of suspected cocaine and three pounds of suspected methamphetamine. At the time, the service copy of the search warrant was "served" on the vehicle.

Due to the nature of the investigation, which included the orders authorizing the interception of wire and electronic communications to and from a number of cellular telephones, the DEA believed that both the continued administrative seizure of the vehicle and notice of the execution of the search warrant would greatly compromise the investigation. Therefore, the DEA requested an order allowing them to remove the

served copy of the warrant from the vehicle, and delay notice to the owner for sixty days in order to avoid jeopardizing the ongoing criminal investigation. The court granted the order, concluding that immediate notification would compromise a major drug trafficking and money laundering investigation.

Approximately twenty-five individuals have been indicted as a result of this investigation (eight of whom are still fugitives), and trial is scheduled for this October.

9. Were any of these cases terrorism cases?

ANSWER: Yes, at least two delayed-notice search warrants based solely on the "otherwise seriously jeopardizing an investigation or unduly delaying a trial" criterion were issued in terrorism cases. The Department, however, cannot disclose any specifics about these warrants as they involve sensitive ongoing investigations.

10. Could other bases for delay, such as destruction of evidence or flight from prosecution, have applied in these cases?

ANSWER: When seeking delayed-notice search warrants, it is conventional for U.S. Attorneys' Offices typically list as many bases under 18 U.S.C. § 2705 as are supported by the facts of the case in order to justify the delay in providing notice. In the Department's experience, multiple grounds for delay are listed in many cases. However, with respect to the 32 warrants referenced above, the Department requested delayed notice based only upon the adverse result "otherwise seriously jeopardizing an investigation or unduly delaying a trial." No arguments were made – and no court rulings were issued – regarding any other adverse result listed in 18 U.S.C. § 2705. Therefore, it is impossible to determine with certainty in hindsight how a court would have responded to arguments that were not made. However, it is fair to say that prosecutors obviously thought the adverse result involving "otherwise seriously jeopardizing an investigation or unduly delaying a trial" was the strongest argument for justifying delayed notice. It is also important to note that there are certain adverse effects of immediate notice that would seriously jeopardize an investigation but would not otherwise implicate other grounds for delaying notice specified in the statute, many of which were present in these cases.

13. Can a recipient of an order under Section 215 effectively challenge such an order, given that the FISA court meets in secret and the law only permits disclosure to "those persons necessary to produce the tangible things" at issue?

ANSWER: The Department of Justice has taken the position in litigation that a recipient of a section 215 order may consult with an attorney and may challenge the order. As the Attorney General testified, the Department supports amending section 215 to clarify that a recipient may disclose receipt to legal counsel and that a recipient could seek judicial

review of the production request. In the Department's view, a challenge to a 215 order should be filed in the FISA court, which consists of Article III judges well-equipped to assess the merits of such a challenge, and capable of handling such a challenge while safeguarding sensitive information.

14. Given the extraordinary nature of FISA investigations—the necessary secrecy and the possible lack of any underlying criminal violation—isn't it reasonable to require a standard beyond simple relevance for orders issued pursuant to Section 215?

ANSWER: FISA is used only in investigations of international terrorism and clandestine intelligence activities, as well as to obtain foreign intelligence information, and raising the standard to something higher than relevance would unduly hamper these serious investigations. Just as grand jury subpoenas are used in the criminal context, section 215 is used in the early stages of national security investigations. The relevance standard is needed in the beginning to obtain evidence to determine whether additional investigation is justified, as is the case in criminal investigations. This purpose would be defeated if the standard were higher than relevance.

Suppose, for example, investigators sought to eliminate a potential target from suspicion and could do so through examination of business records. Requiring investigators to demonstrate a higher standard than that required for a grand jury subpoena could very well prevent investigators from obtaining the section 215 order in that situation. We should not make it more difficult to conduct national security investigations under FISA than it is to investigate ordinary crimes.

Section 215 already provides significant safeguards, while permitting investigators to use this preliminary investigative tool effectively. First, while the relevance standard for obtaining a section 215 order is the same standard that governs grand jury subpoenas, unlike in the grand jury context, investigators must obtain court approval for a section 215 order. Second, a section 215 order has a narrow scope and may be used only (1) "to obtain foreign intelligence information not concerning a United States person"; or (2) "to protect against international terrorism or clandestine intelligence activities." It cannot be used to investigate ordinary crimes, or even domestic terrorism, whereas a grand jury subpoena can be used to obtain business records in investigations of *any* federal crime. Third, section 215 explicitly protects First Amendment rights, providing that the investigators cannot conduct investigations "of a United States person solely on the basis of activities protected by the First Amendment to the Constitution of the United States." Finally, the use of section 215 is subject to congressional and judicial oversight.

Title 18 U.S.C. § 2709, authorizes the use of National Security Letters ("NSLs") to obtain subscriber information, toll records or electronic communication transactional records from wire or electronic communication service providers.

Section 505 of the PATRIOT Act lowered the standard for NSLs to require only that the records sought be "relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities." Last year, U.S. District Judge Victor Marrero held 18 U.S.C. § 2709 unconstitutional. *Doe v. Ashcroft*, 04 Civ. 2614 (S.D.N.Y. September 2004). Specifically, Judge Marrero held that the permanent non-disclosure mandate and the lack of available judicial review violated the First and Fourth Amendments, respectively.

18. Would you support legislative language making it clear that NSLs are judicially reviewable?

ANSWER: The Department of Justice is aware of two Senate bills that enable judicial review of NSLs: the Electronic Communications Privacy Judicial Review and Improvement Act of 2005 (S. 693), and the SAFE Act (S. 737). The Administration is carefully reviewing these proposals and has not taken a position on either piece of legislation. The Department, however, has stated in litigation that an entity or person served with an NSL can challenge the request either: (1) as a defense to any enforcement proceeding commenced by the United States in the face of non-compliance; or (2) through a pre-production action to enjoin enforcement.

19. Would you support legislative language limiting the scope of the non-disclosure requirement for NSLs?

ANSWER: As stated above, the Department of Justice is aware of two Senate bills that would change the non-disclosure requirements accompanying NSLs: the Electronic Communications Privacy Judicial Review and Improvement Act of 2005 (S. 693), and the SAFE Act (S. 737). The Administration is carefully reviewing these proposals and has not taken a position on either piece of legislation.

In general, the Department believes that the nondisclosure requirement accompanying NSLs serves a very important purpose because it is critical that terrorists and spies are not tipped off prematurely about intelligence investigations. Otherwise, they or their conspirators may flee, key information may be destroyed before the government's investigation has been completed, or the plot may be expedited. Furthermore, were information identifying the targets of international terrorism and espionage investigations revealed, according to the D.C. Circuit, such disclosures would "inform terrorists of both the substantive and geographic focus of the investigation[,] . . . would inform terrorists which of their members were compromised by the investigation, and which were not[,] . . . could allow terrorists to better evade the ongoing investigation and more easily formulate or revise counter-efforts . . . [and] be of great use to al Qaeda in plotting future terrorist attacks or intimidating witnesses in the present investigation." *Center for National Security Studies v. U.S. Department of Justice*, 331 F.3d 918, 928-29 (D.C. Cir. 2003). The Department has stated in litigation, however, that current law allows the recipient of an NSL to consult an attorney regarding the request for records.

Follow up Questions from Senator Kennedy

Border vigilante groups continue to engage in unlawful conduct including use of force along the Southwest border to stop illegal immigrants. Federal, state and local law enforcement apparently can't handle the problem, so vigilante groups took the law into their own hands. They recruit volunteers, provide weapons and camouflage, and organize illegal operations. Lawsuits have been filed against them, but they don't stop.

Dozens of similar unlawful incidents have been reported to local law enforcement authorities in a single border county in Arizona, but no action is taken.

22. Does the Department of Justice have a policy on vigilantes? How will the FBI guard against vigilantes, or simply look the other way? What about outright crimes? Do they have immunity? Can laws really allow it to continue as a "no-man's" land? Please provide copies of any policies or regulations regarding vigilantes and an update on the situation along the Arizona-Mexico border.

ANSWER: It is the FBI's position that the enforcement of federal criminal law is the sole responsibility of federal law enforcement agents, and that private citizens are not authorized to exercise this authority. The FBI does, however, welcome and often solicit the assistance of private citizens, provided this assistance does not amount to the direct enforcement of federal law.

If the FBI receives credible information that private citizens are violating the civil rights of other persons in the United States (regardless of the nationality of the victims), the FBI will not "look the other way." The FBI takes its historical responsibility for Civil Rights enforcement seriously. If circumstances indicate a federal criminal violation, including a violation of Chapter 13 of Title 18 of the U.S. Code (the Civil Rights chapter), an investigation will be opened following consultation with the Department's Civil Rights Division and the appropriate U.S. Attorney's Office. If circumstances indicate violations of state law, such as simple assault or unlawful detention, the matter is referred to state authorities.

Absent an indication that activities violate federal or state criminal law, the FBI has no authority to interfere with lawful activities. The FBI has not granted immunity to these border groups and, because only the U.S. Attorney or one of his or her assistants may do so, we know of no plans or basis for such a grant in the future.

The FBI has produced no policy papers or regulations regarding vigilantes.

In recent months, we've seen many reports that the federal courts are inundated with immigration cases. Immigration appeals accounted for 3 percent of the federal circuit court workload in 2001. By 2003, that percentage had soared to 15 percent, and in certain courts of appeals, the percentage is 30 percent. Increases have been so large that many federal judges have expressed grave concerns about their ability to properly review these cases.

This problem traces back to 2002, when Attorney General Ashcroft issued regulations ordering the Board of Immigration Appeals to reduce its backlog of asylum and deportation cases. To speed up the process, the regulations allowed one Board Member to review cases, rather than three-member panels. A single member could issue a decision, without any explanation. The regulations also reduced the size of the Board from twenty-three members to eleven. The federal courts are left with the task of sorting through the cases. Critics of this "streamlining process" say that meaningful administrative review has been eliminated. One federal judge said that the immigration decisions by the Board as are "so inadequate as to raise questions of adjudicative competence."

Mr. Ashcroft claimed that this streamlining will save money, yet, the cost burden has now shifted to the federal courts. These courts are now remanding more cases to the Board for further review, finding erroneous decisions, or finding that the Board impeded judicial review by failing to indicate the basis for affirming an immigration judge's decision.

23. You indicated that once you are confirmed as Attorney General, you plan to review the procedures being followed by the Board of Immigration Appeals (BIA). Have you addressed this problem? What changes will you propose to restore the integrity of the Board of Immigration Appeals?

ANSWER: The Board of Immigration Appeals has a difficult and challenging mission, and it always takes on that mission with integrity. The primary goal of the streamlining reform was to institute a system at the Board where cases could be decided more quickly without sacrificing the quality of the appellate review process. Specifically, the regulation was designed to eliminate unnecessary delays in the adjudication of appeals, thereby reducing the backlog of pending cases and permitting the Board to focus its attention on more complex and precedent-setting cases. The purpose of this "streamlined" approach was, on a timelier basis, to remove the cloud of uncertainty over the heads of those aliens who were legally entitled to stay in this country, and to issue final orders of removal (i.e., deportation orders) against those aliens who were here illegally, some of whom posed a threat to our nation.

Some have argued that the BIA's use of affirmances without opinion (AWOs) is the cause of the increase in the rate of appeal, because aliens are not satisfied with those decisions. However, only about one-third of the BIA's decisions are AWOs. (And we note that in issuing an AWO, the BIA specifically has endorsed the result of the immigration judge's decision, which is an individualized finding of fact and application

of law to the case. Therefore, we do not believe it is accurate to claim that aliens are left without a reasoned decision in their cases.) Other observers, including circuit court judges, have noted that there is a powerful incentive for an alien who is in this country illegally to file an appeal with a circuit court: namely, delay of his removal. It would stand to reason that the elimination of administrative delays would invite aliens to pursue other avenues of postponing their removal from the United States.

Although the number of cases being appealed to the circuit courts has increased in recent years, there has not been any increase in reversal or remand rates from the federal courts. To the contrary, as explained below, the circuit courts have been affirming the decisions of the BLA at a higher rate than before the adoption of the streamlining reforms. It is true that some courts have been remanding several kinds of AWO cases to clarify the basis of the Board's affirmance. However, the Board has been working closely with the federal courts in this process, and has issued instructions to Board Members not to affirm those kinds of cases without opinion in the future.

24. For example, what types of transparency or quality control, if any, will you build into the system to ensure that appeals subject to single member summary affirmances conform to the regulations?

ANSWER: The Board is properly using its AWO powers and is in compliance with the regulation. Further, the Board already has internal guidelines and review procedures that have proven remarkably effective. This is not to say that 100 percent of the Board's decisions are error free; few, if any, courts or other adjudicative bodies would make such a claim. When errors do occur, the Board always welcomes the opportunity to correct them. Motions to reconsider are the most effective means to call apparent errors to the Board's attention, and they are welcomed as such. However, the Board's error rate is remarkably low given the number of decisions it renders each year (approximately 48,000 in fiscal year 2004). For example, in the first half of fiscal year 2005, the Board decisions were affirmed in approximately 90 percent of the cases where aliens sought review through filing a petition for review.

25. What standard, if any, should determine whether a single member may simply affirm the immigration judge decision, or must issue a brief opinion as permitted under the regulations?

ANSWER: The standard is set forth in the regulation in 8 C.F.R. § 1003.1(e)(4):

(4) Affirmance without opinion. (i) The Board member to whom a case is assigned shall affirm the decision of the Service or the immigration judge, without opinion, if the Board member determines that the result reached in the decision under review was correct; that any errors in the decision under review were harmless or nonmaterial; and that (A) The issues on appeal are squarely controlled by existing Board or federal court

precedent and do not involve the application of precedent to a novel factual situation; or (B) The factual and legal issues raised on appeal are not so substantial that the case warrants the issuance of a written opinion in the case. (ii) If the Board member determines that the decision should be affirmed without opinion, the Board shall issue an order that reads as follows: "The Board affirms, without opinion, the result of the decision below. The decision below is, therefore, the final agency determination. See 8 CFR 1003.1(e)(4)." An order affirming without opinion, issued under authority of this provision, shall not include further explanation or reasoning. Such an order approves the result reached in the decision below; it does not necessarily imply approval of all of the reasoning of that decision, but does signify the Board's conclusion that any errors in the decision of the immigration judge or the Service were harmless or nonmaterial. (5) Other decisions on the merits by single Board member. If the Board member to whom an appeal is assigned determines, upon consideration of the merits, that the decision is not appropriate for affirmance without opinion, the Board member shall issue a brief order affirming, modifying, or remanding the decision under review, unless the Board member designates the case for decision by a three-member panel under paragraph (e)(6) of this section under the standards of the case management plan. A single Board member may reverse the decision under review if such reversal is plainly consistent with and required by intervening Board or judicial precedent, by an intervening Act of Congress, or by an intervening final regulation. A motion to reconsider or to reopen a decision that was rendered by a single Board member may be adjudicated by that Board member unless the case is reassigned to a three-member panel as provided under the standards of the case management plan.

Thus, if a Board Member determines that the above regulatory criteria are met, the Board Member is required to issue an AWO. As noted, however, the majority of Board decisions are not AWOs, but rather are orders that contain some explanation of the reasons for the Board's disposition.

26. How will you deal with criticism by the federal courts of the quality of decisions made by the Board and immigration judges? What steps will you take to correct the legal errors by some immigration judges, and correct the Board streamlining errors?

ANSWER: While some courts have expressed occasional criticism regarding Board and immigration judge decisions, such criticism has been relatively rare and, to a certain extent, it has been based on a misunderstanding of the nature and effect of the Board's procedural reforms. The federal courts review many thousands of immigration cases each year, and those courts that have voiced some criticism of Board and immigration judge decisions continue to sustain an overwhelming majority of those decisions. In FY

2004, for example, the agency's determinations were sustained by the courts in more than 90% of the cases decided, and this rate actually has increased since the Board adopted its "streamlining" reforms. These statistics underscore the fact that the agency's decisions are of extremely high quality.

Further, the Board's reforms have sustained the fairness of the adjudicatory process. An immigration case that is "streamlined" is still reviewed by the Board, so each alien continues to have both trial and appellate consideration of his or her claims at the administrative level. Cases are "streamlined" when the Board concludes that the immigration judge's decision is sufficient and there is no need to write a separate opinion. For the reasons fully explained when the reforms were adopted, this allows the Board to rationally allocate its limited resources in the face of an increasing number of appeals filed with the Board each year (approximately 43,000 in FY 04).

The Department has taken a number of measures to ensure that Board and immigration judge decisions are sound. The Board is working closely with the circuit courts, and provides timely guidance to staff in the wake of important court decisions to make sure that these precedents are being followed. Although resources are limited, the Board also offers ongoing training to staff and has long-standing pre- and post-adjudication quality control measures in place. For those administrative decisions that are challenged in federal court, the Civil Division's Office of Immigration Litigation (OIL) makes an independent determination whether the Board or immigration judge's decision has defects that would preclude proper judicial review. Such cases are remanded to the agency. OIL shares with the immigration agencies all federal court decisions, and meets regularly with the Executive Office of Immigration Review and the Department of Homeland Security to discuss the judicial review process, including such comments and criticisms as the courts may make. OIL also meets with the courts to discuss their concerns regarding the immigration docket. This constant and comprehensive dialogue ensures that problems are identified and resolved, and that the immigration agencies continue to improve the process by which we decide our immigration cases.

As a final note, it is important to take into account the successes that the reform regulation has had, particularly in minimizing delays in the adjudicative process. The interests of justice are not served by delay in the context of immigration proceedings. While aliens who do not merit relief from removal may welcome postponement of deportation, no one would agree that this is a proper goal in the administration of this nation's immigration laws. By contrast, those aliens who do merit relief clearly benefit from receiving that relief as promptly as possible. And delays in adjudicating cases involving detained aliens have enormous fiscal and human costs. While reasonable minds may differ on the means to achieve it, timeliness is an important function in any adjudicatory context.

Recent news reports indicate that President Bush is considering a major restructuring of the Justice Department that would create a new national security division in an effort to consolidate terrorism investigations. Although the idea aims to streamline the handling of terrorism cases, it raises serious civil liberties concerns. There are inherent checks on abuse if different supervisors within different divisions, who bring unique perspectives, are forced to collaborate in a single effort. If all terrorism matters are brought under one roof with a single chain of command, the potential for abuse is heightened. The dangers are greater because PATRIOT Act provisions require so little outside oversight of terrorism investigations.

I'm worried that consolidation may lose the expertise developed by the individual components. For example, immigration and civil rights matters that involve trafficking in persons or domestic hate groups may overlap with terrorism investigations. Yet, the methods of investigation and prosecution of those types of cases are specialized.

Moving those types of cases away from the divisions which currently handle them runs the risk of losing the experience of those senior lawyers and supervisors who will remain in those divisions performing non-terrorism related work.

27. How far along are you in plans to re-structure the Justice Department?

ANSWER: It is imperative that the Department of Justice, along with all other federal agencies, periodically reassess whether changes to the way they operate would allow them to be more effective in fulfilling their obligations to the American people. Absent such periodic reappraisals, an agency's structure, policies, and operating procedures are determined in part by inertia; with such reappraisals, the agency can either validate its existing operational methods or respond promptly and agilely to changed circumstances that call for modified methods of fulfilling its mandate.

With that in mind, the Department of Justice has undertaken a comprehensive review to consider whether a departmental reorganization more closely aligning certain components with primary responsibility for national security would better serve to protect the lives and liberty of the American people. As you know, the bipartisan Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction ("WMD Commission") recommended that the "Department of Justice's primary national security elements—the Office of Intelligence Policy and Review, and the Counterterrorism and Counterespionage Sections of the Criminal Division—should be placed under a new Assistant Attorney General for National Security." (WMD Commission Report (unclassified version) at 471.)

The Administration is still reviewing the Commission's recommendations. We can assure you that no restructuring of the Department of the comprehensive sort recommended by the WMD Commission will go forward absent a decision by the President and consultation with the Congress.

28. Do you have a sense of what changes would be made if re-structuring occurs? What are they? What is being considered?

ANSWER: It would be premature to speculate as to any changes that might be made as a result of the Department's comprehensive review and the Administration's consideration of the recommendations of the WMD Commission. A reorganization along the lines recommended by the WMD Commission is certainly under consideration.

29. Have you considered the civil liberties implications? What issues have you identified? How would you address them?

ANSWER: The Department takes very seriously any consequences for civil liberties that might result from a departmental reorganization. Consideration of any such consequences is an integral part of the Department's internal review of any proposal to reorganize the Department. We will fully consider the ramifications that a restructuring may have for Americans' civil liberties, and we will take concrete steps to forestall any deleterious effects if a restructuring is implemented.

30. Given the risks, don't you think you should have to concretely demonstrate the benefit that would come from re-structuring before it takes place? At a minimum, shouldn't you have to provide details about any problems you are encountering now so that the cost-benefit analysis is clear?

ANSWER: The Department will not seek to reorganize itself unless the proposed restructuring will serve to further protect the lives and liberties of Americans. Such a decision would be premised on an assessment that the proposed reorganization will render the Department more effective in fulfilling its obligations to the American people than it is now.

During the April 6, 2005 hearing, I asked Director Mueller about the Government Accountability Office report regarding authorizing gun purchases by people on federal law enforcement watch lists. I'd like your responses to the same questions. The GAO found that a total of forty-four firearm purchase attempts were made by individuals designated as known or suspected terrorists by the federal government from February 3 through June 30, 2004. In thirty-five cases, the FBI specifically authorized the transactions to proceed because field FBI agents were unable to find any disqualifying information (such as felony convictions or illegal immigrant status), within the federally prescribed three business days. In a response to a recent inquiry by Senator Lautenberg, myself, and other Senators, you indicated that the Justice Department was convening a Working Group to study the GAO report and existing law and regulations.

31. Should the FBI be in the business of authorizing the transfer of guns to people on terrorist watch lists?

ANSWER: The FBI applies and enforces the laws as enacted by Congress. Under the Gun Control Act, Congress has established the federal criteria on which the FBI may deny the transfer of a firearm by a Federal Firearms Licensee requesting a NICS check. These prohibiting criteria are set forth in 18 U.S.C. 922(g) and (n). The fact that an individual has been included in the Violent Gang and Terrorist Organization File (VGTOF), the FBI's database on persons suspected of a connection with terrorism, is not a basis on which, under existing law, the FBI may deny the transfer of a firearm. The FBI is taking all the steps it can consistent with current law to seek to determine whether any individual in the VGTOF seeking to acquire a firearm is a prohibited person. Unless there is a legal basis on which to deny the transfer, *i.e.*, the individual is prohibited from acquiring a firearm under current law, the FBI must allow the sale to proceed.

32. What will be the exact scope of the Working Group's review? Will the review include an examination of the reliability of the terrorist watch lists? When do you expect that the review will be completed and that a report will be released?

ANSWER: The Working Group has been directed to review the current process relating to NICS checks hitting on records in the VGTOF and to determine whether to recommend changes to that process or existing law. The Working Group was formed in response to the GAO report on the acquisition of firearms by persons in the VGTOF and is not reviewing the reliability of that file or of any other watch list. The Attorney General expects to receive the results of the Working Group's efforts shortly.

A significant issue on which the Department has been unfortunately silent: the need to expand the ability of federal officials to prosecute hate crimes. Hate crimes are a violation of all our country stands for. They send the poisonous message that some Americans deserve to be victimized solely because of their race, religion, or sexual orientation. They are crimes against entire communities.

In the last Congress, the Senate approved bipartisan legislation against hate crimes by a vote of 65 to 33. The House voted 213 to 186 to instruct its leadership to support the Senate bill. Nevertheless, House conferees on the Defense Authorization Bill had the legislation stripped out of conference.

33. Will you publicly support the expansion of the hate crime statute? If introduced in this session, will you support the specific legislation that was introduced by Senator Smith and myself, S.966, in the 108th Congress?

ANSWER: The Department appreciates the leadership that both you and Senator Smith have shown on this issue. This Administration believes that violent crime, whether

motivated by prejudice or animus, should never be tolerated. Bias-motivated crimes are specifically prohibited by many States and are prosecutable as violent crimes under existing law in all States. This Administration is committed to investigating and prosecuting bias-motivated crimes, at the Federal level, to the fullest extent of federal law.

The Department has stated in response to prior inquiries that President Bush indicated during the 2000 Presidential campaign that he supported the hate crimes legislation introduced by Senator Hatch in the 106th Congress, which shared several features with S. 966. Those common features include provision by the Attorney General of assistance in the investigation or prosecution of any violent crime that constitutes a felony and is motivated by animus against the victim by reason of the membership of the victim in a particular class or group; grants by the Attorney General to State and local entities to assist in the investigation and prosecution of such crimes; and the appropriation of \$5 million for the next two fiscal years to carry out the grant program. The Department would need to review any other legal and policy issues raised by changes to the Federal criminal code before we are able to comment further.

Two weeks ago, the American Civil Liberties Union released a September 14, 2003, memo from Lieutenant General Sanchez that authorized interrogation methods for use in Iraq. The memo authorized the use of military working dogs to exploit Arab fear of dogs, the use of "yelling, loud music, and light control" to create fear, and the use of sleep management and stress positions. In his testimony before the Senate Armed Services Committee on May 19, 2004, Senator Jack Reed asked the following question:

"General Sanchez, today's USA Today, sir, reported that you ordered or approved the use of sleep deprivation, intimidation by guard dogs, excessive noise and inducing fear as an interrogation method for a prisoner in Abu Ghraib prison. Is that correct?"

General Sanchez replied, "Sir, that may be correct that it's in a news article, but I never approved any of those measures to be used within CJTF-7 at any time in the last year."

38. The ACLU sent you a letter last Thursday urging you to open an investigation into whether General Sanchez committed perjury in his sworn testimony before the Senate Armed Services Committee. Do you intend to open an investigation into this matter?

ANSWER: Please see answer to question 39, below.

39. If so, please provide the details of the intended investigation. If not, please explain why not.

ANSWER: We are in receipt of the information, and it would be inappropriate to comment at this time. All allegations of misconduct by officials of the United States government are taken seriously and all such matters are handled fairly, appropriately, and impartially.

As I understand it, under current law, there are no requirements for the Justice Department to report on the use of these orders. That is, the FBI never has to tell Congress or the public how many of these National Security Letters have been issued, what type of information is sought, what kind of recipients are targeted, whether the information is used, at all, or whether it is turned over to other agencies. There are few reporting requirements for surveillance orders either. As I understand it, the Intelligence Reform Act requires the Justice Department to report the number of FISA orders every six months in broad categories, such as physical search, or wiretaps, or pen registers. There are no requirements to report what type of things are sought, what kind of recipients were targeted, or whether the information was useful.

Why shouldn't the American people know what the FBI is doing? We know that policy-making after 9/11 involves a delicate balance between liberty and security.

57. How can the nation have an informed debate about where to draw the line unless we know what's happening? Wouldn't it be useful for Congress and the American people to know if, say, ninety percent of all these orders were used to obtain medical records? Or that half of all them are used to obtain credit reports?

ANSWER: The FBI regularly reports to Congress the number of National Security Letters (NSLs) issued under every statutory grant of authority except 15 U.S.C. §§ 1681v (credit reports), which does not mandate reporting.

Semiannually, the Department reports the usage of FISA to the Intelligence Committees through the Attorney General's Report on Electronic Surveillance and Physical Search under the Foreign Intelligence Surveillance Act. That report, which is classified, is quite detailed. Although we agree that Congressional oversight committees need information as to how the USA PATRIOT Act and other intelligence tools have been used in order to make informed decisions on whether modifications should be made, the classified semiannual report on the use of FISA cannot be made available to the general public without compromising national security.

The Attorney General declassified the number of times the FBI had obtained section 215 orders as of March 30, 2005, and advised that a section 215 order had not been used to obtain medical records. NSLs are not available except to obtain the narrow categories of information discussed above, which do not include medical records.

We all know that success in intelligence is difficult to demonstrate. Unfortunately, it is usually only the failures and disasters that people learn about. The PATRIOT Act asks us to give up some liberty in order to gain – hopefully – more security.

58. Aren't we entitled to know, in a concrete way, that the sacrifices are worth it? Shouldn't we at least know how the information obtained is being used and whether it is actually making us safer?

ANSWER: The Department uses the USA PATRIOT Act ("the Act") as a tool to effectively investigate individuals and groups involved in acts of terrorism and to provide this information to the law enforcement and intelligence communities. This raw intelligence not only provides security, but also ultimately protects individual liberties. For example, while the public has been made safer through the availability of grand jury subpoenas to investigate criminal acts, this tool is not available with respect to national security investigations. The Act permits the use of investigative tools similar to the grand jury subpoena, including National Security Letters (NSLs) and business record orders, for these national security investigations and permits criminal and counterintelligence investigators to share the information obtained through their separate investigations. Because these tools permit the acquisition and sharing of information that may only be meaningful when aggregated with other information obtained using criminal investigative tools provided outside the Act, it is impossible to correlate the issuance of an NSL or a business record order with the success of a counterterrorism investigation, since typically no single piece of information determines the success of an investigation.

An example of how the USA PATRIOT Act has enhanced the government's ability to address national security matters is provided by the authority afforded by section 215 of the legislation. Prior to the passage of the Act, it was difficult for the government to obtain court orders for access to business records and other tangible items in connection with national security investigations. Such records, for example, could be sought from only common carriers, public accommodation providers, physical storage facility operators, and vehicle rental agencies. *See* 50 U.S.C. §§ 1861-1863 (2000 ed.). In addition, intelligence investigators had to meet a much higher evidentiary standard to obtain an order requiring the production of such records than prosecutors had to meet to obtain a grand jury subpoena to require the production of those same records in a criminal investigation. *See id.*

Section 215 of the USA PATRIOT Act made several important changes to the FISA business records authority so that intelligence agents and analysts are better able to obtain critical information in important national security investigations. For example, just as there is no artificial limit to the range of items or types of entities that criminal prosecutors may subpoena, section 215 now allows the FISA Court to issue orders requiring the production of any business record or tangible item. Similarly, just as prosecutors in a criminal case may subpoena any item so long as it is relevant to their investigation, so too may the FISA Court issue an order requiring the production of

records or items that are relevant to investigations to protect against international terrorism or clandestine intelligence activities.

Section 215 changed the standard to compel production of business records under FISA to simple relevance and expands this authority from a limited enumerated list of certain types of business records (i.e. hotels, motels, car and truck rentals) to include "any tangible things (including books, records, papers, documents, and other items) for an investigation to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution."

As noted above, many of the authorities provided by the USA PATRIOT Act to deal with terrorists have long been available to prosecutors to deal with ordinary criminals. An additional example of how the Act enhanced the government's ability to address national security matters is provided by the authority afforded by section 206 of the legislation. Section 206 provides international terrorism investigators with an authority long possessed by criminal investigators. In 1986, Congress authorized the use of multipoint or "roving" wiretaps in criminal investigations. Before the Act, however, these orders were not available for national security investigations under FISA. Therefore, when an international terrorist or spy switched telephones, investigators had to return to the FISA Court for a new surveillance order and risked missing key conversations. Section 206 fixed this problem by authorizing multipoint surveillance of an international terrorist or spy when a judge finds that the target may take action to thwart surveillance and has proven effective in monitoring terrorists and spies, who are trained in sophisticated countersurveillance techniques.

Finally, the Department of Justice remains very concerned about any allegations of abuse of the tools provided in the USA PATRIOT Act. We acknowledge and are pleased to assist in Congress' active oversight of the Department's use of the tools contained in the Act. As Congress decides the fate of these tools, however, we hope that it does so in a thoughtful manner and in response to real concerns, not as a reaction to baseless allegations. Recently, Senator Dianne Feinstein shared with the Department of Justice correspondence from the American Civil Liberties Union (ACLU). That correspondence was in response to the Senator's request for information regarding alleged "abuses" of the USA PATRIOT Act. The Department reviewed the ACLU's allegations and our review demonstrated that each matter cited by the ACLU either did not, in fact, involve the USA PATRIOT Act, or was an entirely appropriate use of the Act. The Department then sent a letter addressing these allegations to Senator Feinstein.

We understand that there will soon be a vacancy in the Executive Office for the U.S. Trustees (EOUST) because Larry Friedman is resigning. The selection of the next Director of the Executive Office will be a very important decision due to the changes in the system caused by the new bankruptcy legislation.

59. What standards and qualifications do you intend to apply in the appointment process for the next Trustee?

ANSWER: One of the Attorney General's priorities is to appoint individuals of the highest ability and strongest ethical and professional integrity to serve in key administrative positions in the Department of Justice. These criteria will be applied in the selection of the next Director of the Executive Office for United States Trustees. The next Director will possess the experience and qualifications necessary to enable him or her to lead the Executive Office for United States Trustees in its mission to promote the fairness and effectiveness of the American bankruptcy system. That mission will include implementation of the recently signed Bankruptcy Abuse Prevention and Consumer Protection Act of 2005.

60. Will you be willing to discuss this matter with the members of the Judiciary Committee before you make a decision?

ANSWER: Although the Attorney General is pleased to answer questions regarding the appointment process, it is not the practice of the Department of Justice to discuss candidates for senior appointments with members of Congress prior to selection. Of course, we welcome your views and those of your colleagues as consideration is given to the appointment of senior Department of Justice officials.

Section [1061] of the Intelligence Reform and Terrorism Prevention Act of 2004 establishes a civil liberties oversight board that shall be composed of a chairman, a vice chairman, and three additional members appointed by the President. The chairman and vice chairman shall each be appointed by the President, by and with the advice and consent of the Senate.

61. Will you consult with the majority and minority members of the Senate before aiding the President in selecting members of the Board?

ANSWER: The Department does not have a role in the selection of members of the board.

62. What is the status of the Administration's efforts to select Board members?

ANSWER: Although the Department did not have a role in selecting members of the Privacy and Civil Liberties Oversight Board ("the Board"), we understand that on June 10, 2005, President George W. Bush announced his intentions to nominate the following two individuals and appoint three other individuals to serve on the Board. The President intends to nominate Carol E. Dinkins, of Texas, to be Chairman of the Privacy and Civil Liberties Oversight Board; and Alan Charles Raul, of the District of Columbia, to be Vice Chairman of the Board. The President also indicated his intention to appoint the following three additional members of the Board: Lanny J. Davis, of Maryland; Theodore B. Olson, of Virginia; and, Francis X. Taylor, of Maryland.

Follow up Questions from Senator Durbin

The government has the authority to request certain information from certain entities and individuals pursuant to each of the following authorities: Section 2709 of Title 18 of the United States Code, Section 1114(a)(5) of the Right to Financial Privacy Act of 1978 (12 U.S.C. 3414(a)(5)), Section 625 of the Fair Credit Reporting Act (15 U.S.C. 1681u), and Section 626 of the Fair Credit Reporting Act (15 U.S.C. 1681v). For the last three calendar years (2002, 2003, and 2004), with respect to each of these authorities:

63. How many requests has the government made?

ANSWER: We would first like to clarify that three of the statutes listed in your question, namely 18 U.S.C. § 2709, the Right to Financial Privacy Act of 1978 (12 U.S.C. § 3414(a)(5)), and Section 625 of the Fair Credit Reporting Act (15 U.S.C. § 1681u), authorize only the FBI to issue requests for records through NSIs under these statutory provisions.

Information regarding NSIs, including the number of requests made pursuant to these authorities, is classified. However, as required by statute, the use of NSI authorities is subject to extensive reporting requirements to and oversight by several committees of Congress. The Senate Select Committee on Intelligence and the House Permanent Select Committee on Intelligence receive reporting under 18 U.S.C. § 2709, the Right to Financial Privacy Act, and the Fair Credit Reporting Act. The Senate Banking, Housing, and Urban Affairs Committee and the House Financial Services Committee receive reporting under the Fair Credit Reporting Act. The Senate and House Judiciary Committees receive reporting under 18 U.S.C. § 2709. The Department transmitted these reports to the respective Committees on December 16, 2003; June 29, 2004; and most recently on April 28, 2005. Therefore, Congress currently has all information that is required under the relevant statutes. We acknowledge that certain reports were not filed within the exact statutory timeframe and efforts are underway to ensure continued accurate and timely filing. It is our understanding that these reports are available for review by any Senator and by appropriately cleared staff with a need to know through the Committees that receive them.

Additional classified information responsive to this question is supplied under separate cover.

64. How many requests were made by the Federal Bureau of [Investigation] and how many were made by other government agencies?

ANSWER: Please see above response to question 63.

65. With how many requests did recipients fail to comply?

ANSWER: The Department does not keep statistics regarding non-compliance with NSLs. According to the FBI, non-compliance is a significant problem only with isolated recipients. For instance, the major credit card companies take the position that they are not subject to the Right to Financial Privacy Act and have refused to respond to NSLs because their customer is not the cardholder but the issuing bank. Further, certain credit reporting companies have failed to respond to requests for redacted credit reports or have responded with full credit reports when the NSL sought only limited information.

66. Has the government attempted to enforce any requests judicially? If yes, how many requests has the government attempted to enforce judicially and what was the outcome of these attempts?

ANSWER: The government has never attempted to enforce an NSL judicially, and there is no expressed statutorily created enforcement mechanism for doing so.

67. Have any requests been challenged judicially by the recipient? If yes, how many requests have been challenged and what was the outcome of those challenges?

ANSWER: NSLs issued pursuant to 18 U.S.C. § 2709 have been challenged judicially in one case filed, *Doe v. Ashcroft*, 334 F. Supp. 2d 471 (S.D.N.Y. 2004). In that case, the district court held that NSLs have been applied in a manner that violates the Fourth Amendment and that the statute's non-disclosure requirement violates the First Amendment. The Department of Justice has appealed that ruling to the Court of Appeals for the Second Circuit. The Department's opening brief on appeal was filed on May 24, 2005.

68. Have any recipients challenged judicially a request's nondisclosure requirement? If yes, how many recipients have challenged a nondisclosure requirement and what was the outcome of those challenges?

ANSWER: The nondisclosure requirement in 18 U.S.C. § 2709(c) has been challenged in the *Doe* case (discussed in Question 67 above). The district court held that the non-disclosure requirement violates the First Amendment to the extent that it does not place any limit on the duration of the non-disclosure obligation. That ruling is being challenged by the Department of Justice in the pending Second Circuit appeal.

69. Would the Justice Department object to giving the recipient of a request pursuant to each of these authorities the right to challenge the request in federal court?

ANSWER: The Department of Justice has stated in litigation that an entity or person served with an NSL can challenge the request either: (1) as a defense to any enforcement proceeding commenced by the United States in the face of non-compliance; or (2) through a pre-production action to enjoin enforcement

70. Would the Justice Department object to giving the recipient of a request pursuant to each of these authorities the right to challenge the request's nondisclosure requirement in federal court?

ANSWER: As stated above, the Department of Justice is aware of two Senate bills that enable judicial review of non-disclosure requirements accompanying NSLs: the Electronic Communications Privacy Judicial Review and Improvement Act of 2005 (S. 693), and the SAFE Act (S. 737). The Administration is carefully reviewing these proposals and has not taken a position on either piece of legislation.

In general, however, the Department believes that the nondisclosure requirement accompanying NSLs serves a very important purpose because it is critical that terrorists and spies are not tipped off prematurely about intelligence investigations. Otherwise, they or their conspirators may flee and key information may be destroyed before the government's investigation has been completed. Furthermore, were information identifying the targets of international terrorism and espionage investigations revealed, according to the D.C. Circuit, such disclosures would "inform terrorists of both the substantive and geographic focus of the investigation[,] . . . would inform terrorists which of their members were compromised by the investigation, and which were not[,] . . . could allow terrorists to better evade the ongoing investigation and more easily formulate or revise counter-efforts . . . [and] be of great use to al Qaeda in plotting future terrorist attacks or intimidating witnesses in the present investigation." *Center for National Security Studies v. U.S. Department of Justice*, 331 F.3d 918, 928-29 (D.C. Cir. 2003).

71. In an April 4, 2005 letter to Senator Leahy, Assistant Attorney General William Moschella states that from April 1, 2003, to January 31, 2005, the Justice Department has delayed notification of searches 108 times pursuant to Section 213 of the Patriot Act. According to the letter, "The bulk of uses have occurred in drug cases; but section 213 has also been used in many cases including terrorism, identity fraud, alien smuggling, explosives and firearms violations, and the sale of protected wildlife." For the 108 times notice was delayed, please provide the number of investigations involved and a breakdown of the suspected criminal violations being investigated.

ANSWER: Of the 108 uses of section 213 from April 1, 2003, to January 31, 2005, eighty-two investigations were involved.

The breakdown of section 213 uses in the 108 warrants reported are as follows: seventy-nine uses in drug investigations and six uses in terrorism investigations. Section 213 was also used in the following other criminal investigations: twelve uses in fraud investigations (including, *inter alia*, identity theft, smuggling of counterfeit goods, and visa fraud), three uses in investigations of violent crime, three uses in investigations of human trafficking, one use in a child pornography investigation, one use in an investigation of computer crimes, one use in an extortion investigation, one use in an investigation of public corruption, and one use in an investigation of the sale of protected wildlife.

72. According to the April 4, 2005 letter, the Justice Department cited "seriously jeopardizing an investigation" as the grounds for delaying notice 92 times, and at least 28 times, "seriously jeopardizing an investigation" was the only grounds cited for delaying notice. For the 92 times, please provide the number of investigations involved and a breakdown of the suspected criminal violations being investigated. For the 28 times, please provide the number of investigations involved and a breakdown of the suspected criminal violations being investigated.

ANSWER: In collecting the information to answer this question, we discovered that, in previous surveys, some U.S. Attorneys' Offices had mistakenly reported extensions of delayed-notice search warrants as new warrants, or had reported the same warrant in multiple surveys, while two U.S. Attorneys' Offices had indicated a single use of section 213 when they had used multiple delayed-notice search warrants in a single investigation. These combined errors caused the numbers that we previously reported to Congress to slightly understate our use of "seriously jeopardizing an investigation" as one of the grounds for delaying notice. To the best of our knowledge, the number of times the Department has used "seriously jeopardizing an investigation" as one of the grounds for delaying notice is 95 times, not 92 as previously reported. To the best of our knowledge the number of times the Department has used "seriously jeopardizing an investigation" as the only ground for delaying notice is 32, not 28 as previously reported.

Of the 95 times that "seriously jeopardizing an investigation" was used as one of the grounds for delaying notice, the breakdown is as follows: seventy-three uses in drug investigations, five uses in terrorism investigations, nine uses in investigations of fraud, three uses in investigations of human trafficking, two uses in investigations of violent crime, one use in an extortion investigation, one use in an investigation of computer crimes, and one use in an investigation of public corruption. "Seriously jeopardizing an investigation" was used as one of the grounds for delaying notice in a total of seventy different investigations.

Of the 32 times that "seriously jeopardizing an investigation" was used as the only ground for delaying notice, the breakdown is as follows: twenty-six uses in drug

investigations, two uses in terrorism investigations, two uses in investigations of fraud, one use in an investigation of violent crime, and one use in an investigation of computer crimes. "Seriously jeopardizing an investigation" was used as the only ground for delaying notice in a total of twenty-two different investigations.

73. Your written testimony states that Section 215 "expressly protects First Amendment rights." The provision that you referred to provides that an investigation of a U.S. person shall not be conducted "solely upon the basis of activities protected by the first amendment to the Constitution." This provision seemingly only protects First Amendment activities if they are the sole basis for the investigation. For example, suppose the government wanted to investigate an Arab-American leader on the basis of his ethnicity and his public criticism of the war in the Iraq. Would the law allow such an investigation, because it is not based solely on the individual's First Amendment activities?

ANSWER: That provision of section 215 provides significant protection for the First Amendment rights of U.S. persons. At the same time, it appropriately recognizes that activities potentially protected by the First Amendment need not be entirely excluded from consideration in conducting an international terrorism or clandestine intelligence investigation where there is a broader predicate for the investigation, which would be the result if the word "solely" were eliminated from the statute. It should also be noted that, although section 215 prohibits only investigations of U.S. persons conducted "solely upon the basis of activities protected by the first amendment to the Constitution," there are circumstances in which other provisions of law, including the Constitution, and guidelines issued by the Attorney General under Executive Order No. 12333, would prohibit investigations solely based on ethnicity and activities protected by the First Amendment.

74. Your written testimony states that, "Section 215 provides for thorough congressional oversight that is not present with respect to grand-jury subpoenas." As an example, you cited the fact that you, as the Attorney General, are required to "fully inform" appropriate congressional committees concerning all requests for records under section 215." However, the Patriot Act only requires you to fully inform the House and Senate Intelligence Committees, not the House and Senate Judiciary Committees, even though the Judiciary Committees have oversight responsibility for the FBI and the Foreign Intelligence Surveillance Act. Would you support revising the Patriot Act to require the Attorney General to fully inform the Senate and House Judiciary Committees on the use of Section 215?

ANSWER: The Department already provides twice a year a detailed report to comply with the requirement that it fully inform Congress of its implementation of FISA, including its use of section 215. This highly classified report, classified at the Top Secret - Sensitive Compartmented Information (SCI) level, is provided to the Senate Select Committee on Intelligence and the Permanent Select Committee on Intelligence of the House of Representatives. We understand that this report is available through those

Committees for review by any member of Congress and by appropriately cleared staff who have a need to know.

75. In your written testimony, you suggested that concerns about so-called "John Doe" roving wiretaps are unfounded because FISA "requires our attorneys to provide a description of the target of the electronic surveillance to the FISA Court." However, FISA does not require the description for a wiretap to contain any level of specificity. The description seemingly could be as vague as "Arab man" or "African-American woman." Would you have any objection to revising FISA to make clear that the description must include some information other than just the race or ethnicity of the target and must contain sufficient detail to identify the person with reasonable certainty?

ANSWER: Yes, because we believe that FISA already requires sufficient specificity. FISA currently requires that each electronic surveillance application include "the identity, if known, or a description of the target of the electronic surveillance[.]" see 50 U.S.C. § 1804(a)(3), and each order approving electronic surveillance must specify "the identity, if known, or a description of the target of the electronic surveillance[.]" See 50 U.S.C. § 1805(c)(1)(A). While in some cases the government might not know the name of the terrorist or spy in question, it can only obtain authorization to conduct surveillance of that individual if it satisfies the FISA Court that there is probable cause to believe the target is a foreign power or its agent. Therefore, simple identification by ethnicity, such as "Arab man" or "African-American woman," would not appear to be sufficient to meet the requirements of FISA. Finally, it is important to remember that FISA has always required that the government conduct every surveillance and search pursuant to appropriate minimization procedures that limit the government's acquisition, retention, and dissemination of communications of Americans. Both the Attorney General and the FISA court must approve those minimization procedures. Taken together, we believe that these provisions adequately protect against unwarranted governmental intrusions into the privacy of Americans.

Follow up Questions for Senator Grassley

On April 1, 2005 the Department of Justice responded to a request by Judge T.S. Elias III to enter a brief in the matter of *United States ex rel. DRC, Inc. et al., v. Custer Battles, LLC* in the Federal District Court for the Eastern District of Virginia. The brief was requested by the court in an effort to determine whether or not the False Claims Act (FCA) applied to contracts entered into by the Coalition Provisional Authority (CPA) during the reconstruction of Iraq. Finding that the FCA did in fact apply to contracts with the CPA, the Department of Justice stated that claims presented to the CPA would violate the FCA when: the claims were knowingly false, for funds in which the U.S. had an interest or exercised dominion over, and were ultimately presented to an officer or employee of the United States government.

76. While I am pleased that the Department of Justice has honored the commitment you made to me during your confirmation hearing to protect the FCA, I have significant concerns regarding this matter that remain unanswered. Specifically, could you please provide a detailed response to me explaining why the Department of Justice declined to intervene in this important matter? Further, could you please provide me a detailed response explaining why the Department of Justice has not reconsidered its position in light of the brief filed on April 1, 2005?

ANSWER: In addition to the brief filed by the Department in *Custer Battles* on April 1, 2005, the United States on April 22, 2005, filed a supplemental brief further stating "[t]he United States believes that the CPA is an instrumentality of the United States for purposes of the False Claims Act."

As a matter of practice, and in order to allow a relator to continue to proceed against a defendant as to whom the Department has declined to intervene without being prejudiced as the *qui tam* statute contemplates, the Department never publicly states the reasons for its declination decisions. To be sure, when a defendant has attempted to represent a declination decision as a governmental determination that the *qui tam* case against it lacks merit, we have been quick to point out that declination decisions cannot be so interpreted and there are many possible grounds for declining.

As you are well aware, the *qui tam* provisions of the False Claims Act give the United States the right to intervene in a previously declined *qui tam* case for good cause shown. The Department remains open in all declined *qui tam* cases to review new evidence and/or developments to consider whether to exercise this authority. That policy is in full effect in connection with the *Custer Battles* case and in that regard we remain in contact with the relator's attorneys.

77. Additionally, could you please tell me if the Department of Justice will be willing to support its current position and intervene in other FCA cases that could possibly arise from contracts entered into with the CPA during the reconstruction of Iraq?

ANSWER: The position of the United States is as stated in the two briefs filed by the government in the Custer Battles litigation. Should we receive new allegations of possible False Claims Act violations, whether through new *qui tam* actions or otherwise, arising from contracts entered into with the CPA during the reconstruction of Iraq that fall within the parameters of the position set forth in our Custer Battles briefs, we would certainly consider intervening or otherwise pursuing such allegations.

Follow up Questions from Senator Biden

In your opening statement, you reported that “from the enactment of the Patriot Act through January 31, 2005, the department used Section 213 to request approximately 155 delayed-notice search warrants, which had been issued in terrorism, drugs, murder and other criminal investigations”.

89. Of the 155 warrants, how many were issued in terrorism investigations?

ANSWER: In collecting the information to answer this question, we discovered that, in previous surveys, some U.S. Attorneys’ Offices had mistakenly reported extensions of delayed-notice search warrants as new warrants, or had reported the same warrant in multiple surveys, while two U.S. Attorneys’ Offices had indicated a single use of section 213 when they had used multiple delayed-notice search warrants in a single investigation. These combined errors caused the numbers that we previously reported to Congress to slightly overstate our use of section 213. To the best of our knowledge, the Department has used section 213 from the enactment of the PATRIOT Act through January 31, 2005, is 153, not 155 as previously reported. Eighteen of these uses involved terrorism investigations.

90. How many were issued in drug investigations?

ANSWER: Section 213 was used in drug investigations a total of ninety-seven times.

91. How many were issued in “other criminal investigations”?

ANSWER: Section 213 was used in “other criminal investigations” a total of thirty-eight times.

In your letter to Senator Leahy of April 4, 2005, you note that, under Section 213, federal judges have approved delays of notice of a search ranging from seven to 180 days.

92. How do these periods of delay compare to the pre-Patriot Act era, during which several Courts of Appeal authorized the use of delayed notice searches?

ANSWER: In the pre-USA PATRIOT Act era, during which several courts across the country authorized use of delayed notice searches, the Department did not keep records as to the length of delays authorized. As a result, we are unable to make a meaningful comparison between pre-USA PATRIOT Act and post-USA PATRIOT Act practice.

93. As you know, critics of the PATRIOT Act have alleged that section 213 does not proscribe any specific temporal limit for the delayed notice to the target(s) of the intercepted communication. This appears to be unique within the federal criminal law section of the U.S. Code, including Titles 18 and 21. While different sections proscribe different temporal limits, all such statutes appear to delimit some outer limit by which, absent good cause shown, the government must notify targets of searches or surveillance. Under 18 U.S.C. 2518(8)(d), for example, the government must notify all individuals whose communications were intercepted under a criminal wiretap “[w]ithin a reasonable time but not later than ninety days” after the conclusion of the wiretap, absent “good cause” shown to the court.

ANSWER: Please see response to question 94, below.

94. Are you aware of any other federal criminal statute, other than section 213, which does not contain a specific time limit?

ANSWER: There are a number of provisions of federal criminal law and procedure that do not set forth a specific time period within which notice must be made. To give two examples: (1) in regard to pen register and trap and trace devices, if no prosecution results from the investigation in which these are utilized, no notice need ever be given to the subject of these; and (2) in regard to permissible disclosure of grand jury matter under section 203 of the USA PATRIOT Act, notice of such disclosure must be made to the court within a reasonable period of time.

95. If not, can the Justice Department provide any reason why Congress should not impose some reasonable time period, as occurs for example in the Title III context?

ANSWER: Determinations of what constitutes a reasonable period of delay should be determined at the outset by a judge who has familiarity with the facts of the individual investigation. Under existing law, judges have the discretion to delay notice for a time period they determine to be reasonable on a case-by-case basis.

As you pointed out during the hearing, the Department of Justice has not changed its organization at all to reflect its post-9/11 recalibrated mission. The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction (“WMD Commission”) labeled your current organizational structure, where the Criminal Division’s Counterterrorism Section and Counterespionage Section report to two different Deputy Assistant Attorneys General, “madness”. The WMD Commission also noted that the Department’s third national security component, the Office of Intelligence Policy and Review, operates independently of the Criminal Division and reports directly to the Deputy Attorney General.

97. What are your views on the WMD Commission's recommendation that we create an Assistant Attorney General for National Security, and place him or her in charge of OIPR, Counterespionage, and Counterterrorism?

ANSWER: The WMD Commission's recommendation raises some very challenging issues for the Department. Nevertheless, the proposal for restructuring the Department's approach to its national security mission merits careful consideration, and, as explained in our response to earlier questions, the Commission's recommendations have been part of a comprehensive review the Attorney General has commissioned.

98. Should this new AAG for National Security also have the Criminal Division under their control? You noted during the hearing that "in the interagency process, I fear that sometimes the department is not as well represented as it should be. If I'm not available, or if a deputy attorney general is not available, then it really falls down to sort of a deputy assistant attorney general and sometimes that's probably not the best representation for the department. And some very decisions [sic] have to be made on the interagency process."

ANSWER: The WMD Commission has suggested only that a National Security Division might include the Counterterrorism and Counterespionage Sections of the Criminal Division. Even if a restructuring of that sort has advantages – an issue that we are still in the process of examining – we do not believe that it would make sense to place *all* of the functions of the Criminal Division within a National Security Division. Although it is true that many criminal cases may end up having counterterrorism or other national security aspects to them, the entire range of federal criminal law enforcement functions handled by the Criminal Division should not be placed under a National Security Division.

99. Would the structure recommended by the WMD Commission align the Department's managerial levels with those of other national security agencies so that the Department is better represented in the interagency process?

ANSWER: Creating a division within the Department of Justice that handled intelligence and national security matters might have the effect of providing the Department a management tier over such issues that could represent the Department more effectively in the interagency process. That is one factor that the Administration is examining in its consideration of the WMD Commission's recommendations.

100. Can you commit to me that, should the Administration seek to make changes to the Department's organization, it will do so through legislation considered in its authorizing committees, and not through executive action or the appropriations process?

ANSWER: The Department will not seek to reorganize itself unless the proposed restructuring will serve to further protect the lives and liberties of Americans. Such a decision would be premised on an assessment that the proposed reorganization will render the Department more effective in fulfilling its obligations to the American people than it is now. Moreover, the Department will not proceed with any restructuring of the comprehensive sort recommended by the WMD Commission absent a decision by the President and consultation with the Congress.

101. Do you agree with me that any new assistant attorney general overseeing national security matters should be a presidential appointee considered for confirmation by this Committee?

ANSWER: It would be premature to comment further until a concrete proposal and exact responsibilities of such a position have been defined.

Section 108 of P.L. 108-21, the PROTECT Act, established two separate 18-month pilot programs for certain organizations to obtain national criminal history background checks. When signing the PROTECT Act into law, the President noted "this law creates important pilot programs to help nonprofit organizations which deal with children to obtain quick and complete criminal background information on volunteers. Listen, mentoring programs are essential for our country, and we must make sure they are safe for the children they serve." The pilot programs commenced in August, 2003. Section 6401 of P.L. 108-458 extended these pilot programs for 12 additional months, but they will expire in early 2006 unless Congress acts. Section 108(d)(1) required you to conduct a study of these pilot programs, and Section 108(d)(2) required you to submit an interim report concerning the implementation of these provisions "not later than 180 days after the date of enactment" of P.L. 108-21. The interim report was due to Congress in February, 2004. It has not yet been submitted to Congress.

102. What is the status of the interim report required by Section 108(d)(2)?

ANSWER: The foundation for the interim report required by section 108(d)(2) of the Prosecutorial Remedies and Other Tools to end the Exploitation of Children Today Act of 2003 (Protect Act) is a detailed feasibility currently study being conducted by the Department of Justice. The Federal Bureau of Investigation (FBI) has been tasked with completing this feasibility study and with drafting the resulting report. The feasibility study is highly dependent on information generated by the implementation of the two pilot programs launched by the FBI on July 29, 2003. Because of the complexity of the programs, it took some time for the two pilot programs to be fully implemented and for a significant number of names of volunteers to be processed. For example, as of May 22, 2004, the fingerprints of only 1,470 volunteers had been submitted under the pilots. This limited participation in the pilots at the outset delayed the gathering of information needed to develop a meaningful feasibility study and interim report. As of April 21,

2005, approximately 8,800 fingerprints submissions have been received under the pilots. While the FBI has now gathered most of the information needed to complete the feasibility study, it is still in the process of gathering supplemental information needed for the report. The interim report will be completed as soon as the remaining information has been gathered and analyzed.

103. Do you agree with the President that these pilot programs are “important”?

ANSWER: The Department of Justice agrees that the two pilot programs are important. The information gathered from these two pilot programs will help to determine the level of interest of volunteer organizations in having background checks conducted of volunteers who work with children. In addition, the pilot programs also will help identify any barriers there may be to increased use of such checks by volunteer organizations and determine which methods of conducting background checks of volunteers are most effective.

104. In light of the importance the President ascribes to these programs and the emphasis given mentoring programs by this Administration, do you agree with me that these pilot programs should be made permanent, or at least extended beyond February, 2006? Section 108(d)(3) requires you to submit a final report “not later than 60 days” after completion of the pilot program.

ANSWER: A decision to make the two pilot programs permanent would be premature until the feasibility study is completed and Congress has an opportunity to review the results of the required reports. The pilots were designed narrowly, to test the value and effects of different approaches to processing these checks -- e.g. processing the checks through the states vs. directly through the FBI, and any potential role of private sector services in conducting such checks. They were not intended as a permanent process for these checks. The Department of Justice believes, however, that the background checks being conducted under the pilots are of value to the organizations that are taking advantage of their availability. As a result, the Department would not object if Congress decides to extend the two pilot programs until it has had a chance to review the reports and determine what next steps are appropriate.

105. In light of the amendment made to Section 108 by P.L. 108-458, when do you expect to submit the final report required by Section 108(d)(3) to Congress?

ANSWER: The Department of Justice will have only 60 days to submit the final report after the conclusion of the two pilot programs. The two pilot programs currently are scheduled to terminate on January 30, 2006. Therefore, the final report will be due by March 30, 2006. The Department expects that the efforts made in developing the feasibility study and the interim report will provide a solid basis for preparing the final report and will make every effort to meet that deadline.

Follow up Questions from Senator Feingold

These questions concern delayed notification search warrants, which were authorized in Section 213 of the Patriot Act.

106. At the hearing, I asked you about a Supreme Court case, *Dalia v. United States*, that was cited in the Justice Department's April 4, 2005 letter regarding delayed notification search warrants. The Court found that the Fourth Amendment permits the government to install a bug in someone's home via covert entry because delayed notification was the "only means by which the warrant effectively may be executed." Do you agree that that standard is stricter than the one codified by the Patriot Act and the one put forth in the SAFE Act? Given the narrow circumstances addressed in that case, do you agree that the *Dalia* decision does not answer the question of whether Section 213 is constitutional under the Fourth Amendment?

ANSWER: The Supreme Court's decision in *Dalia* supports the constitutionality of delayed-notice search warrants. As the *Dalia* court explained, it is "frivolous" to argue "that covert entries are unconstitutional for their lack of notice." The courts of appeals that have specifically upheld the constitutionality of delayed-notice warrants have not interpreted *Dalia* to hold that delayed notice is constitutional only upon a showing that it would be "the only means by which the warrant effectively may be executed." Nor have they held that delayed-notice is only constitutional for installation of a listening device as opposed to execution of a search warrant. Rather, they have upheld the constitutionality of delaying notice of a warrant where immediate notice would have a harmful result. For example, the Second Circuit stated that officers seeking a delayed-notice search warrant must satisfy a court that "there is good reason for delay." Section 213, which requires the court to find that providing immediate notice may have an "adverse result" is consistent with these decisions.

108. In the Department's April 4, 2005, letter to me about delayed notice searches, you stated: "The dilemma faced by investigators in the absence of delayed notification is even more acute in terrorism investigations where the slightest indication of governmental interest can lead a loosely connected cell to dissolve." In that circumstance, why couldn't the government obtain a permanently secret search warrant under the Foreign Intelligence Surveillance Act (FISA)?

ANSWER: Although FISA continues to be an option where appropriate based on the facts and circumstances of the particular case, FISA is not available in domestic terrorism investigations and in cases in which the government does not have probable cause that the target of the search is an agent of a foreign power, as that term is defined in FISA.

The Patriot Act expanded the FBI's authority to obtain real-time, non-content information about telephone and computer communications by making it easier to obtain pen register and trap and trace device orders and by clarifying that the pen/trap authority applies to Internet as well as phone communications. As you acknowledged in the hearing, the line between content and non-content information is sometimes hard to draw in the context of Internet communications. I understand from Deputy Attorney General Comey's April 1, 2005, responses to congressional questions that the Department requires field agents encountering these gray areas with regard to the use of pen/traps to consult with Main Justice.

109. How does the Justice Department evaluate whether an aspect of Internet communications, such as a URL, constitutes "content"?

ANSWER: In evaluating whether an aspect of any communication – whether transmitted on the Internet or by other means – is "contents," the Department looks to the statutory definition at section 2510(8) of Title 18, United States Code. That definition refers in pertinent part to "information concerning the substance, purport, or meaning of [the] communication." We also look at the definitions of electronic surveillance under FISA found in 50 U.S.C. section 1801(f).

113. You stated at the hearing that you would support amendments to Section 215 of the Patriot Act to clarify that the recipient of a Section 215 order may consult with an attorney and may challenge the order in court. Would you also support similar amendments to the National Security Letter provisions?

ANSWER: As stated above, the Department of Justice is aware of two Senate bills that enable judicial review of non-disclosure requirements accompanying NSLs: the Electronic Communications Privacy Judicial Review and Improvement Act of 2005 (S. 693), and the SAFE Act (S. 737). The Administration is carefully reviewing these proposals and has not taken a position on either piece of legislation. The Department of Justice has stated in litigation that an entity or person served with an NSL can challenge the request either: (1) as a defense to any enforcement proceeding commenced by the United States in the face of non-compliance; or (2) through a pre-production action to enjoin enforcement. The Department has also stated in litigation that the recipient of an NSL may consult an attorney regarding the request for records.

114. You stated at the hearing that Section 215 orders have been used to obtain "names and addresses for telephone numbers captured through court-authorized pen register devices." You also stated that "the department anticipates that the use of Section 215 will increase as we continue to use the provision to obtain subscriber information for telephone numbers captured through court-authorized pen register devices." In what circumstances would the FBI obtain a Section 215 order for this type of subscriber information, and in what circumstances would the FBI use a National Security Letter under 18 U.S.C. § 2709?

ANSWER: A pen register/trap and trace device ("pen register") is an investigative tool used with respect to telephone companies and other electronic service providers in both criminal investigations and intelligence investigations. When used with respect to a telephone, a pen register records the numbers called from the telephone and the numbers from which the telephone is called, but it does not identify the subscribers to those numbers.

In order to obtain subscriber information (i.e., the name and address of the person or entity associated with a particular number), some sort of legal process is required if the number does not appear in public databases. The most commonly used processes are: grand jury subpoenas and orders pursuant to 18 U.S.C. § 2703(d) in the criminal context, and National Security Letters ("NSLs") under 18 U.S.C. § 2709 and 215 orders in the intelligence context.

In the criminal context, investigators have for many years obtained orders under 18 U.S.C. § 2703(d) at the same time as they obtain orders authorizing pen registers. Both orders are served on the telephone company or other electronic service provider furnishing the service targeted by the pen register. Pursuant to these orders, the service provider will produce approximately contemporaneous subscriber information for the numbers called by the target number or from which the target number is called.

The FBI had long sought to use a similar mechanism in intelligence investigations. The decision was made to present the Foreign Intelligence Surveillance Court with a combined FISA pen register order and 215 order to create such a mechanism. Now, when a FISA pen register is served on an telephone company or other electronic communication service provider, it is served along with a 215 order that requires the ongoing provision of subscriber information on all numbers calling or called by the target number.

In all other instances in which the FBI seeks subscriber information for telephone numbers in the course of intelligence investigations, the FBI anticipates the continued use of NSLs.

According to Deputy Attorney General Comey's April 1, 2005, response to congressional questions, the President's Board on Safeguarding Americans' Civil Liberties, which the President created in August by Executive Order, has met six times.

115. Is any information about the proceedings of the President's Board going to be made public?

ANSWER: At this time, the President's Board on Safeguarding Americans' Civil Liberties ("the Board") has not made public any information about its internal deliberations. The Board, however, intends to provide the Privacy and Civil Liberties

Oversight Board (created by the Intelligence Reform and Terrorism Prevention Act of 2004) relevant survey results and other information collected by the Board and its subgroups.

116. What has been discussed at the six meetings of the President's Board, and who has attended? Were any decisions made?

ANSWER: As stated above, at this time the President's Board on Safeguarding Americans' Civil Liberties does not intend to make public any information about its internal deliberations.

117. In 2000, Attorney General Reno ordered that the Department's National Institute of Justice contract for a thorough study about how the federal death penalty was being applied, and in 2000 and 2001 the Justice Department issued detailed statistics about federal death penalty prosecutions. In connection with your confirmation hearing, I asked you about the status of the study, and asked you to commit to update the 2001 statistical information about federal death penalty prosecutions so that the public can evaluate how the death penalty has been implemented in the past four years. You said that you would "consider whether the compilation of such data and statistics contributes in a meaningful way to an assessment of capital charging decisions or prosecutions." Will you now commit to updating DOJ statistical information on federal death penalty prosecutions?

ANSWER: The Department has already expended considerable resources in the analysis of capital charging decisions, releasing, in September 2000, a massive compilation of statistics pertaining to the cases submitted for the Department's death penalty protocol review and in May 2001, supplemental statistics pertaining to a limited number of potential capital cases not encompassed by the former protocol review process. In addition, the National Institute of Justice funded a total of \$1,568,793 for the follow-up studies suggested by former Attorney General Reno to investigate factors not revealed by the Department's statistical release. It would be inappropriate to expend resources on further studies or statistical compilations until those studies have been concluded. If at the conclusion of both of these studies, we are convinced that the compilation of such data and statistics contributes in any meaningful way to an assessment of capital charging decisions or prosecutions, we will consider undertaking such a project.

Follow up Questions from Senator Kyl

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

ANSWER: If Section 201 of the USA PATRIOT Act is allowed to expire, thereby removing the chemical-weapons and terrorism-related predicate offenses set forth in new 18 U.S.C. 2516(1)(q), the list of Title III predicates contained at 18 U.S.C. 2516(1) would still include offenses involving biological weapons (18 U.S.C. 175) and prohibited transactions involving nuclear materials (18 U.S.C. 831), as well as any non-specific significant offenses that might otherwise apply, such as Racketeer Influenced and Corrupt Organizations (18 U.S.C. 1962) and Interstate and Foreign Travel in Aid of Racketeering (18 U.S.C. 1952). Still, the loss of the specific USA PATRIOT Act-added Title III predicates involving chemical weapons and violations of the comprehensive terrorism laws in Chapter 113B of Title 18, United States Code, would be a significant blow to the usefulness of Title III in the War on Terror. While other statutes might be available to investigators to provide one or more predicate offenses to justify a wiretap application, resorting to those alternatives would likely require further investigation to fashion a viable approach in the government's application to the court for a Title III order, which would almost certainly delay the investigation at a very critical stage. Because of the nature of the offenses involved, any such delay could have devastating consequences.

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

ANSWER: You are correct. Messages on an answering machine could be obtained via search warrant (or even through issuance of a subpoena to the owner), while the pre-USA PATRIOT Act statutory rules applicable to voicemail messages required law enforcement to seek a wiretap order to obtain stored voice messages held by a third-party service provider. This distinction made no sense, just as it made no sense for stored voicemail to be more difficult to obtain than stored non-voice communications (such as email): the government has long been authorized to obtain stored user e-mail from a provider by means of a warrant. See 18 U.S.C. § 2703.

120. Section 212 of the USA PATRIOT Act allows Internet service providers to voluntarily disclose customer communications and records in life-threatening emergencies. It is my understanding, however, that the Homeland Security Act repealed the portion of section 212 governing the disclosure of the content of

communications in emergency situations, and placed a similar authority in a separate statutory provision. Therefore, would there be any significant change in the law if section 212 were allowed to expire?

ANSWER: There would be significant negative impact if section 212 were allowed to sunset. Section 212 relocated the rules for permissive disclosure of non-content customer records from 18 U.S.C. § 2703(c) to § 2702(c), and – in section 212(b) – made corresponding adjustments to the numbering scheme within § 2703(c). (Section 210, not subject to sunset, depends upon that renumbering.) Allowing section 212 to sunset would produce enormous confusion, as the interdependencies of the amendments – sunset and non-sunset – would be broken, producing essentially unreadable statutory text in a law crucial to law enforcement’s ability to combat Internet crime. In addition, it would restore a statutory anomaly imposing greater restrictions on the voluntary disclosure of non-content customer records than on the disclosure of content.

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

ANSWER: Section 212 has been used often and has already saved lives. To give just a few examples, voluntary disclosures from computer service providers pursuant to section 212 have assisted law enforcement in safely recovering an 88-year-old Wisconsin woman who was kidnapped and held for ransom while bound in an unheated shed during a cold Wisconsin winter and in safely recovering four kidnapped or missing children. For instance, a few months ago, Bobbie Jo Stinnett of Skidmore, Missouri, who was eight months pregnant, was found strangled in her home lying in a pool of her own blood. Her unborn daughter had been cut out of her womb with a kitchen knife. Police officers examined a computer found in Ms. Stinnett’s home. They discovered that she had been active on the Internet in connection with her dog-breeding business. As the investigation intensified, the officers found an exchange from a message board between Ms. Stinnett and someone who called herself Darlene Fischer. Fischer claimed to be interested in a dog. She had asked Ms. Stinnett for directions to her house for a meeting on December 16—the same day as the murder. Using section 212, FBI agents and examiners at the Regional Computer Forensic Laboratory in Kansas City were able to obtain information that led them to Fischer’s messages to a server in Topeka, find Darlene Fischer’s email address, and then trace it to a house in Melvern, Kansas. Darlene Fischer’s real name was in fact Lisa Montgomery. Montgomery was arrested and subsequently confessed, and baby Victoria Jo Stinnett was found alive—less than 24 hours after she was cut from her mother’s womb.

Section 212 was also used to foil an alleged kidnapping plot that turned out to be an extortion racket. Additionally, the provision has been used to successfully respond to a cyber terrorist threat to the South Pole Research Station, a bomb threat to a high school, a threat to kill the employees of a European company as well as their families, and a threat to burn down an Islamic mosque in Texas. In all of these cases, voluntary

disclosures from Internet service providers were critical to apprehending the perpetrators before their threats could be carried out.

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

ANSWER: Yes. All requests for the production of records under section 215 of the USA PATRIOT Act must be approved by a federal judge. Grand jury subpoenas requesting the production of records, by contrast, are issued by federal prosecutors without prior review by a judge.

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

ANSWER: That is a baseless criticism. Section 220 amended 18 U.S.C. § 2703 to enable "a court with jurisdiction over the offense under investigation" to issue warrants and other orders for evidence held by service providers in other districts. The amendment addressed a problem under the prior version of the statute: if a federal prosecutor in New York needed evidence from an Internet service provider in California, the prosecutor and the case agent were obliged to contact federal law enforcement officials in the other district, involve them in the case, and have them apply for the evidence before a federal judge in California. This time-consuming process necessitated a needless waste of scarce law enforcement resources, and imposed substantial burdens on a few districts (in California and Virginia, especially) in which major service providers are located.

Section 220 does not allow investigators to seek search warrants for electronic evidence from any court in the country. Rather, it allows investigators to seek a search warrant only in a court with jurisdiction over the offense under investigation. Thus, for example, while a court in Ohio may issue a search warrant for electronic evidence stored in California in the investigation of a murder committed in Ohio, a judge located in a district with no connection to the investigation, such as North Dakota, is not allowed to issue such a warrant. In practice, judges and prosecutors with the most knowledge of a particular investigation are now permitted to process requests for search warrants to

obtain electronic evidence in that investigation, without needlessly involving a judge in a remote district where the case will not be tried.

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

ANSWER: The Department has yet to use this provision. The USA PATRIOT Act, by its terms, provided for habeas corpus review of certification and subsequent decisions to continue detention. "Judicial review of any action or decision relating to this section (including judicial review of the merits of a determination made under subsection (a)(3) or (a)(6) is available exclusively in habeas corpus proceedings consistent with this subsection." 8 U.S.C. § 1226a(b)(1). Appeals from such decisions on habeas corpus may be taken to the United States Court of Appeals for the District of Columbia. 8 U.S.C. § 1226a(b)(3).

Follow up Questions from Senator Leahy

128. Section 203(a) of the PATRIOT Act authorized criminal investigators to disclose grand jury information to the CIA and other intelligence agencies, but required post-disclosure notification to the court. Can you give us a sense of how the notice requirement in section 203(a) has worked in practice? Has it interfered with information-sharing in any significant way, and if so, how?

ANSWER: We do not believe that the notice requirement in section 203(a) has significantly interfered with information sharing. The notice requirement in section 203(a) accords with long-standing grand jury practice, pursuant to which government attorneys file notices with the court reporting certain disclosures of grand jury information. Because it is limited to grand jury information, the notice requirement in section 203(a) is not especially onerous. For these reasons, the Administration is not seeking the repeal of the notice requirement in section 203(a).

141. Section 217 of the PATRIOT Act allows computer service providers that are victims of attacks by computer trespassers to authorize persons acting under color of law to monitor trespassers on their computer systems in a narrow class of cases. If Congress renews section 217, would the Department agree to report on its use on an annual basis, and if not, why?

ANSWER: Because reporting requirements necessarily reduce the time available to prosecutors and investigators to pursue cases, the Department does not support imposition of a new reporting requirement with respect to this provision. Service providers have long been able to monitor their own networks to guard against harm to their "rights or property" (18 U.S.C. 2511(2)(a)(i)), as well as to disclose to law enforcement the resulting evidence of wrongdoing. See, e.g., *United States v. Harvey*, 540 F.2d 1345, 1352 (8th Cir. 1976). Such disclosures have never been subject to a reporting requirement, and the Department does not believe it any more necessary to report the common-sense measures taken under the authority of Section 217 to protect the rights and privacy of victim computer owners and their users.

143. Was notice provided to Portland attorney Brandon Mayfield pursuant to this provision, and if so, on what date?

ANSWER: By letter dated March 24, 2005, the Department of Justice voluntarily notified Mr. Mayfield that he was the target of physical searches of his residence and of electronic surveillance and other physical searches authorized pursuant to FISA.

When the PATRIOT Act was being negotiated, your predecessor sought the authority to detain aliens suspected of terrorism indefinitely without charge. Section 412 of the Act, while not as broad as the Justice Department requested, gives the executive branch considerable authority to hold such aliens.

147. Has this provision ever been used?

ANSWER: No.

148. If not, why not?

ANSWER: As of yet, there has not been a suitable case for invoking the provision.

149. If this provision has never been used, do you believe it should be retained?

ANSWER: The provision should be retained because it is reasonably conceivable that it could be needed in the future. If the release of an alien would present national security concerns, the government needs the statutory authority to detain the alien. Indeed, for this reason, Congress should more clearly establish the government's detention authority. Section 412 suffers from three potential infirmities. First, the statute does not expressly authorize post-order detention. Second, an alien could argue that detention is impermissible unless the Attorney General certifies that the alien is a danger before the alien is taken into custody, 8 U.S.C. § 1226a(a)(1), and before removal proceedings begin, 8 U.S.C. § 1226a(a)(5). Third, one could contend that classified information may not be used in these proceedings. Although the Department does not find these arguments convincing, there is no reason to run the risk that a court might be persuaded. When an alien is a terrorist or presents other national security concerns, the statute should eliminate any doubt that the government is equipped to protect the American people. Congress should eliminate these potential problems by clarifying the government's detention authority. Moreover, Congress should also establish that the government has the authority to detain beyond six months an alien who presents a danger to the community or to foreign policy. In the wake of *Zadvydas v. Davis*, 533 U.S. 678 (2001) and *Clark v. Suarez-Martinez*, 125 S.Ct. 716 (2005), such express authority is necessary to protect the American public from harm. Finally, it is worth noting that detention decisions under Section 412 are judicially reviewable, so if the government does decide to invoke Section 412, the alien will have access to federal court review.

150. In your written answer to a question (#16) that I submitted following your confirmation hearing, you stated: "The material witness statute should not be used as a broad preventative detention law, to hold suspects indefinitely while investigating them without filing charges. Nevertheless, the fact that the person who is detained as a material witness also is a suspect in the underlying criminal investigation should not prevent the Government from attempting to obtain the

person's testimony through lawful means." Suppose that a suspect detained as a material witness invokes his Fifth Amendment right not to be a witness against himself. If the Government chooses not to grant him immunity for his testimony, can the Government continue to hold him as a material witness, with no reasonable prospect that this will enable the government to obtain and preserve his testimony?

ANSWER: There are adequate checks and balances in the system to prevent abuse.

Most notably, the detention of any material witness must be ordered by a judicial officer, and a detention order is subject to review or appeal within the judiciary branch. It is not up to the Department to unilaterally decide to detain a person as a material witness *at all*, much less indefinitely. Under 18 U.S.C. § 3144, a judicial officer must determine whether the witness's testimony is material in a criminal proceeding, and whether it is impracticable to secure the person's presence by subpoena. Only then can the court order that the material witness be detained pending his testimony.

At the detention hearing, the material witness may be represented by an attorney, and counsel will be appointed if the witness cannot afford one. The material witness has the ability to challenge the basis for detention at the detention hearing itself, and may seek a review of the detention hearing under § 3145(b), or may file an appeal of an order of detention under § 3145(c). If a court finds that the person does not meet the criteria of § 3144, the court may not detain that person as a material witness.

Once a court orders detention, a material witness still has an avenue to challenge his detention. Under the provisions of § 3142(f), the detention hearing may be reopened, either before or after a determination by the judicial officer, if the judicial officer finds that information exists that was not known to the movant at the time of the hearing and that the information has a material bearing on the reasons for detention.

To fully address the hypothetical scenario you describe would require more facts to give a definitive answer, but generally, the material witness could be detained up to the time that he appears before the grand jury and invokes the Fifth Amendment. At that time, if we were not willing to grant the witness immunity, we would go back to the court and inform the court of the circumstances. If, in fact, the witness did not have any further testimony material to the proceeding that could be given, there would most likely be no basis for further detention.

Finally, it remains the Department's position that, even though in certain circumstances it may be proper to seek a material witness warrant for a suspect in the underlying investigation, the material witness statute should not be used to hold suspects indefinitely while investigating them without filing charges. That is not the purpose of the material witness statute.

151. In your same response to question #16, you declined to comment on some proposed changes to the material witness statute, saying that you "would have to

consult with the experts in the Department of Justice to assess the impact the amendments would have on the administration of justice.” Now that you have had an opportunity to consult with DOJ experts, would you support amending 18 U.S.C. §3144 to limit the “reasonable period of time” that a witness may be detained to a time certain (e.g., no more than 3 days, consistent with the requirements of 18 U.S.C. §3142(f)(2)) or, alternatively, to require that the witness’s testimony be taken, whether by grand jury or deposition, at the first available opportunity?

ANSWER: Because the detention of material witnesses is dealt with under § 3142, the provisions of § 3142(f) to which you refer already apply in the case of the detention of a material witness. Under that section, a material witness is entitled to a *detention hearing* before a judicial officer immediately on the witness’s first appearance before a judicial officer, unless either the witness or the government seeks a continuance. Except for good cause, on a motion from the government, the hearing may be continued for no more than three days, and on a motion from the witness, the hearing may be continued no more than five days.

At the hearing, the judicial officer will determine whether the individual’s testimony is material to a criminal proceeding, and whether it is impracticable to secure the presence of the witness by subpoena. The material witness is afforded an opportunity to testify, to present witnesses, to cross-examine witnesses and to present information by proffer or otherwise. The hearing may be reopened before or after a determination by the judicial officer, if the judicial officer finds that information exists that was not known to the movant at the time of the hearing and that has a material bearing on the issue whether there are conditions of release that will reasonably assure the appearance of the person.

We would oppose any specific time limitation on the detention of material witnesses subsequent to a court order, for a number of reasons. First, and most significantly, districts vary significantly in how and when their grand juries convene. In smaller districts, where grand juries meet less frequently, it may be difficult to get a material witness before a grand jury in only a few days. Additionally, it is not always practical to determine how extensive a material witness’s testimony will be. Questioning in the grand jury itself is likely to reveal new lines of questioning that prosecutors may want to pursue—extending the amount of time the witness may need to be detained. Similarly, it is not always possible to determine the extent to which the material witness will be cooperative. It is not unlikely that the material witnesses may be evasive or obstructive in the grand jury—again, extending the possible time of their detention. Putting a rigid time frame on the total time of detention would hamstring federal prosecutors—especially those from less populated districts—and could result in the loss of valuable testimony.

Two questions (#21B and #22) that I submitted to you following your confirmation hearing pertained to the federal death penalty. To both questions, you responded

that you would study the issues “carefully” if confirmed. Please answer those questions now.

160. Will you continue the policy, instituted by former Attorney General Ashcroft, of requiring that U.S. Attorneys clear all plea bargains with you? Why or why not?

ANSWER: The goal of the death penalty protocol is the fair, consistent, and even-handed application of the federal capital sentencing laws nationwide, irrespective of personal or community based bias for or against the death penalty. Clearly, that goal could be undermined by disparate practices regarding the circumstances that justify the withdrawal of a death notice. Accordingly, we consider continuation of this practice essential to the fair and consistent application of the capital sentencing laws.

161. Will you restore the pre-2001 version of section 9-10.070 of the U.S. Attorney’s Manual, which protected the interests of non-death penalty states like Vermont by ensuring that the absence of a state death penalty statute did not by itself establish a sufficient federal interest for capital prosecution? Why or why not?

ANSWER: The protocol in effect from January 27, 1995, to June 6, 2001, provided: “In states where the imposition of the death penalty is not authorized by law, the fact that the maximum federal death penalty is insufficient, standing alone, to show a more substantial interest in federal prosecution.” The elimination of this provision has not resulted in a significant, if any, increase in the number of death penalty prosecutions in non-death penalty states. For a homicide to be prosecuted in federal court, there must be a corresponding federal offense, and the decision whether to prosecute the crime in state or in federal court is usually mutual and founded on a variety of factors. While the elimination of this provision has not had a significant impact on federal charging practices, it could come into play in an appropriate case. The Department is not going to reinstate the identified provision.

163. Following your confirmation hearing, I asked you about a number of immigration cases, including (in question #28) whether you would retain the controversial “automatic stay” policy that was used for the “special interest” immigration detainees who were detained in the wake of the 9/11 attacks and, if so, why the traditional standard for release on bond in immigration proceedings – risk of flight or danger to the community – was inadequate. You replied that you had not had the opportunity to familiarize yourself with the details of immigration procedures, adding, “I look forward to looking into both of these issues if confirmed.” Have you looked into these issues and if so, would you please respond now to the questions?

ANSWER: The automatic stay regulation does not change the "traditional standard" for release on bond in immigration proceedings. See 8 C.F.R. § 1003.19(i)(2). Rather, it provides an orderly process for reconciling conflicting custody decisions by the Department of Homeland Security and an immigration judge, and is supported by the substantial policy considerations described when the regulation was published. See 63 Fed. Reg. 27441, 27447 (May 19, 1998); 66 Fed. Reg. 54909 (Oct. 31, 2001). As explained, "[t]his stay is a limited measure and is limited in time – it only applies where the Service determines that it is necessary to invoke the special stay procedure pending appeal, and the stay only remains in place until the Board [of Immigration Appeals] has had the opportunity to consider the matter." 66 Fed. Reg. at 54910.

The process by which the Attorney General and the Secretary of the Department of Homeland Security exercise their discretion under INA § 236(a) with respect to whether an alien should be detained during removal proceedings involves multiple administrative components. Under the regulations, Immigration and Customs Enforcement makes the initial custody decision in each case – that is, whether to keep the alien in detention pending completion of the removal proceedings, or whether to release the alien on bond or other appropriate conditions. The alien may appeal this determination to an immigration judge. 8 C.F.R. § 236.1(d)(1). That decision may in turn be appealed to the Board. 8 C.F.R. § 236.1(d)(3). See generally *Pisciotta v. Ashcroft*, 311 F. Supp.2d 445, 455 (D. N.J. 2004) ("consistent with the reasoning in [*Kim v. J. Demore*, this Court finds that the automatic stay provision effecting the ongoing detention of Petitioner, a criminal alien in pending removal proceedings, is constitutionally permissible"). The automatic stay regulation preserves the status quo while the Board, and on occasion the Attorney General, finally adjudicates the issue. Accordingly, we intend to retain the regulation.

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

164. Please explain the process followed by the Department and its components in reviewing documents for release under FOIA.

ANSWER: Requests for records under the Freedom of Information Act (FOIA) are initially processed by the Department components that possess the records. If the component does not produce all of the responsive records or redacts information from those records pursuant to FOIA's statutory exemptions, then the requestor is advised of his or her administrative appeal rights. Administrative appeals are adjudicated by the Department's Office of Information and Privacy (OIP) and often result in the release of additional text. A requestor may file suit in U.S. District Court if he or she is dissatisfied with the results of this process. Alternatively, requesters may file suit if the Department component does not respond to the request within the statutory time frame, as the ACLU chose to do in connection with the document request that included the FBI e-mail, dated May 10, 2004, that was described in your question.

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

ANSWER: As indicated above, each Department component (including the FBI) makes the initial determination in response to FOIA requests for its own records. Thereafter, the administrative appeal process conducted by OIP may result in the additional release and, in some cases, further determinations to release may occur in the litigation process.

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

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

A non-identical duplicate of the FBI document, dated May 10, 2004, (Bates 1373) was initially released by the FBI between September 15 and October 15, 2004, in accordance with the schedule for processing 1,388 pages, which the Court imposed in the ACLU litigation. A non-identical duplicate is, in this instance, an e-mail that contains the same information embedded in a different e-mail. The FBI processed the other version of the same document (Bates 2709) in November without the same time constraints, resulting in a different judgment regarding the release of information and, hence, reduced redactions.

In March, OIP was asked to review the document (Bates 2709) as if it were the subject of an administrative appeal and, in that process, the FBI agreed to release additional text, which had previously been withheld to protect privacy interests and deliberative process. This revised version was provided to Senators Levin and Lieberman, as well as the ACLU on March 18, 2005. As the cover letter to the Senators noted, a small amount of text remained redacted because it implicated the interests of the

Department of Defense (DOD) and, in accordance with established third-agency practice, there was an obligation to consult with DOD prior to making a decision on that text. On or about April 6, 2005, a fourth version of the document was disclosed to the Senators and the ACLU, which restored that text based upon the DOD review.

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

ANSWER: The FBI cited FOIA exemption (b)(5) in the margin corresponding to the "suspect at best" redaction, which pertains to "inter-agency and intra-agency memorandums or letters which would not be available by law to a party other than an agency in litigation with the agency." See 5 U.S.C. 552(b)(5). Exemption (b)(5) has been construed by the courts to exempt records that are normally privileged in the civil discovery process and is most commonly invoked to protect information relating to an agency's deliberative process. The "suspect at best" text was restored by the OIP review and was included in the version that was provided to Senators Levin and Lieberman with the Department's letter, dated March 18, 2005, and again, following the DOD consultation, in the version released on April 6, 2005.

168. I recently re-introduced the Restoration of Freedom of Information Act, S.622. The text of the bill is identical to the text of a White-House-endorsed compromise reached in the summer of 2002 regarding the protection of critical infrastructure information. During your confirmation process, I asked you (in question #39) whether you would support my bill. You replied that you did not have great familiarity with the issue, but would review the legislation if you were confirmed and work with me on the issue. Having had an opportunity to review the Restoration of Freedom of Information Act, do you support it and if not, why not?

ANSWER: As emphasized in our response to previous question #39, it is important to safeguard critical infrastructure information that is submitted to the federal government by the private sector for homeland security-related purposes, while at the same time also protecting the interests of openness in government. And we recognize that attempting to achieve this balance as best as possible is at the heart of the proposed legislation to which you refer. This is a matter that is of particular concern to the Department of Homeland Security, given its unique responsibilities in this subject area. As mentioned in our previous response that the Department of Homeland Security was then in the process of moving from an interim rule to a final one in its regulations on this subject, with further relevant information to be obtained during that process, and we are advised that this still remains the case. We are also advised that the Department of Homeland Security has not yet taken a position on this legislative proposal in this Congress, let alone communicated

a position on behalf of the executive branch. So it is most appropriate for the Department of Justice to defer consideration of this proposed legislation at this time. However, we can reiterate that, as the Justice Department stated in its most recent annual report to Congress on the FOIA (dated April 1, 2005), we look forward to continuing to work together with the Congress, in a constructive partnership based upon our mutual interests in sound FOIA administration, on all matters pertaining to the Act.

169. I also asked you after your confirmation hearing (in question #38) whether you would, if confirmed, continue Attorney General Ashcroft's FOIA policy or revert to a policy presumption based upon disclosure. You said you had not had the opportunity to review the Ashcroft FOIA policy, but promised that, "if confirmed, I would undertake an examination of the Department's policies and practices concerning FOIA disclosures." Have you undertaken such an examination and, if so, would you please respond now to the question?

ANSWER: The federal government's overall Freedom of Information Act ("the Act") policy certainly is an important matter, and in the Attorney General's prior position as Counsel to the President he had occasion to become generally familiar with this subject, perhaps more so than most incoming Attorneys General. Consequently, the Attorney General has readily become comfortable with the Department's overall policies for FOIA administration, including the Ashcroft FOIA policy memorandum of October 12, 2001, to which you refer. Insofar as your question asks whether the Attorney General anticipates that the Department will "revert to a policy presumption based upon disclosure," which might appear to be somewhat confusing, we can only reply that information disclosure always has been and remains the dominant objective of the Act, both law and policy. To reiterate what the Department stated in its most recent report to Congress on this subject on April 1, 2005: "I can assure you of the Department of Justice's firm commitment to the Freedom of Information Act, as amended by the Electronic Freedom of Information Act Amendments of 1996, and to its faithful implementation."

170. Shortly after you were confirmed as Attorney General, you gave a speech in which you discussed some of your priorities. You stated, "As we battle crime, we must also defend the rights of crime victims and assist them in their recovery." You then noted the Administration's support of a Victims Rights Constitutional Amendment, which you called, "a priority for the President and a priority for me." Yet just a few weeks earlier, President Bush sent Congress a budget that proposed raiding the Crime Victims Fund of an estimated \$1.2 billion. I find it hard to reconcile your rhetoric with your policies. Did the proposal to rescind the Fund originate at the Justice Department or at the White House? Do you support the President's proposal to rescind the Crime Victims Fund at the end of FY06?

ANSWER: The Administration has consistently supported the rights of crime victims and continues to recognize the need to empower and support those who provide vital services to crime victims. The President's Fiscal Year 2006 budget requests \$650 million to support the Crime Victims Fund. This is \$30 million more than Congress had enacted in Fiscal Year 2005. The Department recognizes that government-wide cuts in programs have been proposed and supports the President's Budget.

The funding source for the Crime Victims Fund, which provides crucial services and assistance to victims, will continue to be criminal fines, forfeited bail bonds, penalties and special assessments, and gifts, bequests or donations from private entities. The rationale for the rescission of remaining funds is that because the balances are controlled by obligation limitations only, the balances "rollover" and become available again every year -- a never ending offset. In essence, it's the same offset year after year. Rescinding the balances prevents them from rolling over on an annual basis, and is a more straight forward approach to budgeting.

Please be assured the Administration, and the Attorney General personally, remain committed to supporting services and assistance for crime victims and their families, and to efforts to improve the treatment of crime victims in the justice system.

173. In 1999, the President signed into law the Treasury and General Government Appropriations Act for Fiscal Year 2000 (P.L. 106-58), which created the National Intellectual Property Law Enforcement Coordination Council. One of the co-chairs of NIPLECC is the Assistant Attorney General of the Criminal Division of the Department of Justice. The President has nominated Alice Fisher to replace AAG Christopher Wray. What steps, if any, are being taken to ensure that during the transition the important work of NIPLECC does not literally get lost in the shuffle?

ANSWER: The protection of intellectual property rights continues to be an important focus of the Department, both through the aggressive investigation and prosecution of criminal intellectual property violations, and through the renewed work of the Department's Task Force on Intellectual Property. The Administration, through the Strategy Targeting Organized Piracy (or "STOP!"), has made intellectual property enforcement a top interagency priority. Given this emphasis on intellectual property protection, the joint work of the NIPLECC agencies has taken on a new importance and even has extended beyond the formal NIPLECC process. AAG Wray's replacement will be fully briefed on all aspects of intellectual property enforcement and all aspects of interagency coordination on these issues, including NIPLECC. Given the importance of intellectual property to the Administration and to the Department, there is no chance that the task of coordinating enforcement will be overlooked in the transition period.

174. **Protecting America's artists and innovators through strong intellectual property enforcement is vital to ensuring that the United States continues to be the world leader in intellectual property. In that effort coordination is critical. Please describe some of the Department's recent efforts in working with NIPLECC to coordinate enforcement efforts.**

ANSWER: The Department continues to work closely with the other agencies in NIPLECC to ensure that the intellectual property rights of U.S. citizens and corporations are enforced through using the full range of appropriate civil, administrative and criminal mechanisms, both domestically and abroad. The Department's domestic criminal enforcement efforts benefit from referrals of IP violations through the Commerce Department's website at www.StopFakes.gov, and the joint FBI/ICE National Intellectual Property Rights Coordination Center website at <http://www.ice.gov/graphics/cornerstone/ipr/>. Internationally, the Department has continued to assist foreign nations in building the criminal law enforcement capacity to protect intellectual property. The Department's success in international capacity building would not be possible without the financial and logistical assistance of the State Department, and the subject-matter expertise of other NIPLECC agencies including the U.S. Patent and Trademark Office, DHS Customs and Border Protection and Immigration and Customs Enforcement. The Department will continue to work with all the NIPLECC agencies to ensure a coordinated response to intellectual property crime by the United States Government.